Director, Operational Test and Evaluation

FY 2017 Annual Report

January 2018

This report satisfies the provisions of Title 10, United States Code, Section 139. The report summarizes the operational test and evaluation activities (including live fire testing activities) of the Department of Defense during the preceding fiscal year.

Robert F. Behler
Director

FY 2017 Annual Report

I was confirmed by the United States Senate November 19, 2017, and appointed by the President on November 21, 2017, as the seventh Director of Operational Test and Evaluation. It is an honor to serve in this position. I know from personal experience there are three imperatives in combat: Believe in yourself and your training; believe in your mission and commanders; and believe in your equipment and weapons. As the Director, Operational Test and Evaluation, I will provide independent and objective assessments so that our soldiers, sailors, airmen, and marines believe in their equipment and weapons, and are confident they are combat ready. I am committed to independently and objectively evaluating our systems to enable the Department of Defense (DOD) to make sound acquisition and deployment decisions. I will always be mindful of the taxpayer investments in our military and the priorities of the Secretary of Defense.

Most of the content in this report is based on tests conducted and independent evaluations completed before my tenure, but I have reviewed the content. In this introduction, I have contributed my own thoughts on future focus areas, the relevance of DOT&E, the importance of our workforce, and acquisition reform.

I submit this report, as required by section 139 of title 10, U.S. Code, summarizing the operational and live fire test and evaluation activities of the DOD during fiscal year 2017.

FOCUS AREAS

As I begin to shape my initiatives as the Director, my past experience, the emergence of new technologies, and the rapid evolution of threats suggest several key focus areas for the future. These areas include testing of software intensive systems and cybersecurity implications, integrated testing, test infrastructure, and modeling and simulation (M&S).

Software Intensive Systems & Cybersecurity

Today, the building material of choice for our weapon systems is software. The amount of software source lines of code in today's weapon systems is growing exponentially. Software does not just increase the functionality of these systems, it fundamentally defines the weapon system. However, as the number of lines of code increases so does the complexity of the system and cybersecurity vulnerabilities. The implications for T&E are profound. We are now making more changes that effect system capability through software than through hardware. For example, the F-35 Joint Strike Fighter's effectiveness in combat relies on software mission data loads, which work in conjunction with the avionics software and hardware to drive sensor search parameters. These files are critical for F-35 identification and correlation of threat and friendly radar signals. This increased dependence of system capabilities on software dictates that T&E must become a continuous, risk-based process for the life cycle of the system.

As weapon systems increase their dependency on software, the potential cybersecurity attack surface also increases. DOT&E has been a steady voice in the need to improve the cybersecurity posture of our systems, networks, and human interactions with networked systems. DOT&E has advocated for improved cybersecurity testing to identify critical problems and their operational impact and is currently funding the development of automated test tools. The cybersecurity section, later in this report, provides a number of recommendations to improve the Department's cybersecurity posture based on the past efforts of this office.

The cybersecurity of our weapons and networks needs increased attention. In support of that, the Department needs to evolve how we monitor our cybersecurity posture. The two-phase Cooperative Vulnerability and Penetration Assessment (CVPA) and Adversarial Assessment (AA) approach currently outlined in DOT&E test guidance is necessary to help inform the cybersecurity posture of DOD systems, but is not sufficient. This testing has greatly improved our understanding of cyber vulnerabilities, but in addition to dedicated assessments, DOD systems must be built to include technologies to continuously monitor cybersecurity, and automatically find and patch software vulnerabilities. Periodic assessments by Red Teams alone are not adequate, because the security of system software can change at any time due to operator errors, or adversary cyber-attacks. Red Teams are critical, but by themselves will never scale to meet the enormity of the cybersecurity challenge facing the Department.

One of my top priorities will be to update cybersecurity and risk-based testing guidance to reflect best business practices. Cybersecurity testing needs to move forward in the acquisition life cycle so that it can influence the system architecture from early development. I will advocate for additional resources for the development of automated software testing tools and the threat teams who use these tools. I will continue to advocate for rigorous cybersecurity testing and include evaluations of cybersecurity vulnerabilities in my assessments of systems. In the context of the rapid pace of software development, I will look for ways to align T&E activities with the velocity of the development of software systems.

Integrated Test and Evaluation

I am supportive of previous efforts by the Department's T&E community to integrate testing, but they have not gone far enough. During my tenure, I plan to expand on those efforts. I know from experience there are many instances where operational and live fire evaluations can benefit from data acquired during developmental testing (DT) and where DT events can benefit from greater operational realism. Incorporating operational factors in DT&E and conducting early operational assessments aids in early discovery of problems and performance shortfalls. My office has often observed that operational testing identifies system performance problems that should have been identified in DT&E. The discovery is often due to bringing together the combination of operational users and realistic environments, missions, and threats for the first time. A more integrated approach could identify these issues early, when there is still time and resources available to fix them.

The implications of integrated testing for taxpayers and the warfighter are undeniable. We must look for better approaches to coordinate the planning of developmental and operational testing with the goal of accelerating our knowledge of system capabilities while reducing discovery later in the program.

I plan to update existing DOT&E guidance to incorporate an integrated testing philosophy. In my independent assessments, I intend to use all credible information to provide the warfighter and the Congress a complete understanding of how the systems the Department acquires will improve the readiness and lethality of our military forces.

Test Infrastructure

The Department needs T&E infrastructure for the five warfighting domains: air, land, sea, space, and cyber. However, much of our test range infrastructure is over 50 years old, with some assets built prior to World War II. Twenty-eight percent of our Major Range and Test Facility Base (MRTFB) facilities are in poor or failing condition, with an estimated cost to repair of over $1.1 Billion. The majority of threats we have on the ranges do not represent the modern capabilities of our potential future adversaries. And, the once seemingly vast space of the open-air ranges is no longer large enough to test modern weapons and sensors at the employment distances envisioned. Test infrastructure for cyber is just now beginning to be realized, while the space domain remains in its infancy. We need to modernize our test ranges. As I stated in my confirmation hearing, I will visit major DOD test ranges early in my tenure to gain first-hand knowledge of their capabilities and limitations, and make recommendations accordingly.

An alarming trend over the past 10 years is that our potential adversaries are increasing their capabilities faster than the DOD test infrastructure can adapt and realistically represent them. The Department must accelerate the speed that threat capabilities are characterized and transferred to the test base. The test infrastructure of the future cannot just focus on open-air test ranges. The Department needs a strategy that incorporates software testbeds, software and hardware-in-the-loop facilities, anechoic chambers, open-air simulators, threat emulators, effects-based M&S, and open-air facilities. Open-air facilities need the ability to incorporate aspects of the virtual and constructive simulations to improve operational realism and span the full operational environment. As we develop infrastructure, particularly in the cyber and space domains, we must leverage virtual and constructive test environments.

The need to develop new test infrastructure quickly is important in the rapidly evolving areas of cyber threats and new software-enabled threat electronic warfare (EW) capabilities. Since 2010, DOT&E has used the yearly budget review process to advocate for resources to improve both cyber test capabilities and EW test range infrastructure to support realistic testing of modern combat systems. Notably, in 2012, DOT&E convinced the Department to invest nearly $500 Million in the Electronic Warfare Infrastructure Improvement Program (EWIIP) to upgrade open-air test ranges, anechoic chambers, and reprogramming laboratories in order to develop and understand the performance of the F-35 and other advanced air platforms against advanced near-peer threat integrated air defense systems. I will monitor those investments to see they come to fruition as the Department rapidly approaches the start of the F-35 IOT&E.

Other significant T&E infrastructure shortfalls that DOT&E has highlighted routinely include: Fifth Generation Aerial Target; Self-Defense Test Ship; multi-stage supersonic targets; torpedo and submarine surrogates for anti-submarine warfare operational testing; the Warrior Injury Assessment Manikin for assessing force protection of ground combat vehicles to underbody blast events; range sustainability; and testing of space programs against offensive space threats. I will review the adequacy of the Department's T&E infrastructure to perform the full range of T&E responsibilities of Department weapons systems and equipment and advocate for improvements for any shortfalls I identify.

Improving the use of Modeling and Simulation (M&S)

Modeling and simulation is a critical element of test and evaluation. DOD acquisition programs are progressively more complex systems that support missions in increasingly complex environments. Programs often rely on M&S to fill data gaps when testing is either too expensive or not technically feasible. Programs can use M&S to provide insights on performance over the entire operational envelope even when testing is limited to a few strategic shots. Future T&E activities will undoubtedly increase their reliance on M&S tools, especially in the domain of space. This will require the acquisition and test communities to improve upon current M&S capabilities, including verification, validation, and accreditation (VV&A) of M&S assets.

For programs that use M&S, program managers and Operational Test Agencies (OTAs) should design system T&E programs to collect adequate data to support the validation of those models. DOT&E issued guidance in March 2016 and January 2017 on ways to improve VV&A activities. VV&A activities should include a comparison of live test data to M&S runs coupled with a quantification of the uncertainty in such assessments. The DOD acquisition community should leverage emerging research methods from academia to improve the efficiency of VV&A activities, while ensuring the methods are scientifically sound. I plan to update DOT&E guidance on the use of M&S and the VV&A of such models to reflect my views on the importance of it in operational and live fire evaluations.

The Department needs to think about a wider application for M&S tools. For example, the Joint Technical Coordinating Group for Munition Effectiveness has initiated development of M&S tools for offensive cyber effects. These cyber effect tools are a non-kinetic threat parallel to the existing Joint Munition Effectiveness Manuals used by the weaponeers and mission planners. Cyber effects models will enable the Department to assess the survivability of our systems against adversary cyber threats. To support these modeling efforts, the Department should start generating data-based network models, threat characterization models, and models to predict the cyber effects for a range of target-weapon pairings. Similar to kinetic threats, such an approach would drive the materiel developers to design for survivability to the cyber threat, it would enable a more robust and quantified review of the system vulnerabilities and vulnerability mitigation features, and would enable a more phased or building block approach to survivability evaluation that includes component, sub-system, system, and full-up system-level testing.

DOT&E RELEVANCE TO THE DEPARTMENT

DOT&E's oversight enables the Department to deliver weapon systems that work though adequate testing. In FY17, DOT&E approved 35 Test and Evaluation Master Plans (TEMPs) and 95 test plans. DOT&E's independent assessments provide objective information to the military Services describing what works and what does not work, as well as provide recommendations for improvement. This objective information informs acquisition and fielding decisions that result in a more lethal force. In FY17, DOT&E provided 46 independent assessments for the Department and the Congress. DOT&E's contributions go beyond the benefits to specific programs. DOT&E's contributions and their impact to the larger DOD community from 2017 include:

- DOT&E improved the DOD cybersecurity posture using threat-representative cyber Red Teaming of Combatant Command networks during 12 major exercises and cyber readiness campaigns. The DOT&E find-fix-verify cybersecurity assessment program approach has improved the ability of Combatant Command network defenders to withstand realistic cyber-attacks and maintain their critical missions. The success of this program resulted in three Combatant Commands instituting permanent cyber Red Team operations on their live operational networks that will continually monitor and improve their cybersecurity posture.
- DOT&E funded improvements to M&S tools to better quantify system survivability. The Joint Live Fire (JLF) program worked to expand the validation of several widely used vulnerability M&S tools and improved the ability of those tools to support the assessment of system survivability. DOT&E's JLF program funded projects that will inform programs on the factors that most affect system vulnerabilities as well as the uncertainty inherent in those predictions.
- DOT&E improved test infrastructure for testing fifth generation systems. DOT&E is leading the development and testing of the Fifth Generation Aerial Targets (5GAT). This target will support operational and live fire testing of advanced weapon systems against low-observable targets. Testing against these targets will inform warfighters on how their weapons will work against advanced adversaries. These relatively low cost targets are currently meeting all early performance and cost goals.
- DOT&E collaborated with international partners to improve testing efficiency by sharing test venues and infrastructure. For example, DOT&E developed and fielded weaponeering tools in support of U.S. Forces Korea/Combined Forces Command to have effective target planning, munitions requirement development, and weapon procurement analysis. These efforts received the attention of General Jeong Kyeong-doo, Chairman of the Republic of Korea Joint Chiefs of Staff. Additionally, DOT&E collaborated with Israel on Army network modernization. The Israeli Defense Forces invited DOT&E and Army personnel to observe the Ground Forces exercise Light of Dagan, Israel's largest military exercise in 19 years.

One way that DOT&E can provide more relevant information to the Department is by proactively encouraging integrated testing. Including operational factors in developmental testing will help identify problems earlier, when they can still influence system design. In cases where systems perform well, programs should be able to take credit for early data, reducing the required resources in IOT&E. While I cannot direct developmental testing, I plan to have my staff engage early to look for opportunities to integrate testing with the goal of facilitating early learning and reducing the overall testing required of systems, when systems perform well. One example of how I plan to be flexible with integrated testing is my engagement with F-35 test stakeholders. I am working with them to allow approval of early test events. We are currently engaging with the test team to approve pre-IOT&E activity for cold weather testing in early 2018, months prior to the official IOT&E. If the program meets system development milestones, I will consider additional pre-IOT&E activity. This early testing will reduce the data required during the formal IOT&E period, which will increase aircraft availability for the core IOT&E missions. Increased aircraft availability will reduce execution risk helping to complete testing on

time. Additionally, because cold weather testing must occur during the winter, my approval of this pre-IOT&E activity may eliminate the need for a cold weather deployment in the middle of the dedicated IOT&E.

In 2018, I will continue to look for ways that DOT&E can use our operational and technical expertise to provide relevant and credible information to the Department and the Congress.

STATUS OF THE OPERATIONAL TEST WORKFORCE

As I mentioned during my confirmation testimony, one of my highest priorities is to assess the current DOT&E and Service Operational Test Agency (OTA) workforce. To adequately assess the operational effectiveness, suitability, and survivability of weapon systems, a skilled workforce must have a clear understanding of the current operational tactics, techniques, and procedures and the operational threats to units equipped with these systems. The workforce must understand the operational mission and the systems under test, and apply scientific, statistical, and analytical techniques to evaluate those systems.

Since 2010, DOT&E has seen reductions in our staffing from a peak in 2010 of 93 civilians, 17 military billets, and 66 contractors to 80 civilians, 17 military billets, and 28 contractors in 2017. By FY20, my staff will be reduced to 76 civilians, 14 military billets, and 28 contractors. DOT&E must maintain the right mix of expertise in both military operations and technical knowledge to independently evaluate a diverse range of systems. In FY17, there were 308 systems under DOT&E oversight; the number and diversity of these systems require a highly skilled workforce. I plan to evaluate the efficacy of the government and contractor mix in the office of the DOT&E and identify areas that may need to be complemented with individuals who are savvy with emergent technologies and current operational experience.

DOT&E also reviews the state of the overall OTA workforce. It is critical that OTA personnel have strong operational, scientific, and analytical expertise. The Services have reduced the OTA workforce during the last decade. The OTA workforce fell over 12 percent between 2006 and 2016, driven mostly by the loss of military personnel. Many of these losses are attributable to draw downs in the overall military. Nonetheless, the loss of military personnel with operational experience diminishes the ability of the OTAs to test and evaluate increasingly complex weapon systems. Since 2010, the OTA workforce has remained relatively stable at approximately 1,900 personnel. At the current level of staffing, my staff has observed that the OTAs sometime have to prioritize programs and have limited access to subject matter experts across the ranges of areas of expertise necessary to test complex military systems.

DOT&E also continues to have a concern about retirement-eligible civilians within the OTA workforce, which increased to 43 percent in 2016. The OTA retirement eligibility rates are well above the GAO predicted rates for both the DOD and overall Federal workforces that could produce mission critical knowledge gaps if left unaddressed (see U.S. Government Accountability Office report GAO-14-215, "Federal Workforce: Recent Trends in Federal Civilian Employment and Compensation," January 2014). Based on the most recent analysis completed this year, I will work with the OTAs to develop workforce strategies that:

- Monitor the number of military personnel supporting T&E so that operational expertise is not lost.
- Develop recruitment plans that prevent mission critical skills gaps from developing as skilled civilians retire and create a future workforce ready for the evolving needs of T&E. In response to evolving technologies, the OTAs should recruit individuals with cybersecurity, statistics, autonomy, machine learning, human factors, and M&S expertise.
- Collaborate on best practices for providing both educational opportunities to targeted members of the workforce and training to the broader workforce, potentially leveraging elements of each other's programs and DOT&E-sponsored training.

I will assess the adequacy of the OTA workforce over the next year and update this assessment.

DOT&E SUPPORT TO THE TEST AND EVALUATION WORKFORCE

The Department will continue to acquire sophisticated technologies and we need a test workforce that is well equipped to test those technologies. Advancing methods for T&E requires partnering with academia, industry, professional test societies, and other government agencies. To that end, my office has collaborated with former Deputy Assistant Secretary of Defense for Developmental Test & Evaluation (DASD DT&E)/Director, Test Resource Management Center (TRMC), National Aeronautics and Space Administration (NASA), and academia to support the T&E Workforce. Going forward, I will continue this collaboration with the future leadership of these organizations.

In collaboration with TRMC, my office funds the Science of Test Research Consortium, which develops new techniques, aids in the education of the T&E workforce, and provides an important link between academia and the T&E community. I look forward to expanding these research efforts to address evolving needs in cybersecurity and software testing. In collaboration with NASA, my office supports the Defense and Aerospace Test and Analysis Workshop (DATAWorks), which seeks to build a community around statistical approaches to T&E in defense and aerospace. I also support DASD DT&E's funding of the Scientific Test and Analysis

Techniques Center of Excellence, which partners with major acquisition programs to develop scientifically sound test programs and has recently expanded to include expertise in software and cybersecurity testing.

DOT&E also supports the workforce by developing training materials and resources that are available to the wider T&E community. Resources are available on TEMP development, test planning, experimental design, software testing, reliability growth planning and testing, cybersecurity, statistical analyses, survey design and analysis, and M&S. Resources are forthcoming on the development of Live Fire Test and Evaluation Strategies.

ENSURING ADEQUATE OT&E AND LFT&E UNDER ACQUISITION REFORM

I am very supportive of acquisition reform efforts to streamline and improve the defense acquisition process to build a more lethal force. DOT&E welcomes smart reforms that make the acquisition system more efficient and allow the DOD to provide warfighters with timely new capabilities that work. The statutory responsibilities provided to this office are essential to ensure adequate and realistic testing. I will collaborate with the Department acquisition community to accelerate the speed of acquisition when prudent to significantly reduce the time to deliver war-winning capability to our soldiers, sailors, airmen, and marines.

I am supportive of efforts to improve testing through the increased use of M&S and integrated developmental and operational testing. I firmly believe that testing early and often will improve acquisition outcomes by informing better system design and providing decision makers with information on system capabilities as they are developed. I support integrated testing to demonstrate system capabilities early and inform what data are needed from operational testing. I will be mindful of the balance between M&S, integrated testing, and operational and live fire testing when approving the adequacy of operational test plans. Additionally, I will focus on ensuring that operational and live fire testing remains adequate, while supporting the intent of acquisition reform, to streamline the DOD acquisition process.

We need to revisit the best practices of competitive system prototyping incorporating new technologies to improve future acquisition outcomes. Competitive system prototyping, followed by live experimentation on the ranges and quick iterations on system design has helped weapon systems evolve quickly. Then, a final fly-before-buy period provided the government and the Congress with the assurances that they needed before fielding systems. On the B-2 program in particular, we used a maturity model to manage expectations and show progress towards acquiring full operational capability. At major milestones, we reviewed progress, compared to the system maturity model, and updated expectations for the future.

In order to improve future acquisitions, we need to integrate testing into the system engineering process starting with early system prototypes. We must acknowledge the degree at which software defines system capabilities and the rate of software updates in our testing philosophy. Rapid prototyping, including digital prototyping using M&S, should focus on rapidly developing stable hardware designs. Once the hardware is stable, using iterative incremental development supports rapid software co-development and testing, and subsequent incremental fielding of software-defined capabilities. As systems become more complex, integrate autonomous capabilities, and software defines system capability, we must engage in testing early and often to inform decisions and manage expectations.

CONCLUSION

I have spent my professional career preparing for the opportunity to be the Director of Operational Test and Evaluation. I have employed weapons in combat environments and have been both a developmental and operational test pilot. And, for the last 5 years, I have been immersed into the technical areas of software engineering and cybersecurity. I will use these experiences to establish a professional core of operational testers that will provide equipment and weapons that are effective, suitable, and survivable in combat. We owe our warfighters and taxpayers nothing less.

Robert F. Behler
Director

Contents

Navy Programs

Air Force Programs

FY17 TABLE OF CONTENTS

DOT&E Activity and Oversight

DOT&E Activity and Oversight

FY17 Activity Summary

DOT&E activity for FY17 involved oversight of 302 programs, including 28 Major Automated Information Systems (MAIS). Oversight activity begins with the early acquisition milestones, continues through approval for full-rate production, and, in some instances, during full production until removed from the DOT&E oversight list.

DOT&E review of test planning activities for FY17 included approval of 31 Test and Evaluation Master Plans (TEMPs), 95 Operational Test Plans, and 3 LFT&E Strategies/Management Plans (not included in a TEMP). DOT&E also disapproved the following TEMP and Test Plan:

- Air Force Distributed Common Ground System (DCGS) Capstone TEMP
- Geosynchronous Space Situational Awareness System (GSSAP) Follow-on Operational Test and Evaluation (FOT&E) Test Plan

In FY17, DOT&E prepared 17 reports for Congress and SECDEF: 1 Cybersecurity report, 5 Early Fielding reports, 4 FOT&E reports, 1 IOT&E report, 2 LFT&E reports, 1 Operational Assessment (OA) report, 1 special report, 1 Limited User Test (LUT) report, and the Ballistic Missile Defense System Annual Report. Additionally, DOT&E prepared 24 non-Congressional reports for DOD stakeholders: 7 Cybersecurity reports, 1 Early Operational Assessment report, 2 FOT&E reports, 1 LFT&E report, 4 Limited User Test reports, 6 OA reports, 1 OT&E report, and 2 special reports. Some of these non-Congressional reports were submitted to Defense Acquisition Board (DAB) principals for consideration in DAB deliberations.

During FY17, DOT&E met with Service operational test agencies, program officials, private sector organizations, and academia; monitored test activities; and provided information to Congress, SECDEF, the Deputy Secretary of Defense, Service Secretaries, USD(AT&L), DAB principals, and the DAB committees. DOT&E evaluations are informed in large part through active on-site participation in, and observation of, tests and test-related activities. In FY17, DOT&E's experts joined test-related activities on 237 local trips within the National Capital Region and 913 temporary duty assignment trips in support of the DOT&E mission.

Security considerations preclude identifying classified programs in this report. The objective, however, is to ensure operational effectiveness and suitability do not suffer due to extraordinary security constraints imposed on those programs.

TEST AND EVALUATION MASTER PLANS / STRATEGIES APPROVED (LIVE FIRE STRATEGIES MARKED WITH *)

AH-64E Version 6 Capability Apache Helicopter TEMP*

Air Force Mission Planning System Increment 5 (MPS-5) MAIS TEMP

AN/BQQ-10 Sonar System Advanced Processing Build 2013 TEMP

APR-39D(V)2 TEMP

B-2 Extremely High Frequency Satellite Communications (EHF SATCOM) Milestone A TEMP

Cartridge, 7.62 Millimeter Advanced Armor Piercing XM1158 / Tracer XM1159 TEMP*

Coastal Battlefield Reconnaissance and Analysis (COBRA) Block I TEMP Revision 1, Change 3

DAI Increment 2 Release 4 TEMP Addendum

Deliberate and Crisis Action Planning and Execution Segments (DCAPES) Increment 2B Milestone B TEMP

Distributed Common Ground System – Army (DCGS-A) Milestone B TEMP

Distributed Common Ground System – Navy (DCGS-N) Increment 2 TEMP

F/A-18 E/F and EA-18G H12 TEMP 1787

Indirect Fire Protection Capability Increment 2 - Intercept (IFPC Inc 2-I) Block 1 Milestone B Pre-MDAP TEMP *

KC-46A Milestone C TEMP*

Maintenance, Repair, and Overhaul initiative (MROi) Milestone B TEMP

Manpack (MP) Radio Full and Open Competition (FOC) TEMP

MQ-1C Extended Range (ER) TEMP

MQ-1C Extended Range (ER) Increment I TEMP

MQ-4C Triton Unmanned Air System TEMP No.1721 Rev D

MQ-8 Fire Scout Unmanned Aircraft System (UAS) Acquisition Category (ACAT) IC TEMP

Next Generation Diagnostic System (NGDS) TEMP

Ohio Replacement (OR) Class SSBN Program Milestone B TEMP*

Patriot System TEMP Change Pages

Soldier Protection System (SPS) Integrated Head Protection System (IHPS) TEMP*

Soldier Protection System (SPS) Torso and Extremity Protection (TEP) TEMP*

Spider M7E1, Dispensing Set, Munition, Network Command Increment 1A for Milestone C and Low-Rate Initial Production (LRIP) Phase TEMP

Standard Missile-6 (SM-6) TEMP TEIN 1675 Revision A Annex*

T-AO 205 (formerly T-AO(X)) Fleet Replenishment Oiler Program TEMP No. 1835*

U.S. Marine Corps CH-53K Heavy Lift Replacement Program TEMP*

Warfighter Information Network-Tactical (WIN-T) Increment 2 (Inc2) TEMP

XM17 Modular Handgun System (MHS) TEMP*

OPERATIONAL TEST PLANS APPROVED

AC-130J Block 20 Cybersecurity (Adversarial Assessment (AA)) Test Plan

AC-130J Block 20 Cybersecurity (Cooperative Vulnerability and Penetration Assessment (CVPA))

Test Plan

AC-130J Block 20 Precision Strike Package Test Plan

Aegis Destroyer Baseline 9.C1 Verification of Correction of Deficiencies Test Plan

Aegis Weapon System (AWS) Baseline 9C (BL 9C) Air Defense Destroyer IOT&E Plan Change 2

Aegis Weapon System (AWS) Baseline 9C (BL 9C) Air Defense Destroyer IOT&E Plan Change 3

AH-64E V6 Live Fire Operational Test Agency (OTA) Test Plan

Air Warfare/Ship Self Defense (AW/SSD) Enterprise (ET15) supporting the Amphibious Assault Ship Replacement (LHA(R)) Flight 0 IOT&E, Ship Self Defense (SSDS) MK 2 Mod 4B FOT&E, and Rolling Airframe Missile (RAM) Block 2 IOT&E Operational Test Plan

Amphibious Assault Ship Replacement (LHA (R) Flight 0) IOT&E Test Plan

Amphibious Assault Ship Replacement (LHA (R)) IOT&E and Ship Self-Defense System (SSDS) MK 2 FOT&E Test Plan

Amphibious Assault Vehicle Survivability Upgrade (AAV-SU) Operational Assessment Test Plan (OATP)

Amphibious Combat Vehicle (ACV) 1.1 Engineering and Manufacturing Development (EMD) Phase System-Level and Exploitation Testing Detailed Test Plan (DTP)

Amphibious Combat Vehicle Phase 1, Increment 1 (ACV 1.1) Armors from BAE Systems (BAE) and from Science Applications International Corporation (SAIC) Behind-Armor Debris (BAD) Testing Detailed Test Plans (DTPs)

AN/APR-39D FOT&E Operational Test Agency (OTA) Test Plan (TP)

AN/BQQ-10 Sonar System Advanced Processing Build 2013 Test Plan Change 1

AN/SSQ-89A(V)15 Surface Ship Undersea Warfare (USW) Combat System Program Cybersecurity Test Plan

AN-BQQ-10 Sonar Systems Advanced Processing Build 2013 Test Plan

Apache Helicopter-64 Echo (AH-64E) v6 Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan

APR-39 (V)2 Operational Assessment Test Plan (OA) Test Plan

Army Tactical Missile System (ATACMS) Modification (Mod) Program System Qualification Test (SQT)-7 User Demo Test Plan

Army/Navy Transportable Radar Surveillance – Forward-based Mode [AN/TPY-2 (FBM)] Superdome Radar and the System of Systems CVPA Test Plan for the Command, Control, Battle Management, and Communications (C2BMC) Spiral 8.2, the Ballistic Missile Defense System (BMDS) Overhead Infrared (OPIR) Architecture (BOA) 5.1, and the AN/TPY-2 (FBM) Superdome Radar Element-Level Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan

Ballistic Missile Defense System (BMDS) Integrated Master Test Plan (IMTP) v18.0

Ballistic Missile Defense System (BMDS) Integrated Master Test Plan (IMTP) v18.1

Amphibious Combat Vehicle (ACV) 1.1 Engineering and Manufacturing Development (EMD) Phase Ballistic Testing of Armor Coupons Detailed Test Plan (DTP)

Battle Control System-Fixed (BCS-F) Release 3.2.4 (R3.2.4) Force Development Evaluation (FDE) Plan

C-130J Block Upgrade 8.1 Cybersecurity Test Plan

Coastal Battlefield Reconnaissance and Analysis (COBRA) IOT&E Test Plan

Columbia Class Submarine Early Operational Assessment Test Plan

Common Analytical Laboratory System (CALS) Man-Portable Subsystem Development/Operational (DT/OT) Test Plan

Common Infrared Countermeasure (CIRCM) System Operational Assessment Test Plan

Countermeasure Anti-Torpedo (CAT)/Torpedo Warning System (TWS) Quick Reaction (QRA) #3 Test Plan

Defense Agency Initiative (DAI) IOT&E Test Plan

Defense Enterprise and Accounting Management System (DEAMS) Increment 1 Operational Utility Evaluation (OUE) Test Plan

Defense Medical Information Exchange (DMIX) Release 5 (R5) Cybersecurity Test Plan

Department of Defense (DOD) Healthcare Management System Modernization (DHMSM) Operational Assessment (OA) Plan

Department of the Navy Large Aircraft Infrared Countermeasures (DON LAIRCM) Advanced Threat Warning (ATW) System as Installed on the MV-22B Quick Reaction Assessment Test Plan

Department of Defense (DOD) Healthcare Management System Modernization (DHMSM) IOT&E Plan

Enhanced Polar System (EPS) Cooperative Vulnerability and Penetration Assessment (CVPA) Plan

Enhanced Small Arms Protective Insert (ESAPI) First Article Test (FAT) Detailed Test Plan

F-22A Increment 3.2B IOT&E Plan Approval

F-35 Joint Strike Fighter (JSF) Air Vehicle (AV) Software Data Load (SDL) Cybersecurity Operational Test Plan

F-35 JSF IOT&E Low Observable Stability Over Time (LOSOT) Test Design

F-35 JSF Autonomic Logistics Information System (ALIS) 2.0.2 Cybersecurity Operational Test Plan

F-35A LOSOT Force Development Evaluation (FDE) Test Plan

Geosynchronous Space Situational Awareness Program (GSSAP) FOT&E Plan

Ground/Air Task Oriented Radar (G/ATOR) Block 1 Operational Assessment Test Plan

Ground/Air Task Oriented Radar (G/ATOR) Developmental Test 1C Integrated Test Plan

Integrated Head Protection System (IHPS) First Article Test (FAT) Detailed Test Plan

Ground/ Air Task Oriented Radar (G/ATOR) Integrated Test Event for OT&E Test Plan

Joint Light Tactical Vehicle (JLTV) Full-Up System-Level (FUSL) Operational Test Agency Test Plan (OTA TP)

Joint Light Tactical Vehicle (JLTV) Production and Deployment Phase Full-up System-Level (FUSL) Live Fire Test Detailed Test Plan (DTP)

Joint Precision Aided Landing System (JPALS) IOT&E Phase I Test Plan

Joint Regional Security Stack (JRSS) v1.5 Operational Assessment Plan

KC-130J with Harvest Hercules Airborne Weapons Kit IT-IIIE Live Fire Test Plan Deviation

Key Management Infrastructure (KMI) Spiral 2 Spin 2 Limited User Test (LUT) Plan

Littoral Combat Ship (LCS) Independence Variant with Increment 2 SUW (MP) IOT&E (OT-C4A) Test Plan Change Pages

Low-Rate Initial Production (LRIP) Autonomic Logistics Operating Unit (ALOU) Release 2.0 Cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) and Adversarial Assessment (AA) Test Plan

Mission Planning Systems (MPS) Increment 5 C-17 IOT&E Plan

Mission Planning Systems (MPS) Increment 5 Mobility Air Forces Automated Flight Planning System (MAFPS IOT&E Plan

Modular Handgun System (MHS) IOT&E Operational Test Agency Test Plan (OTA TP)

MQ-1C Gray Eagle Cooperative Vulnerability Identification (CVI)/ Cooperative Vulnerability and Penetration Assessment (CVPA)

MV-22B FOT&E Test Plan

Next Generation Chemical Detector Early Operational Assessment Operational Test Agency Test Plan (NGCD EOA OTA TP)

Next Generation Diagnostic System (NGDS) Increment 1 Adversarial Assessment Test Plan

Next Generation Diagnostic System (NGDS) Increment 1 IOT&E Test Plan

Next Generation Diagnostics System (NGDS) Sentinel Panel Developmental Test (DT)/Operational Test (OT) Test Plan

Offensive Anti-Surface Warfare (OASuW) Increment (Inc) 1 Long Range Anti-Ship Missile (LRASM) Quick Reaction Assessment (QRA) Test Plan

Ohio Replacement (OR) Class SSBN Live Fire Test and Evaluation (LFT&E) Management Plan

Operational Utility Evaluation (OUE) Test Plan for Joint Space Operations Center (JSpOC) Mission System (JMS) Increment 2 Service Pack 9

P-8A Poseidon Multimission Maritime Aircraft FOT&E Test Plan

Patriot Post-Deployment Build-8 (PDB-8) Cooperative Vulnerability and Penetration Assessment (CVPA) Plan

Patriot Post-Deployment Build-8 (PDB-8) IOT&E Adversarial Assessment Test Plan

Patriot Post-Deployment Build-8 (PDB-8) IOT&E Plan

Public Key Infrastructure (PKI) Increment 2, Spiral 3 FOT&E Plan

Soldier Protection System (SPS) Expanded Developmental Testing (DT) Test Deviation

Soldier Protection System (SPS) Live Fire Test and Evaluation Expanded Developmental Testing of Vital Torso Protection (VTP) Plates and Legacy Plates with Modular Scalable Vest (MSV) Shootpacks

Soldier Protection System (SPS) Live Fire Test Torso and Extremity Protection (TEP) Full-Up System-Level (FUSL) Detailed Test Plan

Soldier Protection System (SPS) Torso and Extremity Protection (TEP) Detailed Test Plan for the Lot Acceptance Test (LAT)

Soldier Protection System (SPS) Torso and Extremity Protection (TEP) Operational Test Agency (OTA) Test Plan (TP)

Soldier Protection System (Vital Torso Protection (VTP) Subsystem Live-Fire Testing OTA Test Plan

Standard Missile-6 Block IA (SM-6 Blk IA) OT-D4 FOT&E Test Plan

Standard Missile-6 (SM-6) IOT&E Deficiency Verification of Correction of Deficiencies Detailed Test Plan

Standard Missile-6 Block I (SM-6 BLK I) FOT&E OT-D2 Test Plan Modeling and Simulation Runs for the Record (RFR)

Stryker Infantry Carrier Vehicle – Dragoon (ICVD) Operational Test Agency Test Plan (OTA TP) and Detailed Test Plan (DTP) for Full-Up System-Level (FUSL) Live Fire Testing

Stryker Infantry Carrier Vehicle Dragoon (ICVD) 30-mm Lethality Upgrade Operational Cybersecurity Test Plan

Submarine Torpedo Defense System (Sub TDS) Increment 1 Integrated Evaluation Framework (IEF)

U.S. Pacific Command, Pacific Sentry 2017-3 (PS 17-3) Capstone Event Plan

USAFRICOM Exercise Judicious Response 2017 Assessment Plan

USS *America* (LHA 6) Total Ship Survivability Trial (TSST) Plan

Virginia Class Submarine Block III Test Plan

Virginia Class Submarine Block III Strike Warfare Test Plan

Warfighter Information Network – Tactical (WIN-T) Increment 2 (INC2) Network Operations Security Center – Lite (NOSC-L) Tactical Communications Node – Lite (TCN-L) FOT&E Operational Test Agency Test Plan (OTA TP)

LIVE FIRE TEST AND EVALUATION STRATEGIES / MANAGEMENT PLANS

Army Tactical Missile System (ATACMS) Modification (Mod) Live Fire Test and Evaluation (LFT&E) Strategy and Operational Test Agency Test Plan (OTA TP)

Ohio Replacement (OR) Class SSBN Live Fire Test and Evaluation (LFT&E) Management Plan

T-AO 205 (formerly T-AO(X)) Fleet Replenishment Oiler Program Live Fire Test & Evaluation (LFT&E) Management Plan

TABLE 1. FY17 REPORTS TO CONGRESS	
PROGRAM	**DATE**
Cybersecurity Report	
Defensive Cyberspace Operations: Findings from Department of Defense (DOD) Operational Tests and Assessments in Fiscal Year 2014 through Fiscal Year 2016	April 2017
Early Fielding Reports	
Littoral Combat Ship with Increment 2 Surface Warfare (SUW) Mission Package (MP)	November 2016
AN/VRC 118 Mid-Tier Networking Vehicular Radio and Joint Enterprise Network Manager	January 2017
AH-64E Installation of Department of the Navy Large Aircraft Infrared Countermeasure (DON LAIRCM) Advanced Threat Warning System (Army Response to U.S. Special Operations Command Joint Urgent Operational Need) Limited Fielding Report	January 2017
SeaRAM System on the *Arleigh Burke* Class Destroyers	January 2017
Next Generation Diagnostic System (NGDS) Increment 1 with classified Annex	June 2017
Follow-on Operational Test and Evaluation Reports	
Joint Standoff Weapon (JSOW) Block III	January 2017
MQ-9 Reaper Unmanned Aircraft System with the Block 5 Aircraft and Block 30 Ground Control Station	January 2017
AN/BLQ-10 (BLQ-10) Submarine Electronic Warfare Support System with the Technical Insertion 2010 Upgrade and the AN/BSD-3 Multifunction Modular Mast	August 2017
AGM-88E Advanced Anti-Radiation Guided Missile	September 2017
Initial Operational Test and Evaluation Report	
Defense Agency Initiative (DAI) with classified Annex	September 2017
Live Fire Test and Evaluation Reports	
Modernized Expanded Capacity Vehicle (MECV) – Survivability	November 2016
M1070A1 Heavy Equipment Transporter (HET) Urban Survivability Kit (HUSK)	June 2017
Operational Assessment Report	
M109 Family of Vehicles Paladin Integrated Management with classified Annex	January 2017
Limited User Test Report	
Army Integrated Air and Missiles Defense (AIAMD) System Increment II	January 2017
Special Report	
Mine Resistant Ambush Protected (MRAP) Cougar Category I A1 Block 1 Upgrades and Category II A1 Seat Survivability Upgrade Report	May 2017
Ballistic Missile Defense System Report	
FY16 Assessment of the Ballistic Missile Defense System (includes unclassified Executive Summary)	April 2017

TABLE 2. OTHER FY17 REPORTS (NOT SENT TO CONGRESS)	
PROGRAM	**DATE**
Cybersecurity Reports	
Global Lightning 2016 Cybersecurity Assessment	December 2016
Theater Medical Improvement Program Joint Increment 2 Release 3 Cybersecurity Assessment	January 2017
Pueblo Chemical Agent-Destruction Pilot Plant (PCAPP) Cybersecurity Assessment	February 2017
Observations During Special Operations Command Europe (SOCEUR) Exercise Jackal Stone 2016	February 2017
Cybersecurity Test and Evaluation of the Aegis Weapons System (AWS) Baseline 9.B1 Installed at the Aegis Ashore Missile Defense System (AAMDS) in Deveselu, Romania	February 2017
Cybersecurity Assessment of U.S. Africa Command Exercise JUDICIOUS RESPONSE 2017	May 2017
U.S. Pacific Fleet Exercise Valiant Shield 2016	July 2017
Early Operational Assessment Report	
Next Generation Chemical Detector (NGCD) Increment 1 Detector Alarm	March 2017
Follow-on Operational Test and Evaluation Reports	
Global Broadcast Service FOT&E-1 with classified Annex	November 2016
Consolidated Afloat Networks and Enterprise Services (CANES)	September 2017
Live Fire Test and Evaluation Report	
Littoral Combat Ship 4 (LCS 4) Total Ship Survivability Trial (TSST)	September 2017
LUT Reports	
Public Key Infrastructure, Increment 2, Spiral 3	November 2016
Spider Increment 1A with Classified Annex	January 2017
Command Web with classified Annex	January 2017
Key Management Infrastructure (KMI) Spiral 2 Spin 2	September 2017
Operational Assessment Reports	
Key Management Infrastructure (KMI) Spiral 2 Spin 2 with classified Annex	April 2017
AN/APR-39D(V)2 Radar Signal Detection Set (RSDS) on the Army AH-64D/E Aircraft	April 2017
Common Analytical Laboratory System (CALS) Field Confirmatory Analytical Capability Sets (FC-ACS)	May 2017
Integrated Defensive Electronic Counter Measure (IDECM) Block 4 Software Improvement Program (SWIP)	June 2017
Department of Defense (DOD) Healthcare Management System Modernization (DHMSM)	July 2017
Operational Test and Evaluation Report	
Battle Control System-Fixed (BCS-F) Release 3.2.3	May 2017
Combined Operational Test and Live Fire Test and Evaluation Reports	
CH-53K Heavy Lift Replacement Program with classified Annex	February 2017
Special Reports	
Large Scale Data Analytics Reveal Stealthy Adversarial Actions Report	December 2016
Assault Amphibious Vehicle - Survivability Upgrade (AAV-SU) Preliminary Report with classified Annex	August 2017

FY17 DOT&E ACTIVITY AND OVERSIGHT

Program Oversight

DOT&E is responsible for approving the adequacy of plans for operational test and evaluation and for reporting the operational test results for all Major Defense Acquisition Programs (MDAPs) to the Congress, SECDEF, Service Secretaries, and Under Secretary of Defense for Acquisition, Technology and Logistics. Any program that meets the criteria established in section 2430 of title 10, United States Code (10 USC 2430) is considered an MDAP and is subject to the requirement for periodic Selected Acquisition Reports (SARs) from SECDEF to Congress. DOT&E may designate any other programs as MDAPs in accordance with 10 USC 139(a)(2)(B) for the purpose of oversight, review, and reporting. These additional MDAPs are not subject to SAR requirements. Including such "non-SAR" programs, DOT&E was responsible for overseeing the OT&E of 302 acquisition programs during FY17.

DOT&E selects non-SAR programs for oversight after careful consideration of the relative importance of individual programs. One or more of the following essential elements factor into this consideration:

- Congress or OSD agencies have expressed a high level of interest in the program.
- Congress has directed that DOT&E assess or report on the program as a condition for progress or production.
- The program requires joint or multi-Service testing (10 USC 139(b)(4) requires DOT&E to coordinate "testing conducted jointly by more than one military department or defense agency").
- The program exceeds or has the potential to exceed the dollar threshold definition of a major program according to DOD Directive 5000.01, "The Defense Acquisition System," but does not appear on the current SAR list (e.g., highly classified systems).
- The program has a close relationship with or is a key component of a major program.
- The program is an existing system undergoing major modification.
- The program was previously a SAR program and operational testing is not yet complete.

DOT&E is also responsible for the oversight of LFT&E programs, in accordance with 10 USC 139. The DOD uses the term "covered system" to include all categories of systems or programs identified in 10 USC 2366 as requiring LFT&E. In addition, systems or programs that do not have acquisition points referenced in 10 USC 2366, but otherwise meet the statutory criteria, are considered covered systems for the purpose of DOT&E oversight. DOT&E was responsible for overseeing the LFT&E of 124 acquisition programs during FY17.

A covered system, for the purpose of oversight for LFT&E, has been determined by DOT&E to meet one or more of the following criteria.

- A major system, as defined in 10 USC 2302(5), that is:
  - User-occupied and designed to provide some degree of protection to the system or its occupants in combat
  - A conventional munitions program or missile program
- A conventional munitions program for which more than 1 million rounds are planned to be acquired.
- A modification to a covered system that is likely to affect significantly the survivability or lethality of such a system.

Following is the list of DOD, Army, Navy, and Air Force programs under DOT&E oversight in FY17, as taken from the September 2017 DOT&E Oversight List.

DOD PROGRAMS

AC-130J

BMDS - Ballistic Missile Defense System Program

CHEM DEMIL-ACWA - Chemical Demilitarization Program - Assembled Chemical Weapons Alternatives

CHEM DEMIL-CMA - Chemical Demilitarization (Chem Demil) - Chemical Materials Agency (Army Executing Agent)

Common Analytical Laboratory System - Field Confirmation - Analytical Confirmatory Set (CALS-FC-ACS)

Common Analytical Laboratory System - Field Confirmatory - Integrated System (CALS-FC-IS)

Common Analytical Laboratory System - Theater Validation - Integrated System (CALS-TV-IS)

Defense Agency Initiative (DAI)

Defense Enterprise Accounting and Management System - Increment 1 (DEAMS - Inc. 1)

Defense Medical Information Exchange (DMIX)

Defense Security Assistance Management System (DSAMS) - Block 3

DoD Healthcare Management System Modernization (DHMSM)

EDS - Explosive Destruction System

Global Command & Control System - Joint (GCCS-J)

Joint Aerial Layer Network

Joint Biological Tactical Detection System

Joint Information Environment

Joint Light Tactical Vehicle (JLTV)

Joint Operational Medicine Information Systems

Joint Regional Security Stack (JRSS)
Joint Warning and Reporting Network (JWARN)
Key Management Infrastructure (KMI) Increment 2
Long-Range Discrimination Radar
Mid-Tier Networking Vehicle Radio
milCloud
Mission Partner Environment - Information System
Multi-Functional Information Distribution System (includes integration into USAF & USN aircraft)
Next Generation Chemical Detector
Next Generation Diagnostic System Increment 1 (NGDS Inc 1)
Public Key Infrastructure (PKI) Incr 2
SOCOM Dry Combat Submersible Medium (DCSM)
Teleport, Generation III
Theater Medical Information Program - Joint (TMIP-J) Block 2

ARMY PROGRAMS

3rd Generation Improved Forward Looking Infrared (3rd Gen FLIR)
Abrams Active Protection Systems (APS)
ABRAMS TANK MODERNIZATION - Abrams Tank Modernization (M1E3)
Abrams Tank Upgrade (M1A1 SA / M1A2 SEP)
Advanced Field Artillery Tactical Data System (AFATDS) Version 7
Advanced Multi-Purpose (AMP) 120mm Tank Round
AH-64E Apache Remanufacture/New Build
Airborne and Maritime/Fixed Site Joint Tactical Radio System (AMF JTRS) Small Airborne Networking Radio (SANR)
AN/TPQ-53 Radar System (Q-53)
Armored Multipurpose Vehicle (AMPV)
Armored Truck - Heavy Dump Truck (HDT)
Armored Truck - Heavy Equipment Transporter (HET)
Armored Truck - Heavy Expanded Mobility Tactical Truck (HEMTT)
Armored Truck - M915A5 Line Hauler
Armored Truck - M939 General Purpose Truck
Armored Truck - Palletized Loading System (PLS)
Army Integrated Air & Missile Defense (AIAMD)
Army Integration of the Department of the Navy (DON) Large Aircraft Infrared Countermeasure (LAIRCM) Advanced Threat Warning (ATW) System on the AH-64E Helicopter
Army Tactical Missile System - Service Life Extension Program (ATACMS-SLEP)
Army Vertical Unmanned Aircraft System
Assured - Positioning, Navigation, & Timing (Assured - PNT)
Biometrics Enabling Capability (BEC) Increment 1
Biometrics Enabling Capability Increment 0
Black HAWK (UH-60M) - Utility Helicopter Program
Bradley Active Protection Systems (APS)
Bradley Engineering Change Proposal (ECP) and Modernization
Brownout Rotorcraft Enhancement System (BORES)
C-17 Increase Gross Weight (IGW) and reduced Formation Spacing Requirements (FSR) with T-11 parachute
Cannon Delivered Area Effects Munitions (C-DAEM) Family of Munitions
CH-47F - Cargo Helicopter
Chinook H-47 Block II
Command Post Computing Environment (CPCE)
Common Infrared Countermeasures (CIRCM)
Common Remotely Operated Weapons System III
Data Center / Cloud / Generating Force Computing Environment (DC/C/GFCE)
Department of Defense Automated Biometric Information System
Distributed Common Ground System - Army (DCGS-A)
EXCALIBUR - Family of Precision, 155mm Projectiles
Extended Range Cannon Artillery (ERCA)
Family of Small Unmanned Aircraft Systems
FBCB2 - Force XXI Battle Command Brigade and Below Program
FBCB2 - Joint Capability Release (FBCB2 - JCR)
Fixed-Wing Utility Aircraft
FMTV - Family of Medium Tactical Vehicles
Future Vertical Lift Capability Set 3 (FVL CS 3)
Gator Landmine Replacement Program (GLRP)
General Fund Enterprise Business System (GFEBS)
Global Combat Support System Army (GCSS-A)
Ground Mobility Vehicle (GMV)
Guided Multiple Launch Rocket System - Unitary (GMLRS Unitary)
Guided Multiple Launch Rocket System Alternate Warhead (GMLRS AW)
HELLFIRE Romeo
High Explosive Guided Mortar (HEGM)
High Mobility Artillery Rocket System (HIMARS)
High Mobility Multipurpose Wheeled Vehicle (HMMWV)
Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs)
Improved Turbine Engine Program (ITEP)
Indirect Fire Protection Capability Increment 2 - Intercept (IFPC Inc 2-I)
Integrated Personnel and Pay System - Army (Army IPPS) Increment 1
Integrated Personnel and Pay System - Army (IPPS-A) Increment 2
Interceptor Body Armor
Javelin Antitank Missile System - Medium
Joint Air-to-Ground Missile (JAGM)
Joint Assault Bridge (JAB)

Joint Battle Command Platform (JBC-P)

Joint Enterprise Network Manager (JENM)

Joint Tactical Radio System, Handheld, Man pack, and Small Form Fit [Leader Radio]

Joint Tactical Radio System, Handheld, Man pack, and Small Form Fit [Manpack]

Logistics Modernization Program (LMP)

Long Range Precision Fires (LRPF)

M270A1 Multiple Launch Rocket System (MLRS)

M829A4

M88A2 Heavy Equipment Recovery Combat Utility Lift Evacuation System (Hercules)

Mine Resistant Ambush Protected Vehicle Systems - including SOCOM vehicles

Mobile / Handheld Computing Environment (M/HCE)

Mobile Protected Firepower Increment 1 (MPF Inc 1)

Modernized Expanded Capacity Vehicle (MECV) - Survivability Project

Modular Handgun System (XM17/XM18)

Mounted Computing Environment (MCE)

MQ-1C Unmanned Aircraft System Gray Eagle

Near Real Time Identity Operations

Nett Warrior

One System Remote Video Terminal

Paladin/FASSV Integrated Management (PIM)

PATRIOT PAC-3 - Patriot Advanced Capability 3

Real Time / Safety Critical / Embedded Computing Environment (RT/SC/ECE)

RQ-7B SHADOW - Tactical Unmanned Aircraft System

Sensor Computing Environment (SCE)

Soldier Protection System

Spider XM7 Network Command Munition

Stryker Active Protection Systems (APS)

STRYKER ECP - STRYKER Engineering Change Proposal

Stryker M1126 Infantry Carrier Vehicle including Double V-Hull variant

Stryker M1127 Reconnaissance Vehicle

Stryker M1128 Mobile Gun System

Stryker M1129 Mortar Carrier including the Double V-Hull variant

Stryker M1130 Commander's Vehicle including the Double V-Hull Variant

Stryker M1131 Fire Support Vehicle Including the Double V-Hull Variant

Stryker M1132 Engineer Squad Vehicle Including the Double V-Hull Variant

Stryker M1133 Medical Evacuation Vehicle Including the Double V-Hull Variant

Stryker M1134 ATGM Vehicle Including the Double V-Hull Variant

Stryker M1135 NBC Reconnaissance Vehicle (NBCRV)

UH-60V Black HAWK

UH-72A Lakota Light Utility Helicopter

Warfighter Information Network - Tactical Increment 3 (WIN-T Inc 3)

WIN-T INCREMENT 1 - Warfighter Information Network - Tactical Increment 1

WIN-T INCREMENT 2 - Warfighter Information Network - Tactical Increment 2

XM1156 Precision Guidance Kit (PGK)

XM1158 7.72mm Cartridge

XM25, Counter Defilade Target Engagement (CDTE) System

NAVY PROGRAMS

Acoustic Rapid COTS Insertion for SONAR

Advanced Airborne Sensor

Advanced Arresting Gear

AEGIS Modernization (Baseline Upgrades)

AGM-88E Advanced Anti-Radiation Guided Missile

AH-1Z

AIM-9X - Air-to-Air Missile Upgrade Block II

Air and Missile Defense Radar (AMDR)

Air Warfare Ship Self Defense Enterprise

Airborne Resupply/Logistics for Seabasing

Amphibious Assault Vehicle Upgrade (AAVU)

Amphibious Combat Vehicle Phase 1 Increment 1 (ACV 1.1)

AN/APR-39 Radar Warning Receiver

AN/AQS-20X Minehunting Sonar and Tow Vehicle (all variants)

AN/SQQ-89A(V) Integrated USW Combat Systems Suite

Assault Breaching System Coastal Battlefield Reconnaissance and Analysis System (all variants)

Barracuda Mine Neutralization System

CANES - Consolidated Afloat Networks and Enterprise Services

Carrier Based Unmanned Air System

CH-53K - Heavy Lift Replacement Program

Close-In Weapon System (CIWS) including SEARAM

CMV-22 Joint Services Advanced Vertical Lift Aircraft - Osprey -- Carrier Onboard Delivery (COD)

COBRA JUDY REPLACEMENT - Ship-based radar system

Columbia Class SSBN - including all supporting PARMs

Cooperative Engagement Capability (CEC)

Countermeasure Anti-Torpedo

CVN-78 - *GERALD R. FORD* CLASS Nuclear Aircraft Carrier

DDG 1000 - *ZUMWALT* CLASS Destroyer - includes all supporting PARMs and the lethality of the LRLAP and 30mm ammunition

DDG 51 Flight III and associated PARMS

Department of Navy Large Aircraft Infrared Countermeasures Program (DON LAIRCM)

Distributed Common Ground System - Navy (DCGS-N)

E-2D Advanced Hawkeye

EA-18G - Airborne Electronic Attack

Electro-Magnetic Aircraft Launching System

Electronic Procurement System

Enhanced Combat Helmet

Enterprise Air Surveillance Radar

Evolved Sea Sparrow Missile (ESSM)

Evolved Sea Sparrow Missile Block 2

Expeditionary Transfer Dock (formerly Mobile Landing Platform (MLP) Core Capability Set (CCS) Variant) and Expeditionary Mobile Base (formerly MLP Afloat Forward Staging Base (AFSB) Variant)

F/A-18E/F - SUPER HORNET Naval Strike Fighter

Frigate Class Small Surface Combatant

Future Pay and Personnel Management Solution (FPPS)

Ground/Air Task Oriented Radar (G/ATOR)

Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs)

Infrared Search and Track System

Joint and Allied Threat Awareness System

Joint Precision Approach and Landing System

Joint Stand-Off Weapon C-1 variant (JSOW C-1)

KC-130J

LCS Surface Warfare Mission Package Surface to Surface Missile (Longbow Hellfire Missile) including its lethality

LHA 6 - *AMERICA* CLASS - Amphibious Assault Ship - includes all supporting PARMs

LHA 8 Amphibious Assault Ship (*America* Class with well deck)

Light Armored Vehicle

Light Weight Tow Torpedo Countermeasure (part of LCS ASW Mission Module)

Littoral Combat Ship (LCS) - includes all supporting PARMs, and 57mm ammunition lethality

Littoral Combat Ship Frigate modifications

Littoral Combat Ship Surface Warfare Mission Package including 30mm ammunition lethality

Littoral Combat Ship Variable Depth Sonar (part of LCS ASW Mission Package)

Logistics Vehicle System Replacement

LSD 41/49 Replacement

Mk 54 torpedo/MK - 54 VLA/MK 54 Upgrades Including High Altitude ASW Weapon Capability (HAAWC)

MK-48 CBASS Torpedo including all upgrades

Mobile User Objective System (MUOS)

MQ-4C Triton

MQ-8 Fire Scout Unmanned Aircraft System

Multi-static Active Coherent (MAC) System

MV-22 Joint Services Advanced Vertical Lift Aircraft - Osprey

Naval Integrated Fire Control - Counter Air (NIFC-CA) From the Air

Navy Enterprise Resource Planning (ERP)

Navy Multiband Terminal Program (NMT)

Next Generation Jammer - Increment ONE

Next Generation Land Attack Weapon

Offensive Anti-Surface Warfare Increment 1

Offensive Anti-Surface Warfare, Increment 2 (Air and Surface Launch)

Over The Horizon Weapon System

P-8A Poseidon Program

Rolling Airframe Missile Block 2 Program

RQ-21A Unmanned Aircraft System (UAS)

Ship Self Defense System (SSDS)

Ship to Shore Connector

Standard Missile 2 (SM-2) including all mods

Standard Missile-6 (SM-6)

Submarine Torpedo Defense System (Sub TDS) including Next Generation Countermeasure System (NGCM)

Surface Electronic Warfare Improvement Program (SEWIP) (All variants)

Surface Mine Countermeasures Unmanned Undersea Vehicle (also called Knifefish UUV) (SMCM UUV)

Tactical Tomahawk Modernization and Enhanced Tactical Tomahawk (Maritime Strike) (includes changes to planning and weapon control system)

T-AO 205 Oiler

Torpedo Warning System including all sensors and decision tools

TRIDENT II MISSILE - Sea Launched Ballistic Missile

UH-1Y

Unmanned Influence Sweep System (UISS) include Unmanned Surface Vessel (USV) and Unmanned Surface Sweep System (US3)

USMC MRAP-Cougar

USSOCOM JUONS- Navy and USAF Development/Integration of the Distributed Aperture Infrared Countermeasure System on the USAF HH-60G, Army A/MH-6, Navy MH-60S, AH-1Z, UH-1Y

VH-92A Presidential Helicopter

Virginia Class SSN (all variants)

AIR FORCE PROGRAMS

20mm PGU-28/B Replacement Combat Round

Advanced Pilot Trainer

AEHF - Advanced Extremely High Frequency (AEHF) Satellite Program

AIM-120 Advanced Medium-Range Air-to-Air Missile

Air Force Distributed Common Ground System (AF-DCGS)

Air Force Integrated Personnel and Pay System (AF-IPPS)

Air Force Mission Planning Systems Increment 5

FY17 DOT&E ACTIVITY AND OVERSIGHT

Air Force Organic Depot Maintenance, Repair, and Overhaul Initiative (MROi)

Air Operations Center - Weapon System (AOC-WS) 10.1

Air Operations Center - Weapon System (AOC-WS) 10.2

Airborne Signals Intelligence Payload (ASIP) Family of Sensors

Airborne Warning and Control System Block 40/45 Computer and Display Upgrade

B-2 Defensive Management System Modernization (DMS-M)

B-2 Extremely High Frequency (EHF) SATCOM

B-21 Long Range Strike Bomber

B-52 Radar Modernization Program (RMP)

B61 Mod 12 Life Extension Program

Battle Control System - Fixed (BCS-F) 3.2

C-130J - HERCULES Cargo Aircraft Program

Combat Rescue Helicopter (CRH)

Command and Control Air Operations Suite (C2AOS)/Command and Control Information Services (C2IS) (Follow-on to Theater Battle Management Core System, new capabilities for AOC and joint software suites)

CV-22 Joint Services Advanced Vertical Lift Aircraft - Osprey

Deliberate and Crisis Action Planning and Execution Segments (DCAPES) Inc. 2B

Enclave Control Node (ECN)

Enterprise Ground Services

EPS - Enhanced Polar System

Evolved Strategic Satellite Communications

F-15 Eagle Passive Active Warning Survivability System

F-15C Infrared Search and Track (IRST)

F-16 Radar Modernization Program

F-22 - RAPTOR Advanced Tactical Fighter

F-35 - Lightning II Joint Strike Fighter (JSF) Program

FAB-T - Family of beyond Line-of-Sight Terminals

Full Scale Aerial Target

GBS - Global Broadcast Service

Geosynchronous Space Situational Awareness Program

GPS OCX - Global Positioning Satellite Next Generation Control Segment

GPS-IIIA - Global Positioning Satellite III

Ground Based Strategic Deterrent

Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs)

Integrated Strategic Planning and Analysis Network (ISPAN) Increment 4

Joint Air-to-Surface Standoff Missile Extended Range

Joint Space Operations Center Mission System (JMS)

Joint Surveillance Target Attack Radar System (JSTARS) Recapitalization (Recap)

KC-46 - Tanker Replacement Program

Long Range Stand Off (LRSO) Weapon

Massive Ordnance Penetrator (MOP)

Military GPS User Equipment (GPS MGUE)

MQ-9 REAPER - Unmanned Aircraft System

NAVSTAR Global Positioning System (GPS) (Includes Satellites, Control and User Equipment)

Nuclear Planning and Execution System

Presidential Aircraft Recapitalization

Presidential National Voice Conferencing

Protected Tactical Enterprise Service

Protected Tactical Satellite Communications (SATCOM)

RQ-4A/B Global Hawk Unmanned Aircraft System

SBIRS HIGH - Space-Based Infrared System Program, High Component

SBSS B10 Follow-on - Space-Based Space Surveillance Block 10 Follow-on

SF - Space Fence

Small Diameter Bomb, Increment II

Three-Dimensional Expeditionary Long-Range Radar (3DELRR)

UH-1N Replacement

Weather Satellite Follow-on (WSF)

Wide Area Surveillance (WAS) Program

Problem Discovery Affecting OT&E

In 2011, Congress expressed concern that acquisition programs are discovering significant performance problems during operational testing that should have been discovered during developmental testing. Congress also expressed concern that programs were entering operational testing with known performance problems that previously should have been corrected. Since 2011, DOT&E annual reports have documented programs that either (1) have observed performance shortfalls during operational testing or (2) may soon begin operational testing with known performance problems that could affect the evaluation of their effectiveness, suitability, or survivability. This year, as in previous years, examples of both categories are present.

Operational testing identifies significant system performance problems, which provides opportunities for correction before systems are fielded or deployed.[1] In many cases, an operational environment or user is necessary to uncover the problem. However, performance shortfalls that can be discovered in developmental testing should more appropriately be resolved prior to operational testing. Resolving system performance problems before operational testing reduces the cost and schedule impact to the program if retesting is required and enables an accurate evaluation of the operational capabilities of the system under test in its final configuration. It is also a benefit to discover problems when the prime contractor is more accountable than the government to correct them, such as before certain contractual decisions.

The following discussion provides a summary of the significant problems discovered or observed in analyses of operational test events conducted or reported in FY17. Detailed accounts of the problems are in the individual program articles in this report. Twenty-nine programs have discovered significant problems during early testing of systems that have a scheduled operational test in the next two fiscal years. If left uncorrected, these problems could negatively affect my evaluation of operational effectiveness, suitability, or survivability.

Figure 1 shows the breakdown of problem discoveries in FY17. This year's Annual Report includes 92 programs on the DOT&E oversight list with 114 operational tests conducted, reported, or planned between FY17 and FY19. Of those, 56 programs had a total of 64 operational tests or DOT&E reports issued in FY17. It is noteworthy that over 40 percent (27/64) of the operational tests did not observe significant problems. Of the 37 operational tests with problems significant enough to adversely affect my evaluation of the system, over one-third (15/37) observed previously known problems; less than one-third (10/37) observed newly discovered problems; and approximately one-third (12/37) observed both known and new problems.

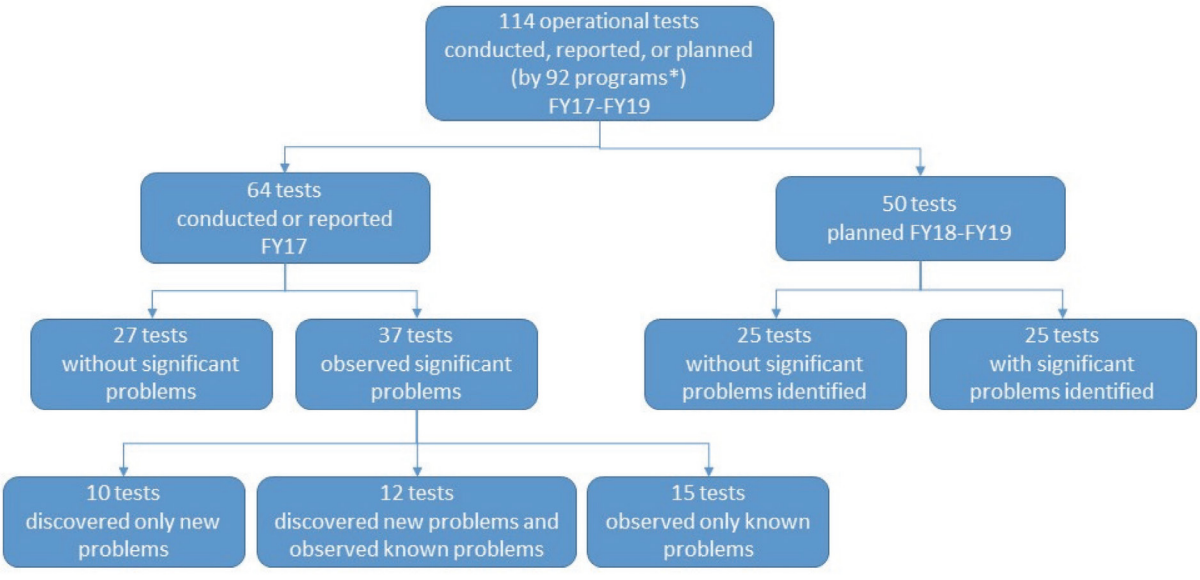


FIGURE 1. PROGRAMS UNDER OVERSIGHT WITH OPERATIONAL TESTS IN FY17-FY19
(Note: The number of tests is not the same as the number of programs because multiple programs have more than one operational test reported, conducted, or scheduled in FY17-FY19 and some operational tests feature multiple programs.).

[1] DOT&E Briefing, "The Value of Operational Testing and Evaluation," March 2016.

The 37 tests with significant problems experienced 102 distinct problems across the 3 operational evaluation categories of effectiveness, suitability, and survivability. Approximately 70 percent of the problems (72/102) were known before operational testing. Figure 2 shows the distribution of the significant problems found during operational testing by area and whether the problem was known prior to the operational test.

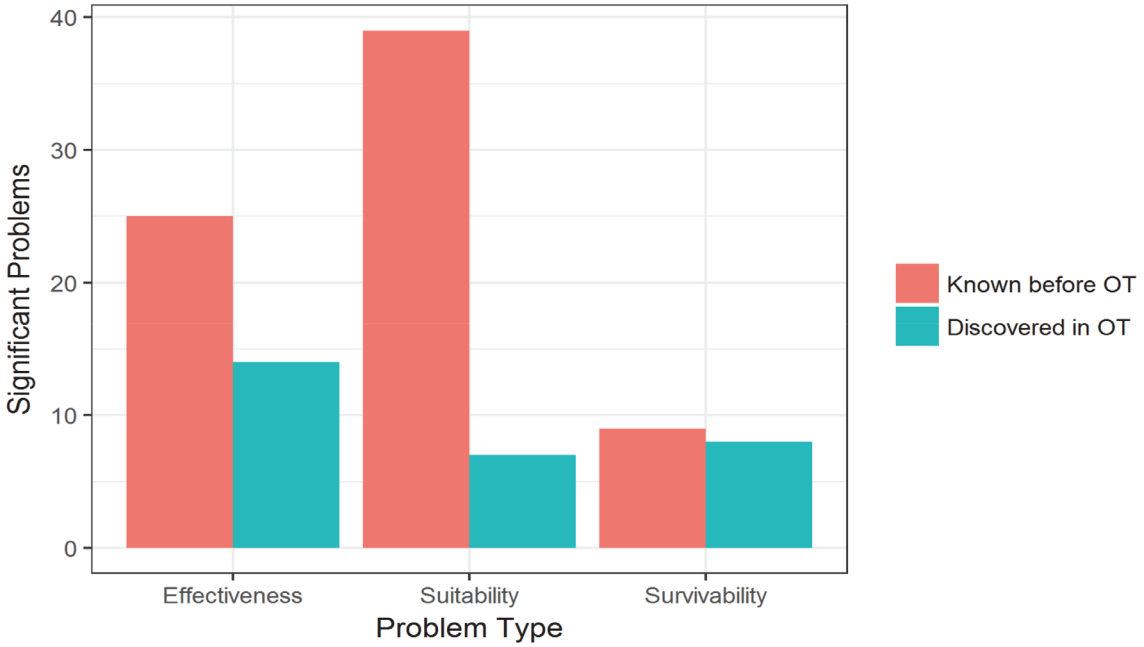


FIGURE 2. BREAKDOWN OF PROBLEMS BY TYPE AND WHETHER THEY WERE KNOWN PRIOR TO OPERATIONAL TESTING

As in previous years, it was common this year to find programs that either began operational testing with known problems or delayed testing due to a lack of allocated time or funding to fix problems that were discovered prior to the operational test. Approximately 40 percent (26/64) of operational tests began with known problems that adversely affected the system evaluation. In previous analyses of the reasons behind program delays, my office has reported that programs are commonly delayed by problems discovered in developmental or operational testing.[2] When programs are driven by a rigid schedule and the assumption that no major problems will be discovered during testing, they often run into delays and cost overruns when those schedules are adjusted to accommodate unforeseen additional development. For example, the Joint Regional Security Stack (JRSS) IOT&E was delayed in part because the Services and Defense Information Systems Agency did not have sufficient time to mitigate survivability problems that were discovered during a previous operational assessment. On the other hand, the APR-39 Radar Warning Receiver program displayed a significant reliability shortfall that was known from earlier integrated testing because it proceeded without delay into an operational assessment and an FOT&E. The Program Office had chosen not to update the software between test periods so as not to invalidate the data from earlier test phases because it did not plan time or funding for any necessary post-fix regression testing.

In some cases, the Program Office identified a fix for the problem but did not plan for the time or funding to finish implementing it. For example, the Assault Amphibious Vehicle Survivability Upgrade (AAV-SU) program entered an operational assessment with known reliability problems: the mean time between operational mission failures was below the requirement. Despite knowing these limitations, the Program Office decided to continue with the test so that a low-rate initial production decision could be made before a fiscal year deadline. Limited funding rather than time allowed known reliability problems to persist during the Spider Increment 1A Limited User Test. The Program Office chose not to make necessary software changes until after the IOT&E due to lack of funding.

Some problems can only be discovered during operational testing because they are revealed only by the system's interaction with representative users and/or operationally realistic environments, which can include final operational configurations. For example, the Defense Agencies Initiative (DAI) program discovered suitability shortfalls when operational testing found that most agencies are experiencing additional staffing requirements for their own Tier 1 help-desk support. This problem was discovered only through discussions with DAI users at various defense agencies. Similarly, the DOD Healthcare Management System Modernization program's operational assessment revealed suitability problems with the system usability, due in part to inadequate training and outdated system manuals provided to end users. Troop egress problems in the AAV-SU were only discovered when the vehicles were fully loaded with troops in combat gear. Additionally, the Standard Missile-6 program was only able to discover problems with the seeker when up against operationally representative targets.

Cybersecurity problems often require operational configurations, users, and environments to be discovered. Thirteen of 17 survivability problems observed or reported this year are related to cybersecurity, 9 of which were discovered in operational testing. Specific problems will not be addressed in this

[2] IDA Briefing, "Reasons behind Program Delays – 2017 Update."

unclassified report. In general, some cybersecurity problems are only found under realistic threat activity, such as that emulated in a Cooperative Vulnerability and Penetration Assessment and an Adversarial Assessment. In other cases, cybersecurity vulnerabilities emerge as the system software evolves through successive upgrades.

Although operational testing often provides the necessary conditions to discover problems, these conditions can also be used during developmental testing to promote earlier problem discovery, when it is less disruptive to a program to fix them. Developmental and integrated testing, when conducted under operationally relevant conditions to collect early operational data, provide an opportunity for early problem identification. For example, the Common Analytical Laboratory System – Field Confirmatory – Analytical Capability Set man-portable subsystem DT/OT tested the commercial off-the-shelf chemical identification instruments in high humidity and cold temperature conditions. The test revealed that one of the instruments could not reliably operate in the test conditions. This discovery prompted changes in guidelines for use of the system in these environmental conditions prior to IOT&E. On the other hand, the M109 Family of Vehicles Paladin Integrated Management program had to suspend IOT&E due to suspected safety issues when cannon breech and bore evacuator problems, along with inadequate maintenance training, appeared to expose crew members to excessive amounts of toxic fumes from the explosive propellant. Developmental testing of the Paladin did not employ operationally realistic firing sequences with rates of fire and frequency using Modular Artillery Charge System charge 5H propellant increments.

Figure 3 breaks down the number of significant problems observed per operational test by each of the Services and other DOD agencies, including the 27 of 64 operational tests with no problems. These histograms show that, in general, the Services experience similar trends in observing only a few problems during a given operational test, with very few outliers that are labeled in the figure.

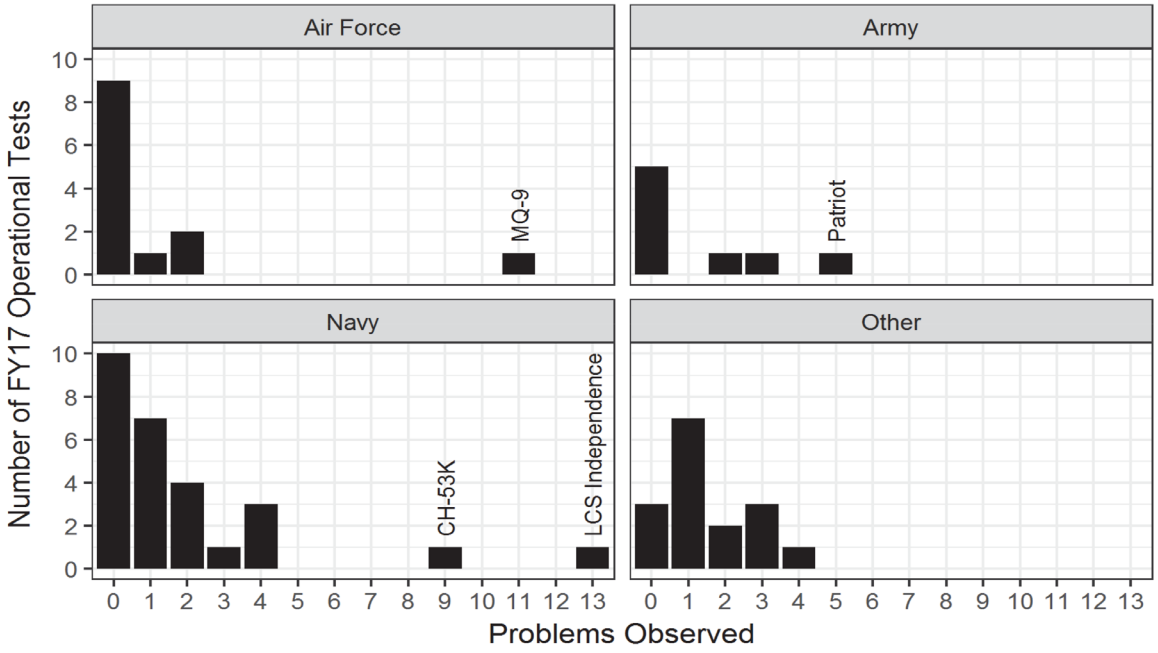


FIGURE 3. HISTOGRAM OF NUMBER OF PROBLEMS OBSERVED IN EACH OPERATIONAL TEST, BY SERVICE.

(Note: "Other" includes non-service branch DOD agencies such as U.S. Special Operations Command, Defense Information Systems Agency, or the Missile Defense Agency.)

Tables 1 and 2 list the 64 operational tests discussed in this year's Annual Report. Table 1 lists the 27 operational tests that had no significant problems to report. Table 2 lists the 37 operational tests discussed in this year's Annual Report that observed significant problems. Each row provides the name of the system and operational test and indicates which categories of problems were observed. For details on the problems observed, see each system's entry elsewhere in this report.

TABLE 1. OPERATIONAL TESTS IN FY17 WITH NO SIGNIFICANT PROBLEM DISCOVERY*

System Name	OT Name
AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM) (pg. 235)	AIM-120C7 Tape 1 Initial Operational Test and Evaluation (IOT&E)
AMRAAM	AIM-120C7 Tape 2 IOT&E
Air Force Mission Planning Systems Increment 5 (MPS-5) (pg. 267)	Mobility Air Force Automated Flight Planning Service (MAFPS) IOT&E
Air Force MPS-5	MPS-5 C-17 IOT&E
Army Integration of the Department of the Navy (DON) Large Aircraft Infrared Countermeasures (LAIRCM) Advanced Threat Warner (ATW) system on the AH-64E, CH-47F, HH/UH-60M, and UH-60L (pg. 97)	DON LAIRCM ATW Integration on AH-64E
Battle Command System - Fixed (BCS-F) 3.2 (pg. 243)	BCS-F R3.2.4 Force Development Evaluation (FDE)
Common Analytical Laboratory System – Field Confirmatory – Analytical Capability Set (CALS-FC-ACS) (pg. 19)	CALS-FC-ACS User Demonstration
Cooperative Engagement Capability (pg. 165)	Aegis B/L 9.C Combat System Follow-on Operational Test and Evaluation (FOT&E)
Defense Enterprise Accounting and Management System (DEAMS) Increment 1 (pg. 245)	DEAMS Inc 1 Operational Utility Evaluation (OUE)
DOD Healthcare Management System Modernization (DHMSM) (pg. 27)	DHMSM IOT&E
F-22A - RAPTOR Modernization (pg. 247)	F-22A Increment 3.2B IOT&E
Ground/Air Task Oriented Radar (G/ATOR) (pg. 179)	G/ATOR Block 1 and 2 Early Fielding Assessment
Javelin Close Combat Missile System - Medium (pg. 105)	Javelin Spiral 2 Missile Live Fire Test and Evaluation (LFT&E)
Massive Ordnance Penetrator (MOP) (pg. 263)	Enhanced Threat Response (ETR)-IV
Miniature Air Launched Decoy - Jammer (pg. 265)	MALD-J FDE
Modular Handgun System (XM17/XM18) (pg. 133)	Modular Handgun System IOT&E
Navy Multiband Terminal (NMT) (pg. 201)	NMT FOT&E
Next Generation Diagnostic System Increment 1 (pg. 79)	Next Generation Diagnostic System IOT&E
Offensive Anti-Surface Warfare (OASuW) Increment 1 (pg. 203)	Long Range Anti-Ship Missile (LRASM) Quick Reaction Assessment (QRA)
P-8A Poseidon (pg. 205)	P-8A Engineering Change Proposal (ECP) 2 OT&E
Rolling Airframe Missile (RAM) Block 2 (pg. 209)	RAM Block 2 IOT&E
Ship Self-Defense for LSD 41/49 Class (pg. 215)	Ship Self-Defense System MK 2 Mod 5 FOT&E
Soldier Protection System (pg. 121)	Integrated Head Protection System (IHPS) Limited User Test
SSN 774 *Virginia*-Class Submarine (pg 217)	SSN 774 *Virginia*-Class Submarine Block III FOT&E
Standard Missile-6 (SM-6) (pg. 219)	SM-6 Block IA FOT&E
Surface Ship Torpedo Defense (SSTD) System: Torpedo Warning System (TWS) (pg. 223)	TWS/Countermeasure Anti-Torpedo (CAT) QRA
Warfighter Information Network - Tactical (WIN-T) (pg. 129)	WIN-T Increment 2 Tactical Communications Node – Lite (TCN-L) and Network Operations Security Center - Lite (NOSC-L) FOT&E

* Note: Several systems listed in Table 1 are currently in test. Their inclusion here indicates that no major problems have been discovered at the time of this report. Future DOT&E reports will update this assessment.

TABLE 2. OPERATIONAL TESTS IN FY17 WITH DISCOVERY OF SIGNIFICANT PROBLEMS				
System Name	**Operational Test**	**Effectiveness**	**Suitability**	**Survivability**
AC-130J Ghostrider (pg. 231)	AC-130J Block 20 Initial Operational Test and Evaluation (IOT&E)	X	X	
Aegis Modernization (pg. 139)	Aegis Baseline Upgrade Operational Test (OT)	X		X
Air Force Distributed Common Ground System (AF DCGS) (pg. 237)	3 different OT events			X
AGM-88E Advanced Anti-Radiation Guided Missile (AARGM) (pg. 143)	AGM-88 AARGM Block 1 Follow-on Operational Test and Evaluation (FOT&E)	X	X	
AN/APR-39D(V)2 Radar Signal Detection Set (RSDS) (pg. 147)	APR -39 Radar Warning Receiver FOT&E		X	
AN/BLQ-10 (pg. 149)	AN/BLQ-10 (Technical Insertion (TI)-10) FOT&E	X		
AN/BQQ-10 Acoustic Rapid Commercial Off-the-Shelf Insertion(A-RCI) Sonar (pg. 137)	A-RCI Advanced Processing Build 2013 (APB-13) variant FOT&E			X
AN/SQQ-89A(V)15 Integrated Undersea Warfare (USW) Combat System Suite (pg. 151)	AN/SQQ-89A(V)15 Advanced Capability Build 2011 (ACB-11) variant FOT&E	X		
Air Operations Center – Weapon System (AOC-WS) Initiatives 10.0 & 10.1 (pg. 239)	AOC-WS 10.1.13.3 assessment	X		X
AOC-WS Initiatives 10.0 & 10.1	AOC-WS 10.1.14E assessment	X		X
Assault Amphibious Vehicle - Survivability Upgrade (AAV-SU) (pg. 153)	AAV-SU Operational Assessment (OA)		X	
CH-53K - Heavy Lift Replacement Program (pg. 157)	CH-53K OA	X	X	X
Coastal Battlefield Reconnaissance and Analysis (COBRA) System (all variants) (pg. 161)	COBRA Block I IOT&E Test Period One	X		
Common Analytical Laboratory System – Field Confirmatory – Analytical Capability Set (CALS-FC-ACS) (pg. 19)	CALS-FC-ACS Man-portable chemical subsystem DT/OT	X	X	
Consolidated Afloat Networks and Enterprise Services (CANES) (pg. 163)	CANES Force-level variant FOT&E			X
CVN-78 *Gerald R. Ford* Class Nuclear Aircraft Carrier (pg. 167)	OT-B4 OA	X	X	
Defense Agencies Initiative (DAI) (pg. 21)	DAI IOT&E		X	
Defense Medical Information Exchange (DMIX) (pg. 25)	DMIX Cybersecurity Assessment and DHMSM IOT&E			X
DOD Healthcare Management System Modernization (DHMSM) (pg. 27)	DHMSM OA	X	X	
Global Command and Control System - Joint (GCCS-J) (pg. 61)	Joint Operation Planning and Execution System (JOPES) v4.2.0.3 Maintenance Release (MR) 4 OT	X		
Integrated Defensive Electronic Countermeasures (IDECM) (pg. 181)	IDECM Block 4/Software Improvement Program (SWIP) OA	X		
Joint Regional Security Stack (JRSS) (pg. 69)	JRSS IOT&E	X		
Key Management Infrastructure (KMI) Increment 2 (pg. 73)	KMI Spiral 2 Spin 2 Limited User Test (LUT)		X	
KMI Increment 2	KMI Spiral 2 Spin 2 OA		X	
LHA 6 (pg. 183)	LHA 6 IOT&E			X
Littoral Combat Ship (LCS) Seaframes, *Independence* Variant (pg. 187)	OT-C4 *Independence* variant with Increment 2 Surface Warfare (SUW) mission package	X	X	X
LCS SUW Mission Package (pg. 187)	OT-C4 *Independence* variant with Increment 2 SUW mission package	X	X	
M109A7 Paladin Integrated Management (PIM) (pg. 113)	PIM IOT&E 1	X	X	
MQ-9 Reaper Unmanned Aircraft System (pg. 269)	MQ-9 Block 5 Remotely Piloted Aircraft (RPA) Block 30 Ground Control System (GCS) FOT&E	X	X	X
Next Generation Chemical Detector (NGCD) (pg. 77)	NGCD Early OA		X	
Patriot Advanced Capability-3 (PAC-3) (pg. 119)	Post-Deployment Build-8 (PDB-8) IOT&E	X	X	X
Public Key Infrastructure (PKI) Increment 2 (pg. 81)	PKI Spiral 3 FOT&E	X	X	
PKI Increment 2	PKI Inc. 2 Token Management System (TMS) Release 4 LUT	X	X	X
Ship Self-Defense for LHA 6 (pg. 211)	Ship Self-Defense System FOT&E MK 2 Mod 4 OT-IIIH	X	X	
Spider XM7 Network Command Munition (pg. 123)	Spider Increment 1A LUT	X	X	X
Standard Missile-6 (SM-6) (pg. 219)	SM-6 Block I Verification of Correction of Deficiencies	X		
Terminal High-Altitude Area Defense (THAAD) (pg. 297)	Flight Test THAAD (FTT)-18		X	

There are 57 programs that have 50 operational tests (including joint testing of multiple programs) scheduled to begin in the next two fiscal years, and I am aware of significant problems that, if not corrected, could adversely affect my evaluation of the effectiveness, suitability, or survivability of 29 of these systems in 25 of the tests. Table 3 lists the upcoming operational tests for systems discussed in this year's Annual Report with identified problems (see individual system write-ups in this report for details on the problems).

TABLE 3. PROGRAMS IN FY17 ANNUAL REPORT WITH PROBLEMS THAT MAY ADVERSELY AFFECT UPCOMING OPERATIONAL TESTING

System Name	Upcoming Test	Effectiveness	Suitability	Survivability
Aegis Ballistic Missile Defense (Aegis BMD) (pg. 291)	Flight Test Operational (FTO)-03 Event 1		X	
Aegis Modernization Program (pg. 139)	Advanced Capability Build (ACB)-16 Phase 0 Operational Test (OT)	X		
Air Force Distributed Common Ground System (AF DCGS) (pg. 237)	AF DCGS Operational Utility Evaluation (OUE)			X
AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM) (pg. 235)	AIM-120D System Improvement Program (SIP)-2 Initial Operational Test and Evaluation (IOT&E)	X		
AN/SQQ-89A(V)15 Integrated Undersea Warfare (USW) Combat System Suite (pg. 151)	AN/SQQ-89A(V)15 Advanced Capability Build 2013 (ACB-13) variant Follow-on Operational Test and Evaluation (FOT&E)	X		
Air Operations Center – Weapon System (AOC-WS) Initiatives 10.0 & 10.1 (pg. 239)	AOC-WS 10.1.15 assessment			X
Assault Amphibious Vehicle - Survivability Upgrade (AAV-SU) (pg. 153)	AAV-SU IOT&E		X	
Ballistic Missile Defense System (BMDS) (pg. 279)	FTO-03 Event 2	X	X	
BMDS Sensors/Command and Control Architecture (pg. 283)	FTO-03 Event 2		X	
Bradley Family of Vehicles (BFoV) Engineering Change Proposal (ECP) (pg. 101)	Abrams-Bradley FOT&E		X	
CH-53K - Heavy Lift Replacement Program (pg. 157)	CH-53K IOT&E	X	X	X
Defense Agencies Initiative (DAI) (pg. 21)	DAI Increment 2 FOT&E		X	
F-35 Joint Strike Fighter (JSF) (pg. 31)	F-35 IOT&E	X	X	
Ground-based Missile Defense (GMD) (pg. 287)	Flight Test, Ground-based Interceptor (FTG)-11	X		
Joint Space Operations Center Mission System (JMS) (pg. 255)	JMS Increment 2, Service Pack 9 and 11 OUE	X		
Joint Regional Security Stack (JRSS) (pg. 69)	JRSS Version 2.0 IOT&E	X		
KC-46A (pg. 259)	KC-46A IOT&E	X		
Key Management Infrastructure (KMI) Increment 2 (pg. 73)	KMI Increment 2 FOT&E	X	X	
LCS Anti-Submarine Warfare (ASW) Mission Package to include all associated vehicles, communications, sensors, weapon systems, support equipment, software, crew detachments, and support aircraft that are in development (pg. 187)	ASW Mission Package IOT&E		X	
M109A7 Paladin Integrated Management (PIM) (pg. 113)	PIM IOT&E 2	X	X	
MK 54 Lightweight Torpedo and Its Upgrades including High-Altitude Anti-Submarine Warfare Capability (pg. 195)	MK 54 Mod 1 FOT&E	X		
Modular Handgun System (XM17/XM18) (pg. 133)	Modular Handgun FOT&E		X	
Patriot Advanced Capability-3 (PAC-3) (pg. 119)	FTO-03 Event 2	X	X	X
Public Key Infrastructure (PKI) Increment 2 (pg. 81)	PKI Increment 2 FOT&E	X	X	
RQ-4B Global Hawk (pg. 273)	RQ-4B Global Hawk MS-177 OUE	X		
Spider XM7 Network Command Munition (pg. 123)	Spider Increment 1A IOT&E		X	
Surface Ship Torpedo Defense (SSTD) System: Countermeasure Anti-Torpedo (CAT) (pg. 223)	TWS/CAT Quick Reaction Assessment (QRA)	X	X	
Surface Ship Torpedo Defense (SSTD) System: Torpedo Warning System (TWS) (pg. 223)	TWS/CAT QRA	X	X	
Terminal High-Altitude Area Defense (THAAD) (pg. 297)	FTO-03 Event 2	X	X	X

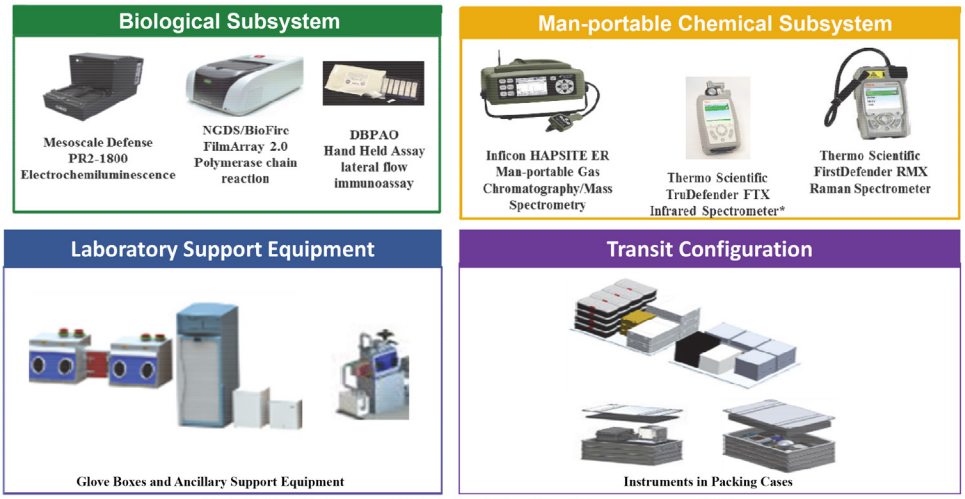
DOD Programs

DOD Programs

Common Analytical Laboratory System - Field Confirmatory - Analytical Capability Set (CALS-FC-ACS)

Executive Summary

- The Common Analytical Laboratory System – Field Confirmatory – Analytical Capability Set (CALS-FC-ACS) consists of commercial and government off-the-shelf equipment to provide analysis of environmental samples to identify the presence of chemical and biological threats.
- The Army Test and Evaluation Command (ATEC) conducted a user demonstration and combined developmental/operational testing during FY17.
- The CALS-FC-ACS analytical instruments have the capability to identify some of the required chemical and biological threats in environmental samples to support operational decision-making.
- The most capable chemical analysis instrument was not able to reliably operate in cold and hot humid conditions during chemical chamber testing.



DBPAO - Defense Biological Product Assurance Office
NGDS - Next Generation Diagnostic System

System

- The CALS-FC-ACS is one of three variants of CALS. The CALS-FC-ACS is composed of commercial and government off-the-shelf equipment to provide analysis of environmental samples (e.g., air, soil, water) to identify chemical and biological hazards.
- The CALS-FC-ACS is composed of a biological subsystem, a man-portable chemical subsystem, laboratory support equipment, analytical workflows, an instrument control computer with information management software, external disc data storage, a printer, and protective cases for transit.
- The biological subsystem consists of the Next Generation Diagnostic System FilmArray 2.0, Mesoscale Defense PR2-1800, and the Defense Biological Product Assurance Office Hand Held Assay. The chemical subsystem consists of the Inficon HAPSITE ER, Thermo Scientific TruDefender FTX, and the Thermo Scientific FirstDefender RMX spectrometer; laboratory sample preparation equipment; two class III gloveboxes; an uninterruptible power supply; and power distribution unit.

Mission

Commanders use Army, Navy, Air Force, and National Guard Bureau's Civil Support Team field analytic units equipped with the CALS-FC-ACS to analyze environmental samples, identify chemical and biological hazards, and report the results to support force protection and health surveillance decisions.

Major Contractor

Battelle Memorial Institute – Columbus, Ohio

Activity

- ATEC's West Desert Test Center conducted a combined developmental/operational test of the ACS man-portable chemical subsystem agent from July 11 to October 2, 2017, at Dugway Proving Ground, Utah. DOT&E approved several deviations to the test plan due to the inability of some of the equipment to function in certain environmental conditions. This test event was conducted to support the Full-Rate Production decision planned for FY19.
- The Army Research Laboratory, Survivability/Lethality Analysis Directorate conducted a cybersecurity Cooperative Vulnerability and Penetration Assessment of the CALS-FC-ACS from October 3-7, 2016, in conjunction with the operational assessment at the Edgewood Chemical and Biological Center, Maryland.
- ATEC conducted a user demonstration of the CALS-FC-ACS from October 13-17, 2016, at the Edgewood Chemical and Biological Center. The test was conducted in accordance with the DOT&E-approved test plan.

Assessment

- The CALS-FC-ACS has the capability to identify some of the required chemical warfare agents, precursor chemicals and breakdown products in environmental samples at operationally representative concentrations.
- During the combined developmental/operational test of the man-portable subsystem, the most capable of the chemical analysis instruments experienced numerous failures in cold and hot humid conditions during chemical chamber testing.
- Cybersecurity testing identified numerous, significant cybersecurity vulnerabilities in the CALS-FC-ACS commercial off-the-shelf instruments.
- During the user demonstration, units were able to employ the system to accurately identify chemical targets in 77 percent and biological targets in 85 percent of environmental samples that the systems had the capability to identify.

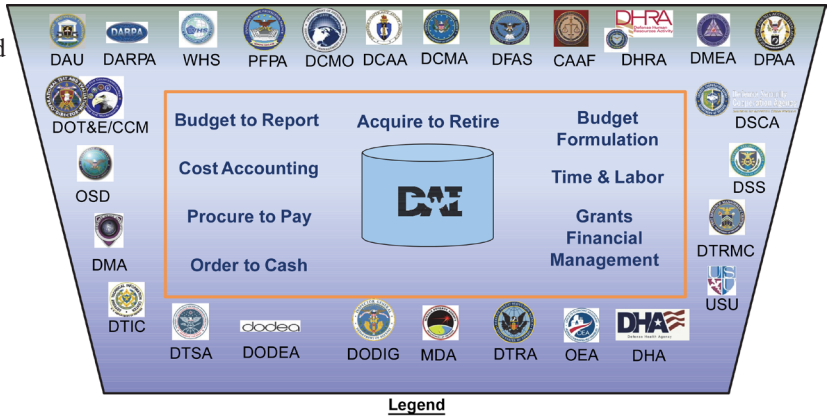
Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendations. The Program Office should:
  1. Identify the capabilities and limitations of the analytical instruments in user training materials.
  2. Conduct additional developmental testing to characterize the environmental conditions in which the analytical instruments are able to properly function to inform tactics, techniques, and procedures.
  3. Address the cybersecurity vulnerabilities to ensure the integrity of the analytical results.

Defense Agencies Initiative (DAI)

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted IOT&E of Defense Agencies Initiative (DAI) Increment 2 from March 6 through April 7, 2017.
  - During the IOT&E, JITC evaluated new and existing capabilities implemented by DAI-equipped defense agencies, DOD field activities, and other defense organizations (collectively referred to here as Agencies).
  - JITC also evaluated new functionality for Agencies that recently migrated to DAI (Defense Security Cooperation Agency, DOD Inspector General, Defense Human Resources Activity, and DOT&E).
- DAI is operationally effective and operationally suitable, and has made improvements compared to previous test and evaluation events.
  - During this IOT&E and the previous operational assessments (OAs), DAI successfully completed 99 percent of the users' critical tasks in seven business process areas.
  - During this IOT&E, DAI demonstrated improved operational reliability and availability as compared to the previous OAs; however, the system continues to require improvements in usability.
  - Help desk metrics indicate the DAI system is sustainable. However, most Agencies provide additional funding to sustain Tier 1 (local) help desk support, training, and support for new capability development, which masks the true cost of DAI sustainment for the DOD enterprise.
- JITC and the Defense Information Systems Agency (DISA) Risk Management Executive Red Team conducted a Cooperative Vulnerability and Penetration Assessment (CVPA), an Adversarial Assessment, and a Cyber Economic Vulnerability Assessment (CEVA) from March 6 to May 19, 2017, to test the cybersecurity of DAI.
  - DAI is secure from an outsider cyber threat having limited capabilities; however, DAI is vulnerable to an insider cyber threat operating with limited to moderate capabilities.
  - Program defenders failed to detect and react to Red Team activities.
- DAI's continuity of operations (COOP) tabletop exercise in 2017 verified that the alternate site could restore partial mission or business processes. The ability of the alternate site to provide required performance levels under load and then restore full capability to the primary site remains unknown until DAI conducts a full COOP event.



Legend

CAAF - Court of Appeals for the Armed Forces
DAI - Defense Agencies Initiative
DARPA - Defense Advanced Research Projects Agency
DAU - Defense Acquisition University
DCAA - Defense Contract Audit Agency
DCMA - Defense Contract Management Agency
DCMO - Deputy Chief Management Officer
DFAS - Defense Finance and Accounting Service
DHA - Defense Health Agency
DHRA - Defense Human Resources Activity
DMA - Defense Media Activity
DMEA - Defense Microelectronics Activity
DODEA - Department of Defense Education Activity
DODIG - Department of Defense Inspector General
DOT&E/CCM - Director, Operational Test & Evaluation including Center for Countermeasures (CCM)
DPAA - Defense Prisoner of War/Missing In Action Accounting Agency
DSCA - Defense Security Cooperation Agency
DSS - Defense Security Service
DTIC - Defense Technical Information Center
DTRA - Defense Threat Reduction Agency
DTRMC - Defense Test Resource Management Center
DTSA - Defense Technology Security Administration
MDA - Missile Defense Agency
OEA - Office of Economic Adjustment
OSD - Office of the Secretary of Defense
PFPA - Pentagon Force Protection Agency
USU - Uniformed Services University of the Health Sciences
WHS - Washington Headquarters Services

System

- DAI is an integrated financial management solution that provides a real-time, web-based system of integrated business processes used by defense financial managers, program managers, auditors, and the Defense Finance and Accounting Service. The DAI core functionality is based on the Oracle E-Business Suite (currently release 12.2.5), which is a commercially available enterprise solutions system.
- DAI subsumes many systems and standardizes business processes for multiple DOD Agencies. It modernizes these processes by streamlining management capabilities to address financial reporting material weaknesses, and support financial statement auditability.
- DISA provides facilities, network infrastructure, and the hardware operating system for DAI servers at its Ogden, Utah, and Columbus, Ohio, Defense Enterprise Computing Centers.
- Agencies employ DAI worldwide and across a variety of operational environments via a web portal on the Non-classified Internet Protocol Router Network using each Agency's existing information system infrastructure.
- DAI includes two software increments with a third in planning for future fielding:
  - Increment 2 replaced Increment 1 and has four software releases, each adding capabilities and deploying to additional Agencies. With the completion of Increment 2 Release 4 fielding in October 2017, DAI provides services to 22 Agencies with 39,342 users at 1,148 locations worldwide.
  - The DAI Program Management Office (PMO) is planning for Increment 3 to provide additional capabilities

to existing Agencies and to add DISA, the Defense Commissary Agency, and potentially other Agencies from FY19 through FY23.
- DAI supports financial management requirements in the Federal Financial Management Improvement Act and DOD Business Enterprise Architecture and is a key tool for helping DOD Agencies have their financial statements validated as ready for audit.

Mission

Financial Managers in defense agencies use DAI to transform their budget, finance, and accounting operations to achieve accurate and reliable financial information in support of financial accountability and effective and efficient decision-making.

Major Contractors
- CACI Arlington – Arlington, Virginia
- International Business Machines – Armonk, New York
- Northrop Grumman – Falls Church, Virginia

Activity
- The DAI PMO conducted six developmental test events in FY17:
  - DAI Increment 2 Release 3.1
    - Development integration test from December 16, 2016, through March 3, 2017
    - System integration test from March 13 through April 7, 2017
    - User acceptance test from May 8 through June 2, 2017
  - DAI Increment 2 Release 4
    - Development integration test from March 29 through June 21, 2017
    - System integration test from June 22 through July 28, 2017
    - User acceptance test from August 3 through September 8, 2017
- In coordination with DISA, the DAI PMO conducted its annual COOP tabletop exercise on January 26, 2017. Neither JITC nor DOT&E were invited by the DAI PMO to observe the event, so DAI's COOP capability remains unassessed by DOT&E.
- From March 6 through April 7, 2017, JITC conducted an IOT&E of DAI Increment 2, in accordance with a DOT&E-approved test plan.
- From March 6 through May 19, 2017, JITC and the DISA Risk Management Executive Red Team completed a CVPA, an Adversarial Assessment, and a CEVA to test the cybersecurity of DAI. The DAI PMO deferred the data fraud analysis portion of the CEVA until Increment 3 testing.
- On June 29, 2017, the USD(AT&L) signed an Acquisition Decision Memorandum establishing DAI Increment 3 and authorizing the PMO to conduct analysis activities in preparation for an Authority to Proceed decision review.
- DOT&E published its "Defense Agencies Initiative Increment 2" IOT&E report in September 2017.
- Based on DOT&E recommendations and emerging results of the IOT&E, the DAI PMO created a dedicated "Customer Liaison" relationship with each Agency. The goal of the relationship is to provide greater focus on particular problem areas within each Agency, with the overall objective of reducing Tier 2 help desk tickets (i.e., Tier 2 tickets are incidents that require support from technicians with great technical knowledge of DAI and the Tier 2 help desk is staffed by technicians who have troubleshooting capabilities beyond the Tier 1 support at the Agencies).
- JITC and the DAI PMO are planning an FOT&E and a cybersecurity test during 2Q-3QFY18. The FOT&E will focus on new Agencies (high-priority Measures of Performance only), new functionality, and those Measures of Performance that were not tested or that were inconclusive at the end of IOT&E. The cybersecurity testing will consist of a validation of corrected findings from IOT&E, Adversarial Assessment, and COOP.
- On October 3, 2017, the USD(AT&L) signed the DAI Increment 2 and 3 Acquisition Decision Memorandum (ADM). The memorandum authorized the full deployment of DAI Increment 2 and development activities for DAI Increment 3.

Assessment
- DAI is operationally effective and has made significant improvements compared to previous test and evaluation events.
  - During the Increment 2 IOT&E and previous two OAs combined, DAI successfully completed 2,054 of 2,073 critical tasks (99 percent). The 19 unsuccessful tasks include hardware, software, or system errors that the PMO has corrected, and user errors that better training and user documentation could address.
  - Two system failures occurred over a 6-month period from November 2016 to April 2017 and the mean time between system failures was 2,004 hours. The mean time to repair the two system failures was 2.05 hours, and operational availability was 93 percent. Ten scheduled maintenance periods, averaging 30.2 hours, affected operational availability. Inherent system availability, which does not include scheduled downtime, was 99 percent, meeting system requirements.
  - The DAI PMO has a goal of one 27-hour maintenance period completed during one weekend per month.

Achieving that goal would improve operational availability to 96 percent. This would better support worldwide operations and improve weekend operations during peak periods, especially during the critical closeout period near the end of the fiscal year.

- DAI is operationally suitable; however, the program has not made gains in operational suitability that would correspond with those realized in operational effectiveness.
  - The DAI Increment 2 Business Case defines the High Level Outcomes (HLOs), which quantitatively establish the value added by DAI Increment 2. During the IOT&E, the HLO dashboard in DAI reported on 6 of 18 HLOs. In some cases, Agencies are not using the full suite of Increment 2 capabilities, are not monitoring the HLO dashboard, and have not achieved the HLO thresholds. DOT&E will reassess the HLOs during Increment 3 testing.
  - In spite of the improvements in the DAI system, users continue to give the program a marginal System Usability Score of 54, up from 48 reported in the Release 2 OA. Factors causing that marginal user rating include:
    - Experience is a statistically significant factor. Four out of 16 Agencies surveyed during IOT&E had used DAI for less than 2 years. Users at those four Agencies assessed usability to be unacceptable (less than 50). Users with more experience scored DAI higher.
    - Frequent user comments on DAI functionality related to the slowness and difficulty of entering data and generating DAI reports, queries, and search requests.
  - DAI Help Desk support for the Agency help desks is sustainable, but most Agencies provide additional funding to obtain additional manning for help desk support, training, and support for new capability development. This user funding masks the true cost of DAI sustainment for the DOD enterprise.
  - The DAI Help Desk processed 6,479 service requests or incidents between November 1, 2016, and April 1, 2017, with the number of open tickets decreasing from 690 to 523 over that period.
  - The DAI PMO resolved 81 percent (525 of 647) Priority 2 tickets within 30 days. Customer satisfaction with the DAI Help Desk was 68 percent, compared to 92 percent for the local Agency help desk support. The DAI Tier 2 Help Desk provides users with workarounds to all Priority 2 issues until a permanent resolution is determined. Improving resolution times for Priority 2 issues should improve overall customer satisfaction.
- DAI is secure against an outsider cyber threat having limited capabilities; however, DAI is vulnerable to an insider cyber threat operating with limited to moderate capabilities.
  - During the Adversarial Assessment, the DISA Red Team – using limited cyber-attack capabilities – was unable to exploit DAI as an outsider. However, as an insider, the Red Team identified four vulnerabilities, and the network defenders did not detect the Red Team.
- During the CEVA, Agencies' financial experts concluded that the existing technical checks would make it difficult to exploit known or potential vulnerabilities to commit fraud.
- Per DISA and Defense Logistics Agency Chief Information Officer policy, the DAI PMO conducts a remote recovery exercise once every 3 years, with a tabletop exercise conducted in the years between.
- During the FY17 COOP exercise, the DAI PMO and DISA conducted a tabletop exercise where personnel reviewed and updated the Information Security Contingency Plan. Previously in FY16, DAI PMO testers successfully executed selected business functions on alternate site servers, which verified that the alternate site could restore partial mission or business essential functionality. Because of the limited number of users and tasks, testing did not include load or performance testing. The alternate site does not currently have the capacity to support a full service restoration of DAI capabilities.

Recommendations

- Status of Previous Recommendations. The program has implemented changes to address many of the FY16 recommendations; however, the following recommendations remain applicable:
  1. DISA and DAI personnel failed to detect and react to Red Team activities during two consecutive Adversarial Assessments; therefore, DAI should work with DISA to improve real-time cybersecurity detect and react capabilities for DAI and mitigate known vulnerabilities.
  2. The PMO still needs to conduct the fraud analysis portion of the CEVA. It is currently planned for the first operational assessment of DAI Increment 3 in FY19.
  3. The DAI PMO should continue to monitor and improve system performance to reduce response times and unexpected errors.
- FY17 Recommendations. The full list of recommendations is available in the September 2017 DOT&E report on DAI IOT&E; highlighted recommendations are below. The DAI PMO should:
  1. Complete the HLO dashboard by working with the Office of the Under Secretary of Defense (Comptroller) to identify who manages the Agencies as they reengineer business processes to achieve HLO standards.
  2. Maintain "Customer Liaison" positions within the PMO to consolidate and share lessons learned with the Agencies as they implement DAI.
  3. Improve real-time cybersecurity detect and react capabilities for DAI and verify fixes during the FY18 FOT&E.
  4. Decrease the time to resolve DAI PMO Help Desk tickets.
  5. Continue to improve COOP site architecture and capabilities with a goal of developing a full DAI restoration capability from COOP to production site.
  6. Coordinate for all DAI Agencies participation in the next annual COOP event, with JITC and DOT&E observing.

Defense Medical Information Exchange (DMIX)

Executive Summary

Defense Medical Information Exchange Program

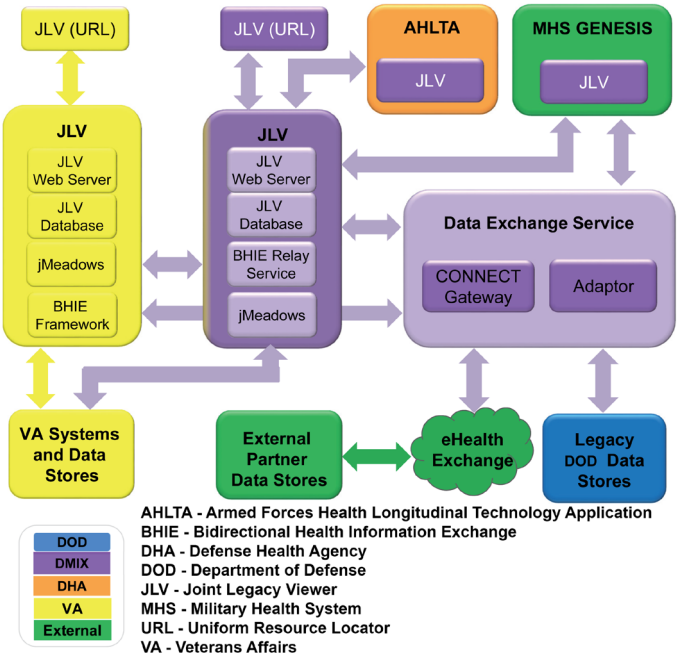
- The Program Executive Office (PEO) Defense Healthcare Management Systems (DHMS) moved the Defense Medical Information Exchange (DMIX) program under the DOD Healthcare Management System Modernization (DHMSM) Program Manager in August 2016. The DHMSM Program Manager is acquiring the Military Health System (MHS) GENESIS system as part of the DHMSM program, of which DMIX is a critical component.

Defense Medical Information Exchange Release 5

- The Army Test and Evaluation Command (ATEC) and Space and Naval Warfare (SPAWAR) Red Team conducted a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) on DMIX Release 5 from May 1-19, 2017, at Walter Reed National Military Medical Center (WRNMMC).
- ATEC, the Army Research Laboratory (ARL), and the SPAWAR Red Team conducted a cybersecurity Adversarial Assessment (AA) on DMIX R5 from August 28 through September 1, 2017, at WRNMMC.
- DMIX Release 5 is not survivable against cyber-attacks. DMIX cybersecurity testing discovered three high severity vulnerabilities that could allow an adversary to compromise patient data.

Defense Medical Information Exchange Release 6

- PEO DHMS fielded DMIX Release 6 in September 2017. DMIX Release 6 implemented a capability to parse MHS GENESIS notes into individual Joint Legacy Viewer (JLV) widgets and a capability to view Veterans Affairs (VA) scanned documents and artifacts in JLV.
- The Joint Interoperability Test Command (JITC) will operationally test DMIX Release 6 during the MHS GENESIS IOT&E to validate DMIX fixes from previous releases and to assess new capabilities.



System

- The DMIX program supports integrated sharing of standardized health data among MHS GENESIS, DOD legacy systems, VA, other Federal agencies, and private-sector healthcare providers.
- Together, MHS GENESIS and DMIX are intended to modernize the Military Health System to enhance sustainability, flexibility, and interoperability for improved continuity of care.
- The DOD is developing DMIX incrementally, delivering upgrades to already fielded capabilities. DMIX comprises two main components:
  - The JLV provides an integrated, read-only, chronological view of health data from DOD and VA electronic health record systems, eliminating the need for VA or DOD clinicians to access separate viewers to obtain real-time patient information. DOD and VA users log on to their respective JLV web servers using a URL address in their web browser. Users of the Armed Forces Health Longitudinal Technology Application can connect to the JLV web server through the system menu.
  - The Data Exchange Service (DES) receives user queries entered through JLV and queries DOD, VA, and external partner data stores, returning the results to jMeadows. jMeadows maps local VA and DOD clinical terms to standard medical terminology and aggregates the data for presentation by the JLV web server.

Mission

The DOD, VA, Federal agencies, and private-sector health providers use the DMIX infrastructure and services to:

- Share standardized health data using standard terminology
- Exchange standardized electronic health data securely and reliably with all partners
- Access a patient's medical history from a single platform, eliminating the need to access separate systems to obtain patient information
- Maintain continuity of care
- Exchange outpatient pharmacy and medication allergy data and check for drug-to-drug and drug-to-allergy interaction

Major Contractors
- DES/JLV: ManTech – Arlington, Virginia, and Hawaii Resource Group – Honolulu, Hawaii
- Test Support: Deloitte – Falls Church, Virginia
- Program Manager Support: Booze Allen Hamilton – McLean, Virginia

---

Activity

Defense Medical Information Exchange Program
- PEO DHMS moved the DMIX program under DHMSM in August 2016.
- PEO DHMS transitioned DMIX into sustainment in October 2016.

Defense Medical Information Exchange Release 5
- PEO DHMS fielded DMIX Release 5 in October 2016 and issued seven patches in FY17 that implemented new capabilities and fixed defects. The capabilities included a new widget to view MHS GENESIS patient data in JLV and created a mechanism to prepopulate MHS GENESIS with Procedure, Allergies, Medications, Problems, and Immunization patient data from legacy systems.
- ATEC, ARL, and the SPAWAR Red Team conducted a cybersecurity CVPA on DMIX Release 5 from May 1-19, 2017, and a cybersecurity AA from August 28 through September 1, 2017, both at WRNMMC. ATEC and SPAWAR conducted the testing in accordance with the DOT&E-approved test plan.

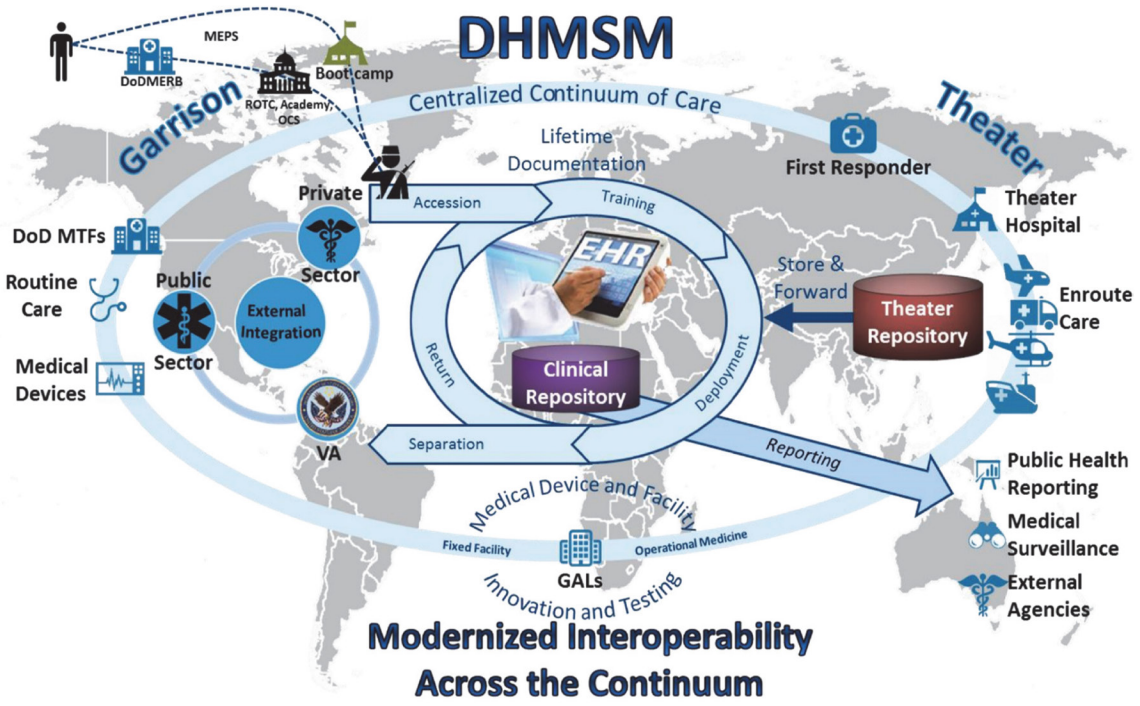
Defense Medical Information Exchange Release 6
- The program manager conducted developmental testing from August 4 through September 14, 2017, at Allegany Ballistics Laboratory (ABL), Rocket Center, West Virginia. DMIX Release 6 functionality improvements include the parsing of MHS GENESIS notes in individual widgets as well as the ability to view VA scanned documents and artifacts in JLV.
- PEO DHMS fielded DMIX Release 6 in September 2017.
- JITC will operationally test DMIX Release 6 during the MHS GENESIS IOT&E to validate DMIX Release 3 fixes and to assess new capabilities, such as the ability of DOD and VA users to view scanned documents and artifacts in JLV.

Assessment

Defense Medical Information Exchange Release 5
- DMIX Release 5 is not survivable against cyber-attacks. The CVPA revealed several vulnerabilities that could allow an adversary to compromise patient data. The cyber test aggressors then exploited these vulnerabilities during the Adversarial Assessment.

Recommendations
- Status of Previous Recommendations. The DHMSM Program Manager has addressed all FY16 recommendations, with the exception of the following which require support from the VA:
  - PEO DHMS has not expanded VA testing of correlation between the DOD and VA terminology maps.
  - The VA has not allowed a DOD Red Team to perform cybersecurity testing of DMIX components and interfacing systems on VA networks.
- FY17 Recommendations. The DHMSM Program Manager should:
  1. Correct the three cybersecurity vulnerabilities identified during DMIX Release 5 cybersecurity testing.
  2. Verify DMIX cybersecurity fixes as part of the MHS GENESIS cybersecurity testing.

DOD Healthcare Management System Modernization (DHMSM)



LEGEND:			
DHMSM	DoD Healthcare Management Systems Modernization	MERB	Medical Examination Review Board
DoD	Department of Defense	MTF	Military Treatment Facility
EHR	Electronic Health Record	OCS	Officer Candidate School
GAL	Government Authorized Laboratory	ROTC	Reserve Officers' Training Corps
MEPS	Military Entrance Processing Station	VA	Veterans Affairs

Executive Summary

- The DOD Healthcare Management System Modernization (DHMSM) Program Manager completed go-live of the Military Health System (MHS) GENESIS at all four Initial Operational Capability (IOC) sites in 2017.
- The Joint Interoperability Test Command (JITC) conducted the MHS GENESIS operational assessment (OA) from May through June 2017 at the Fixed Facility (FF) Government Approved Laboratory (GAL).
  - During the OA, users completed the majority of the tasks required to accomplish their missions. However, users identified 26 high-priority deficiencies, 14 of which remained open at the end of the OA. The 14 defects were subsequently either resolved by the Program Manager or accepted by the Function Advisory Council prior to receiving authority to go-live at Naval Hospital Bremerton (NHB) and Madigan Army Medical Center (MAMC). Users encountered deficiencies in the dental, immunization, and pharmacy clinical areas, and in common user tasks across multiple clinical areas.
  - JITC only completed a partial interoperability assessment during the OA because the DHMSM Program Manager did not provide data for all of the planned interfaces. Of the interfaces tested, the majority did not conform to the data standard and/or the Interface Control Document.
  - Users at all sites rated the system poorly for usability. Users at Fairchild AFB and Naval Hospital Oak Harbor (NHOH) also indicated that the training they received did not prepare them for using the system to conduct their daily jobs.
- Separate from the OA, the DOD Chief Information Officer (CIO) conducted system scans of MHS GENESIS that revealed a high number of Category (CAT) I cybersecurity vulnerabilities. As of October 2017, 313 CAT I cybersecurity vulnerabilities remained outstanding. These gaps in security indicate MHS GENESIS is not survivable in a contested cyberspace environment. Furthermore, there is currently no alternate server site to support Continuity of Operations.
- JITC is conducting the MHS GENESIS IOT&E, which includes cybersecurity testing, from September 25, 2017, through February 16, 2018. DOT&E plans to release the IOT&E Report in April 2018.

System

- The DOD DHMSM Program Manager will acquire and field MHS GENESIS, a modernized Electronic Health Records (EHR) system, to 153,000 Military Health System personnel, providing care for 9.4 million DOD beneficiaries worldwide.
- MHS GENESIS comprises three major elements:
  - The Millennium suite of applications, developed by Cerner, which provides clinical capabilities
  - Dentrix Enterprise, developed by Henry Schein Inc., which provides dental capabilities
  - Orion Rhapsody Integration Engine, developed by Orion Health, which enables the majority of the external information exchanges
- The DHMSM Program Manager established two program segments to support deployment of the DHMSM EHR System to the DOD enterprise:
  - Fixed Facility (Segment 1) supports all medical and dental services delivered by permanent inpatient hospitals and medical centers, ambulatory care clinics, and dental clinics.
  - Operational Medicine (Segment 2) supports theater hospitals, hospital ships, forward resuscitative sites, naval surface ships, and submarines. The EHR System will be configured to work in the tactical environment. The DHMSM Program Manager will provide MHS GENESIS to the Joint Operational Medicine Information System Program Office for implementation.
- MHS GENESIS will replace legacy healthcare systems including the Armed Forces Health Longitudinal Technology Application (AHLTA), Composite Health Care System (CHCS), and Essentris inpatient system. MHS GENESIS will replace legacy Operational Medicine components of the Theater Medical Information Program (TMIP) – Joint software suite including AHLTA-Theater, TMIP CHCS Caché, and AHLTA-Mobile.

Mission

DOD medical staff will use MHS GENESIS to deliver enroute care, dentistry, emergency department, health, immunization, laboratory, radiology, operating room, pharmacy, vision, audiology, and inpatient/outpatient services. DOD medical staff will also use MHS GENESIS to perform administrative support, front desk operations, logistics, billing, and business intelligence.

Major Contractors

- Leidos – Reston, Virginia
- Cerner – Kansas City, Missouri
- Accenture Federal Services – Arlington, Virginia
- Henry Schein Inc. – Melville, New York

Activity

- The DHMSM Program Manager completed MHS GENESIS go-live at all four IOC sites in 2017:
  - Fairchild AFB, Washington, on February 7, 2017
  - NHOH, Washington, on July 15, 2017
  - NHB, Washington, on September 23, 2017
  - MAMC, Washington, on October 21, 2017
- The DOD CIO began cybersecurity scans of MHS GENESIS on January 20, 2017, and plans to continue scanning and performing other evaluation activities through July 2018.
- JITC conducted the MHS GENESIS OA from May 22 through June 23, 2017, at the FF GAL at Auburn, Washington.
- JITC conducted the first component of the MHS GENESIS IOT&E from September 25 through October 6, 2017, at NHOH and Fairchild AFB. JITC will conduct the next two components at NHB and MAMC in FY18.
- JITC intends to conduct a Cooperative Vulnerability and Penetration Assessment and an Adversarial Assessment following go-live at MAMC.
- JITC is conducting MHS GENESIS IOT&E, which includes cybersecurity testing, from September 25, 2017 through February 16, 2018. DOT&E plans to release the IOT&E Report in April 2018.

Assessment

- JITC conducted the MHS GENESIS OA at the FF GAL in accordance with a DOT&E-approved test plan. Data from the Fairchild AFB go-live assessment that JITC conducted in February 2017 augmented the OA results.
  - Users completed the majority of the tasks required to accomplish their missions, but also identified 25 high-priority deficiencies, 14 of which remained open at the end of the OA. The 14 defects were subsequently either resolved by the Program Manager or accepted by the Function Advisory Council prior to receiving authority to go-live at NHB and MAMC. Users encountered deficiencies in the dental, immunization, and pharmacy clinical areas, and in common user tasks across multiple clinical areas. In the area of Dentistry Services Management, users could not fully document patient care because of problems with scanning and uploading documents. Millennium and Dentrix failed to exchange data in some instances, resulting in MHS GENESIS failing to exchange information via its internal interfaces and interrupting dental patient care. Users could not complete the mass vaccination of multiple patients in a timely manner because of a defect that required them to restart the application to document vaccines given to each patient. Pharmacists identified discrepancies between prescription order quantities and the amount filled by the interfacing system, preventing management of prescriptions by the pharmacist. Common user tasks span all clinical areas. Users experienced problems managing appointments,

medical records, radiology imaging orders, medical history, referrals, physical exams, and patient eligibility through the Defense Enrollment Eligibility Reporting System. Operational users at Fairchild AFB reported problems with MHS GENESIS billing and report generation.
  - The DHMSM Program Manager identified 42 interfaces required to support operations at the four IOC sites. The DHMSM Program Manager did not provide data on 17 of 36 interfaces planned for JITC's pre-IOT&E assessment of interoperability. Of the interfaces with data available, the majority did not conform to the data standards and/or the Interface Control Document.
  - MHS GENESIS users at Fairchild AFB, NHOH, and OA participants rated MHS GENESIS usability as "low." Inadequate training, outdated system manuals, the need for multiple roles to accomplish mission tasks, and the increased length of workflows compared to the legacy systems negatively affected users' opinions of the system.
  - Users at both Fairchild AFB and NHOH reported similar concerns with the training, stating that clinical specialty training was non-existent or not relevant, they required more practice before go-live, and the training did not prepare them for using MHS GENESIS. The Program Manager incorporated lessons learned from OA and Fairchild AFB, however there is more work required in the area of training effectiveness and planning.
  - After the Program Manager discontinued the Leidos Partnership for Defense Health Command Center at Fairchild AFB, users did not have sufficient visibility into trouble tickets, and the lack of consistency in the trouble ticketing process during go-live hindered their ability to follow-up on trouble tickets created.
- The system scans of MHS GENESIS revealed a high number of high severity (CAT I) cybersecurity vulnerabilities. Exploitation of a CAT I vulnerability directly leads to loss of confidentiality, availability, or integrity of data. Though the DHMSM Program Manager and DOD CIO have been working aggressively to identify and resolve high severity MHS GENESIS cybersecurity vulnerabilities, 313 CAT I cybersecurity vulnerabilities remain outstanding as of October 2017. These gaps in security indicate MHS GENESIS is not survivable in a contested cyberspace environment. Furthermore, there is currently no alternate server site to support Continuity of Operations. Without a functional alternate site, DOD healthcare providers and patients are at risk if the primary site goes down.

Recommendations

- Status of Previous Recommendations. The DHMSM Program Manager addressed one of the two previous recommendations; however, the Program Manager did not fix or mitigate high severity cybersecurity vulnerabilities prior to go-live at Fairchild AFB.
- FY17 Recommendations. The DHMSM Program Manager should:
  1. Resolve high severity cybersecurity vulnerabilities as soon as possible to minimize the risk of a cyber-attack against MHS GENESIS comprising current and former service members' private health records.
  2. Complete the alternate site buildout to enable a functional Continuity of Operations site.
  3. Identify the root causes of the open defects found during the OA and implement fixes in both the test and production environments.
  4. Improve trouble ticket tracking and user follow-up.
  5. Improve training so that clinical specialty training is relevant to each clinical area and specific to the MHS GENESIS Military Baseline and implement the improved training before further fielding.
  6. Incorporate lessons learned from previous go-live events when fielding to future sites.

F-35 Joint Strike Fighter (JSF)

Executive Summary

Test Strategy, Planning, and Activity

- The F-35 Joint Strike Fighter (JSF) program focused on completing developmental testing (DT) and verifying compliance with JSF contract specifications by the end of CY17. The program completed two reviews of the DT work remaining and deleted test points in an attempt to stay on schedule. Some test points were considered to be in excess, but others were deemed important for DT or OT. Despite the test point deletions, continued test delays, particularly for mission systems and F-35B flight sciences, will likely push the end of DT into the first or second quarter of CY18, even as time and funding are running out for System Development and Demonstration (SDD).
- Preparations for IOT&E are progressing, although the program will not meet several of the readiness criteria until late CY18; as a result, formal entry into IOT&E will not occur before then.
- The F-35 Joint Program Office (JPO) plans to transition into the next phase of development – Continuous Capability Development and Delivery (C2D2) – beginning in CY18, to address deficiencies identified in Block 3F development and to incrementally provide planned Block 4 capabilities. However, the original C2D2 schedule was not executable due to inadequate test resources in the timelines allocated for both developmental and operational testing to field the planned new capabilities. The program's C2D2 acquisition strategy and development and delivery timelines were under review at the time of this report.

Completing SDD

Developmental Testing

- Flight sciences testing for all variants continued into CY17.
  - F-35A testing completed in March 2017, with the exception of drag chute testing – a Norway-unique test requirement.
  - F-35B testing continued throughout CY17 and will not be complete until early CY18. The need for test-unique tail coatings to prevent overheating the horizontal tails at high airspeed test points, repairing unanticipated cracks in the main landing gear and structural frame, and engine restrictions prohibiting some flight operations resulted in delays to testing.
  - F-35C work included testing of the redesigned outboard wing structure, required to support carriage of the AIM-9X air-to-air missile on a pylon.
- Block 3F mission systems testing continued throughout CY17. DOT&E estimates mission systems testing will continue through February 2018. The program will not be able to completely mitigate the many open deficiencies by the end of SDD, resulting in shortfalls in fielded Block 3F capabilities identified in the JSF Operational Requirements Document (ORD), capabilities the F-35 needs in combat against current threats.

- Static structural and durability testing continued in CY17 for the third lifetime of the F-35A and F-35C test articles (one lifetime is 8,000 equivalent flight hours). F-35A testing completed in October 2017 and F-35C testing at the end of CY18.
- The JPO suspended durability testing for the F-35B after completion of the second lifetime of testing in February 2017; the test article had so many repairs it was no longer representative of the production aircraft. The program has not yet procured another durability test article for the F-35B to begin the third lifetime of testing. The effect of the failures observed and repairs required during the first two lifetimes of testing on the service life certification of the F-35B aircraft is still to be determined. The service life for all three variants is planned to be 8,000 hours, however the F-35B service life may be less than that, even with extensive modifications to strengthen the aircraft already produced.

Mission Data Load Development and Testing

- The U.S. Reprogramming Laboratory (USRL) continues to operate with cumbersome software tools and outdated or incomplete hardware. The lab began creating Block 3F mission data files (MDFs) in the summer of 2017, and it will take 12 to 15 months to deliver a fully-verified mission data load (MDL), made up of a compilation of MDFs, for IOT&E.
- Installation of improved radio frequency signal generators within the USRL test lines, necessary to partially address shortfalls in the replication of realistic signals, was delayed until the JPO placed Lockheed Martin on contract in November 2017.

- The lab test lines need a number of key hardware upgrades to effectively and efficiently develop Block 3F MDFs, and to test and verify their signal detection, identification, and geolocation performance in scenarios representative of combat against the advanced adversaries for which the F-35 was designed.
- The Department programmed $45 Million in FY14-15 for upgrades, but the JPO failed to initiate the contract actions.
- The USRL procured 16 new radio frequency signal generator systems known as Advanced Pulse Generators (APGs) – 8 for each of 2 reprogramming test lines – which will overcome the lab's signal fidelity shortfalls, but still will not provide enough signal density.
- The USRL plans to complete installation and checkout of the APGs, and the new computer hardware that controls them, in the fall of CY18. The installation was delayed until the JPO put Lockheed Martin on contract in November 2017 to conduct the security certification, accreditation, and configuration management processes necessary to obtain authorization to operate in the new configuration. This process is expected to take a year to complete.
- Even after the installation and certification of the new configuration, the lab will still lack a sufficient number of signal generators to simulate a realistic, dense threat laydown with the multiple modern surface-to-air missiles, combat aircraft, and many supporting air defense radars that make up such a laydown.

• Substantial additional investments that have yet to be fully planned or funded are required as soon as possible to upgrade the USRL in order to support F-35 C2D2 MDL development.
  - The C2D2 plan includes new Technical Refresh 3 processors and other new hardware.
  - Concurrent F-35 development and production has resulted in multiple fielded F-35 configurations, many of which will remain active during the C2D2 phase. The USRL, or an additional reprogramming lab, will need to have the capability to simultaneously create and test MDLs for existing and future avionics hardware and software configurations.

Weapons Integration and Demonstration Events

• The JPO completed planned Block 3F Weapons Delivery Accuracy events in CY17 for bombs and missiles, with 15 of 27 results still in analysis. These events have continued to be a source of discovery of deficiencies, and frequently paused progress until corrections could be developed and tested.
• The JSF Operational Test Team (JOTT), along with the associated Service operational test squadrons, conducted weapon demonstration events for both air-to-ground bombs and air-to-air missiles. The JOTT conducted these activities in accordance with a DOT&E-approved test plan using Block 2B and Block 3i operational test aircraft.
  - The air-to-ground weapons events identified mission systems-related deficiencies that adversely affected the completion of the find, fix, track, target, engage, and assess kill chain. These deficiencies included errors in the Launch Acceptability Region (a range displayed to the pilot for the weapon release to meet terminal requirements), the inability of the pilot to confirm coordinates sent to the Joint Direct Attack Munition (JDAM), and deficiencies associated with the Electro-Optical Targeting System.
  - The air-to-air weapons events identified classified integration problems and pilot-identified deficiencies, as well as mission planning and debriefing shortfalls – all of which the JOTT documented in formal deficiency reports.
• The test centers continued gun testing on all variants in CY17. The gun capability is new to the Block 3F weapons suite.
  - Integration, helmet alignment, and line-of-sight problems discovered with the first F-35A air-to-ground aimed firing in February 2017 delayed further testing until the problems could be addressed. Once allowed to proceed, accuracy testing of the F-35A gun showed that it consistently had a long and to-the-right aiming bias, a deficiency that the JPO and Lockheed Martin are investigating.
  - Initial accuracy testing of the F-35B and F-35C podded guns showed better results than that of the F-35A model. Both the F-35B and the F-35C gun pods exhibited the same right aiming bias as the F-35A, however the long bias is not manifested in the podded gun systems.

LFT&E

• In FY17, the live fire test team completed the final F-35 LFT&E ballistic vulnerability test series using the F-35C full-scale structural test article. This test series completed the testing defined under the LFT&E Alternative Test Plan that provides the information needed to adequately assess F-35 vulnerability to the prescribed threats.
• Lockheed Martin completed final ballistic vulnerability analyses for all three F-35 variants against four likely threats. DOT&E is in the process of evaluating the results.
• The JPO evaluated the chemical and biological agent protection and decontamination systems during full-up system-level decontamination testing. The test plan to assess chemical and biological decontamination of pilot protective equipment is not adequate; the JPO does not plan to test either the Gen III or the Gen III Lite Helmet Mounted Display System (HMDS).
• The JPO and DOT&E have not received a report from the Navy on the results of vulnerability testing completed in 2016, which tested F-35B electrical and mission systems against electromagnetic pulses. DOT&E is awaiting the Navy's report in order to adequately assess this vulnerability before the Full-Rate Production decision.
• The 780th Test Squadron at Eglin AFB, Florida, completed ground-based lethality tests of three 25 mm round variants against armored and technical vehicles, aircraft, and personnel-in-the-open targets. The rounds tested were the PGU-32/U Semi-Armor Piercing High Explosive Incendiary round, PGU-47/U Armor Piercing High Explosive Incendiary

with Tracer round, and PGU-48/B Frangible Armor Piercing round. The results are classified.

Operational Suitability

- The operational suitability of the F-35 fleet remains below requirements and is dependent on work-arounds that would not meet Service expectations in combat situations. Over the previous year, most suitability metrics have remained nearly the same, or have moved only within narrow bands which are insufficient to characterize a change in performance.
- Overall fleet-wide monthly availability rates remain around 50 percent, a condition that has existed with no significant improvement since October 2014, despite the increasing number of new aircraft. One notable trend is an increase in the percentage of the fleet that cannot fly while awaiting replacement parts – indicated by the Not Mission Capable due to Supply rate.
- Reliability growth has stagnated. It is unlikely that the program will achieve the JSF ORD threshold requirements at maturity for the majority of reliability metrics. Most notably, the program is not likely to achieve the Mean Flight Hours Between Critical Failures threshold without redesigning aircraft components.

Autonomic Logistics Information System (ALIS)

- The program attempted to test and field ALIS software version 2.0.2.4 throughout CY17. Testing identified deficiencies, some of which the program addressed with corrections prior to fielding. After converting four operating locations to ALIS 2.0.2.4, the Marine Corps units at Marine Corps Air Station (MCAS) Yuma, Arizona, suspended flight operations in June after determining that ALIS was not properly tracking life usage on engine components.
- The program addressed deficiencies with ALIS 2.0.2.4.4, which began testing at Nellis AFB, Nevada, in September. This testing discovered additional deficiencies that caused the Air Force to stop fielding ALIS 2.0.2.4.4 until the program corrected the deficiencies. The Air Force restarted fielding ALIS 2.0.2.4.4 at Eglin AFB, Florida, in November 2017, to be followed by Luke AFB, Arizona, in January 2018.
- The program completed development of ALIS 2.0.2.5 in late CY17 to address some of the existing deficiencies and usability problems within ALIS and upgrade the browser to Internet Explorer 11. This version will include a filtering function designed to decrease false alarms in the Prognostic Health Management System, but no new capabilities.
- ALIS 3.0, the last increment to be released within SDD, has begun regression testing and the JPO expects it to be ready for fielding in CY18. Even though the program has deferred many of the capabilities planned for ALIS 3.0 to ALIS 4.0, the schedule is at risk.

Cybersecurity Testing

- The JOTT continued to conduct cybersecurity testing on F-35 systems, in partnership with certified cybersecurity test organizations and personnel. The testing was conducted in accordance with the DOT&E-approved cybersecurity strategy.
- In 2017, the JOTT conducted Cooperative Vulnerability and Penetration Assessments (CVPAs) and Adversarial Assessments (AAs) of ALIS 2.0.2.4 at all three levels of operation:
  - Autonomic Logistics Operating Unit (ALOU), the collection point and hub for global F-35 logistics data
  - Central Point of Entry (CPE), the component for collecting and staging the data distributed to and from field locations
  - Squadron Kit (SQK), the operational component at the field units
- The AAs did not all complete satisfactorily due to events beyond the control of the JOTT; the JOTT is planning to reschedule uncompleted portions of the AAs in CY18.
- Cybersecurity testing in 2017 showed that some of the vulnerabilities identified during earlier testing periods still had not been remedied.
- More testing is needed to assess the cybersecurity structure of the air vehicle and supporting logistics infrastructure system (i.e., ALOU, CPE, and SQK) and to determine whether, and to what extent, vulnerabilities may have led to compromises of F-35 data. The JOTT has scheduled this testing in CY18.

IOT&E Readiness

- Despite good progress in preparations for starting IOT&E, the program will not complete all readiness criteria until late CY18.
- The 23 aircraft OT fleet will not complete modifications to the Block 3F production-representative configuration until August 2018.
- Required aircraft instrumentation and integration with the test ranges need to be completed and tested prior to starting formal test. These include the Air-to-Air Range Infrastructure system, Air Warfare Battle Shaping system, and flight certification for the Data Acquisition Recording and Telemetry pod. The program should complete testing of all required aircraft instrumentation required for IOT&E test adequacy.
- The Joint Simulation Environment, although not required for start of IOT&E, will likely not be completely accredited before the completion of the open-air portion of IOT&E.
- The program continued working to address unresolved technical deficiencies. These include open deficiency reports identified during developmental testing, modifications to the pilot escape system, a growing number of physiological incidents, production line quality lapses, inadequate tire durability for the F-35B, deficiencies with the helmet display and night vision camera, and restrictions in air refueling for the F-35B and F-35C. The operational effect of these deficiencies, if unresolved, will be assessed during IOT&E.

System

- The F-35 JSF program is a tri-Service, multinational, single-seat, single-engine family of strike aircraft consisting of three variants:
  - F-35A Conventional Take-Off and Landing
  - F-35B Short Take-Off/Vertical-Landing
  - F-35C Aircraft Carrier Variant
- The F-35 is designed to survive in an advanced threat environment (year 2015 and beyond). It is also designed to have improved lethality in this environment compared to legacy multi-role aircraft.
- Using an active electronically scanned array radar and other sensors, the F-35 with Block 3F software is intended to employ precision-guided weapons (e.g., GBU-12 Laser-Guided Bomb, GBU-31/32 JDAM, GBU-39 Small Diameter Bomb, Navy Joint Stand-Off Weapon version C1) and air-to-air missiles (e.g., AIM-120C Advanced Medium-Range Air-to-Air Missile (AMRAAM), AIM-9X infrared-guided, short-range, air-to-air missile).
- The SDD program was designed to provide mission capability in three increments:
  - Block 1 (initial training; two increments were fielded: Block 1A and Block 1B)
  - Block 2 (advanced training in Block 2A and limited combat capability with Block 2B)
  - Block 3 (limited combat capability in Block 3i and full SDD warfighting capability in Block 3F)
- The F-35 is under development by a partnership of countries: the United States, United Kingdom (UK), Italy, the Netherlands, Turkey, Canada, Australia, Denmark, and Norway.

Mission

- The Combatant Commander will employ units equipped with F-35 aircraft in joint operations to attack targets during day or night, in all weather conditions, and in heavily defended areas.
- The F-35 will be used to attack fixed and mobile land targets, surface units at sea, and air threats, including advanced aircraft and cruise missiles.

Major Contractor

Lockheed Martin, Aeronautics Company – Fort Worth, Texas

Test Strategy, Planning, and Activity

- Developmental Testing
  - As of November 6, 2017, the JPO had collected data and verified performance to close out 252 of 476 (53 percent) contract specification paragraphs; 2,516 of 3,452 (73 percent) success criteria derived from the contract specifications had been completed.
  - The JPO completed two reviews of remaining mission systems testing in CY17 and deleted test points in an attempt to keep developmental flight testing on schedule. Some test points were considered to be in excess, but others were deemed important for DT or OT. The deleted test points included those needed for air-to-air gun accuracy, IOT&E instrumentation, and validation of the IOT&E simulation. Despite these cuts, the projected completion of Block 3F mission systems and flight sciences testing has continued to slip into the first or second quarter of CY18. The delays are caused by immature capabilities, continued discoveries, development of corrections, and regression testing, as well as typical test attrition for ground aborts, weather, etc.
  - Staffing at the test centers decreased as qualified, cleared personnel left due to uncertainty over program funding and manning in FY18. The program recently sought to reassure the test centers that funding is available, but decreased staffing continues to adversely affect flight test operations and data analyses.
  - The "final" Block 3FR6.3 software for SDD was released in October 2017, but this planned final version has already been superseded by two additional software updates; more software patches will likely be needed as the program continues to work ongoing problems with weapons and avionics.
  - The F-35A gun has been consistently missing ground targets during strafe testing; the program is still troubleshooting the problems.
  - The F-35B ground test article is unable to start third-life structural testing due to the extensive repairs that were required to complete the second-life testing. The JPO has not yet funded, nor put on contract, a new ground test article.
  - Although the time and funding for SDD are running out in CY17, it is clear that SDD-related work will continue well into CY18. The program's proposed new C2D2 plan attempts to mitigate some of the SDD unresolved deficiencies by funding two more deficiency-fix software releases and flight test in CY18.
- Preparations for IOT&E. The JPO, Lockheed Martin, and the JOTT continued to prepare for IOT&E. Despite significant effort and progress since the FY16 DOT&E Annual Report, DOT&E estimates the program will not meet numerous readiness criteria required for a formal IOT&E start until late CY18.
  - The JPO planned to complete DT by the end of CY17, but flight testing will likely be completed no earlier than the first quarter of CY18 due to delays and problem discoveries (particularly for F-35B flight sciences and mission systems testing).
  - The Services' airworthiness authorities and the JPO plan to incrementally release, by variant, flight clearances

for the Block 3F envelope and weapons releases. All variants are not projected to have the full weapons and envelope clearances until the second quarter of CY18. The airworthiness authorities and weapons contractors have concerns with certifying the full planned Block 3F weapons and flight envelope, so there may be limitations that affect F-35 mission effectiveness in both IOT&E and fielded aircraft.

- The MDL that the operational test squadrons will use for IOT&E will not be complete and verified until the third quarter of CY18. Poor software tools and late delivery of Block 3F software to the USRL have hindered mission data development.
- Modifications to all of the 23 operational test aircraft, most of which are from early production lots and require avionics and structural modifications to the production-representative Lot 9 configuration, will not be complete until August 2018. The Services loaned some of their aircraft, which are already instrumented for IOT&E, to assist DT. As a result, these aircraft will not be available to begin the modification process to become production representative for IOT&E until their DT work is complete in late CY17 or early CY18.
- The program will likely not meet test instrumentation requirements until the third quarter of CY18. These include:
  - Air-to-Air Range Infrastructure system, version 2 (AARI 2) integration and testing, required for mission test trials on the Nevada Test and Training Range.
  - Cleared flight envelope for the Data Acquisition Recording and Telemetry (DART) pod. The envelope for the DART pod must be equivalent to that of the internal weapons for Block 3F, since the aircraft carry it internally on a weapons station. The DART pod must be cleared for weapons bay door cycling during simulated weapon launches during IOT&E to ensure operational realism.
  - Air Warfare Battle Shaping (AWBS), which can host AARI 2 on the Navy's Pacific Sea Test Range and China Lake test range.
  - Integration and testing of range threat emitters with F-35 AARI and AWBS.
- ALIS 3.0, planned for use in IOT&E and the completion of SDD, will likely not be ready for fielding until early to mid-CY18
- The Joint Simulation Environment (JSE), needed to assess F-35 capabilities against modern threat aircraft and dense, modern surface-to-air threat laydowns, will not be verified, validated, and accredited (VV&A) until the first quarter CY19 at the earliest; this would be late-to-need for IOT&E.
- Multiple security challenges must still be coordinated and resolved to allow the different types of aircraft, simulated threat systems and international partners to fly together, and for the resulting data to be processed during IOT&E.
- The program is still carrying a large number of unresolved deficiencies involving the air vehicle itself, Block 3F mission systems, ALIS, and mission planning. There are still approximately 1,000 open deficiencies, with only 88 of 301 Priority 1 and 2 "must fix" deficiencies, as reported by the Services, actually in-work as of November 19, 2017. These unresolved deficiencies will likely have a cumulative effect on F-35 mission capability during IOT&E.
- The program continued to develop, verify, and validate Joint Technical Data (JTD), the formal publications used by pilots and maintenance personnel, throughout CY17. Despite the many drawbacks of concurrency, the fielding of aircraft during development helped the program validate JTD modules in the field, particularly for standard, common maintenance actions. Having all Block 3F JTD written and verified is a readiness criterion for formal entrance into IOT&E.

• Continuous Capability Development and Delivery (C2D2)
- The JPO continued planning for the transition out of SDD to the next phase of development, formerly referred to as "Follow-on Modernization." This phase of development will now include a period of fielding Block 3F software patches, which will primarily address technical debt and deficiencies identified in flight testing into CY19. This will be followed by incremental development and testing of planned Block 4 capabilities at 6-month intervals.
- DOT&E assessed the original C2D2 schedule was not executable due to inadequate test resources (e.g., test aircraft, high-fidelity instrumentation, and software and mission data reprogramming laboratory lines) and too much new content in the rapid timelines proposed. The program's C2D2 acquisition strategy and development and delivery timelines were under review at the time of this report. Also, the 6-month software release cycle does not align with other increments of capability needed to support the entire JSF system (i.e., ALIS, mission data, training simulators, aircraft modifications), which have historically taken much longer for the F-35, F-22, and F/A-18. The program should re-plan C2D2 to have a more realistic schedule and content that includes adequate test infrastructure (labs, aircraft, and time) and modifications that align the other fielding requirements.
- Configuration management may become challenging as the Services will have aircraft fielded in multiple hardware and software configurations that will need software and test resources, including instrumented test aircraft.
- F-35 modernization is on OT&E oversight, so DOT&E will review the content of each C2D2 increment and, if the increment contains significant new capabilities, will require a tailored formal OT&E. DOT&E routinely conducts "agile" OT for other programs, so each OT&E would be tailored to be as efficient as possible while maintaining test adequacy by leveraging integrated testing with DT and focusing on evaluating the new capabilities and affected mission areas.

Developmental Testing

F-35A Flight Sciences

- Flight Test Activity with AF-1, AF-2, and AF-4 Test Aircraft
  - The program completed F-35A flight sciences testing for SDD in March 2017, with the exception of testing the drag chute on AF-2 (a Norway-unique testing requirement). Analyses of the test data are ongoing.
  - Testing in CY17 consisted of four of eight planned AIM-9X weapons separations tests on AF-1. In March, the program determined that the remaining four separation events were no longer required.
  - Flight test activity continued with AF-1 supporting testing as a chase aircraft and AF-2 conducting drag chute testing. AF-4 entered flyable storage in January, after completing the final phase of chemical and biological testing in December 2016.
  - Through the end of October 2017, the test team completed 58 of 62 test flights and 240 of 301 test points planned for the year. The balance of the remaining F-35A testing is for the Norwegian drag chute.
  - The program plans to conduct flight testing of the DART instrumentation pod, which is needed for IOT&E data collection, on AF-1 from December 2017 to January 2018.
- F-35A Flight Sciences Assessment
  - The Air Force airworthiness authorities are analyzing strain loads, flutter (from flight envelope expansion), weapons separations, and weapons bay acoustic and environmental data to determine the acceptable and safe envelope for flight operations and weapons carriage and employment, with both internal and external weapons stores.
    - The program expects to complete analysis and provide Block 3F military flight releases by late CY17, first for fielded Lot 9 aircraft and 2 months later for OT aircraft, which were produced in earlier lots.
  - The full planned F-35A Block 3F envelope is up to Mach 1.6, and 700 knots, and 9.0 g. Whether airworthiness authorities will clear the F-35A for the full planned envelope, for all planned configurations, without limitations remains to be determined.
    - Aerodynamic loads and environmental conditions within the weapons bay have either caused flight certification authorities to impose limitations to the weapons envelope or have caused weapon vendors to impose life limits on the weapons. Excessive temperatures in the weapons bay at low altitudes while at high speeds may result in speed and time restrictions when carrying internal weapons.

F-35B Flight Sciences

- Flight Test Activity with BF-1, BF-2, BF-3, BF-4, and BF-5 Test Aircraft
  - Through the end of October 2017, the test team flew 244 of 321 flights planned for CY17, and completed 936 of 1,337 test points for the year.
  - F-35B flight sciences focused on:
    - Continued data collection of strain loads, flying qualities and weapons separations for clearing the F-35B Block 3F flight envelope (i.e., Mach 1.6, 630 knots, and 7.0 g)
    - High angle-of-attack flying qualities
    - Podded gun fire testing
    - Air refueling operations
    - Ski jump testing to support UK ship-board operations
    - Rolling vertical landing testing
- F-35B Flight Sciences Assessment
  - The program plans to complete F-35B flight sciences testing by January 2018, enabling a military flight release for the full Block 3F flight envelope in May 2018, but delays are likely. As of the end of October 2017, the program had over 500 test points remaining to complete F-35B flight sciences testing.
  - The following discoveries affected F-35B flight sciences testing:
    - Excessive heating on the horizontal tail surfaces limited the time the aircraft could operate in afterburner at a high Mach number to collect necessary strain load data. To reach high Mach number test points, the program designed and installed flight-test-unique horizontal tail thermal barrier coatings on BF-3.
    - Cracks discovered in the main landing gear doors on BF-2 and in the FS472 bulkhead in the right-hand-side weapons bay required repairs which delayed testing.
    - Cracks discovered in the fuselage frame (FS346) and problems with the seal between the aircraft and the gun pod on BF-1 required repairs, delaying airborne gun fire testing.
    - DT aircraft BF-1, BF-2, BF-3, and BF-4 are equipped with an early, flight test-only engine model. Restrictions prohibiting flight operations slower than 60 knots, including hover and vertical landings, delayed testing.

F-35C Flight Sciences

- Flight Test Activity with CF-1, CF-2, CF-3, and CF-5 Test Aircraft
  - Through the end of October 2017, the test team flew 175 of 202 flights planned for CY17, and completed 720 of 950 test points for the year.
  - F-35C flight sciences focused on:
    - Continued data collection of loads, flying qualities, and weapons separations for clearing the F-35C Block 3F flight envelope (i.e., Mach 1.6, 700 knots, and 7.5 g)
    - Weapons separation testing of the AIM-9X missile (external only for all variants), Joint Standoff Weapon (internal only), and GBU-12 bomb (external carriage added for Block 3F)
    - Buffet and loads testing with a redesigned outboard wing structure due to excessive loads observed during testing with the AIM-9X missile on the outboard external pylons
    - Podded gun fire testing

  - Ship suitability testing with modified nose gear hold-back procedures for catapult launches to reduce vertical oscillations during launch.
- F-35C Flight Sciences Assessment
  - The program made progress mitigating excessive, disorienting vertical oscillations during catapult launches by reducing the hold-back release load and adjusting pilot procedures. Shipboard launches in September 2017 using these proposed fixes appeared to reduce the oscillations, but data and pilot surveys were still in review as of the writing of this report.
  - Although the test teams completed testing of the redesigned outboard wing structure, any limitations to carrying weapons on the outboard wing stations will be determined by the Navy's airworthiness authorities when they release the F-35C Block 3F flight envelope, expected in the second quarter of CY18.

Mission Systems

- Mission systems are developed, tested, and fielded in incremental blocks of capability:
  - Block 1 (no longer in use, 26 U.S. aircraft delivered in Block 1 configuration)
    - Block 1 provided initial training capability for Lots 2-3 aircraft, but no combat capability. The Services have since upgraded all of these aircraft to the Block 2B configuration through a series of modifications and retrofits. Additional avionics and structural modifications will be required to configure these aircraft in the Block 3F configuration.
  - Block 2A (62 U.S. aircraft)
    - The program designated Block 2A for advanced training capability and delivered 62 U.S. aircraft in production Lots 4 and 5 in this configuration.
    - No combat capability was available in Block 2A. The Services have upgraded all of the Block 2A aircraft to the Block 2B configuration with modifications and retrofits. Additional avionics and structural modifications will be required to fully configure these aircraft in the Block 3F configuration.
  - Block 2B (no aircraft delivered in this configuration; 88 Block 1 and Block 2A U.S. aircraft upgraded to Block 2B)
    - The program designated Block 2B for initial, limited combat capability with selected internal weapons (AIM-120C, GBU-31/32 JDAM, and GBU-12). This block is not associated with the delivery of any lot of production aircraft, but with an upgrade of mission systems software capability for aircraft configurations through Lot 5.
    - Block 2B is the software that the Marine Corps accepted for the F-35B Initial Operational Capability (IOC) configuration, declaring IOC in July 2015.
    - Corrections to some deficiencies identified during Block 2B and Block 3i mission systems testing were included in the latest production release of Block 2B software – version 2BR5.3 – fielded in May 2016.
    - The Services began converting aircraft from these earlier production lots to the Block 3i configuration by replacing the older Technical Refresh 1 integrated core processor with newer Technical Refresh 2 (TR2) processors in 2016, as well as other hardware upgrades. As of the end of October 2017, 69 of the 88 aircraft (39 F-35A, 26 F-35B, and 4 F-35C) remained in the limited Block 2B (Technical Refresh 1) configuration.
  - Block 3i (108 U.S. aircraft delivered; capable of upgrading to Block 3F)
    - The program designated Block 3i for delivery of aircraft in production Lots 6-8 and a portion of Lot 9, as these aircraft are equipped with upgraded TR2 integrated core processors.
    - Block 3i software began flight testing in May 2014, but experienced many delays and problems due to software immaturity and instability during startup and in flight. As a result, the program paused flight testing of Block 3F software in February 2016 (software version 3FR5) and returned to Block 3i development and flight testing, fielding version 3iP6.21 to operational units in April 2016 with improved stability performance. The Air Force declared IOC with Block 3i-capable aircraft in August 2016.
  - Block 3F (7 U.S. aircraft delivered as of the end of October 2017)
    - The program designated Block 3F as the full SDD warfighting capability for production Lots 9 and later, with plans to upgrade the earlier block aircraft in the future. Block 3F will expand the flight envelope for all variants and includes additional weapons, external carriage of weapons, and the gun.
    - Flight testing with Block 3F software began in March 2015. Block 3F software was too unstable for productive flight testing and hampered progress. After improving the flight stability of the Block 3i software, the program applied the corrections to Block 3F software and continued Block 3F testing.
    - Due to immature Block 3F capabilities and discoveries of deficiencies, the program released multiple versions of Block 3F software, including Quick Reaction Cycle (QRC) versions in attempt to quickly address key deficiencies that were blocking test points.
    - The program delivered the final planned version of Block 3F software – 3FR6 – to flight testing in December 2016. However, flight testing in 2017 revealed the need for several more full and QRC versions of Block 3F software. As of late October 2017, the program was preparing a second version of Block 3FR6.3 (3FR6.32), the 31st version of Block 3F, software as it continues work to resolve key remaining deficiencies.
    - Notably, all of the aircraft from earlier production lots (i.e., Lots 2-5) will need to be modified – to include structural modifications and the installation of TR2 processors – in order to have full Block 3F capabilities.

  - The JPO agreed to allow Lockheed Martin to deliver the initial Lot 9 aircraft with Block 3i software. The first Air Force F-35A delivered with Block 3F software was AF-123, a Lot 9 aircraft delivered to Nellis AFB, Nevada, in September, 2017.
  - The production software version of Block 3F, designated 3FP6.2, was released to test in May 2017. The aircraft accepted with the early version of Block 3FP6.2 software are still not cleared for the full Block 3F envelope and have partially tested MDLs.
- Post-Block 3F Development, now referred to as Continuous Capability Development and Delivery (C2D2)
  - The program's post-SDD development program was previously referred to as Follow-on Modernization (FoM). The FoM plan was not executable due to too much content for the planned schedule and inadequate test resources.
  - The program developed the new C2D2 modernization plan in mid-2017. The C2D2 plan attempts to reduce some of the SDD technical debt by funding several needed deficiency correction software releases with limited flight testing in 2018-2019. This phase will be followed by incremental development and testing of planned Block 4 capabilities at 6-month intervals.

• Flight Test Activity with AF-3, AF-6, AF-7, BF-4, BF-5, BF-17, BF-18, CF-3, CF-5, and CF-8 Flight Test Aircraft and Software Development Progress
- Through the end of October, the six mission systems developmental flight test aircraft assigned to the Edwards AFB Air Force Test Center in California flew an average rate of 10.2 flights per aircraft, per month, slightly above the planned rate of 10.0, and flew 107 percent of the planned number of flights (583 flown, compared to 543 planned).
- Mission systems testing focused on:
  - Completing Block 3F mission systems development, testing, and deficiency corrections.
  - Completing weapons separation and integration, and testing for the remaining Block 3F weapons, including the Small Diameter Bomb version I, U.S. Navy Joint Standoff Weapon, version C1 (JSOW-C1), UK Paveway IV bomb and Advanced Short-Range Air-to-Air Missile (ASRAAM).
  - Testing of an organic light-emitting diode (OLED) prototype of the Gen III Helmet Mounted Display System (HMDS), designed to correct excessive "green glow" during night carrier operations.
- The program jumped ahead in the DT Joint Test Plan and conducted many complex missions at the Nevada Test and Training Range to quickly assess each new version of Block 3F software and sign off as many capabilities as possible without doing all the planned and necessary build-up testing.

• Mission Systems Assessment
- Delays in starting Block 3F testing in 2015, pausing to redo Block 3i work in 2016, and the immaturity of the Block 3F software delivered to flight test caused the program to continue to fall behind schedule in 2017. The program cut many test points in an attempt to finish mission systems flight test in 2017. However, due to continued discoveries and delays, DOT&E estimates Block 3F development and flight testing will likely not finish prior to February 2018. This estimate is based on the JPO's estimates and its intent to close out SDD, transition to C2D2, get to IOT&E, and start full-rate production.
- Substantial risks are associated with the program's plan to complete SDD and transition to C2D2.
  - As of late October 2017, there have been 31 versions of Block 3F software as the program works to address key deficiencies. However, the program is using test point data from older versions of software to sign off capability specifications and justify baseline test point deletions, even though the old data may no longer be representative of the latest version of Block 3F software.
  - The program's testing, which skipped some of the planned and necessary build-up testing to sign off capabilities, created a shortfall of necessary test data and proved to be inefficient.
    - » While this method allowed the program to quickly sample key capabilities, the more thorough build-up testing of each capability may not have been conducted.
    - » The limited availability and high cost of range periods, combined with high re-fly rates for test missions completed on the Nevada Test and Training Range, make it difficult for the program to efficiently conduct this testing.
    - » The complex mission scenarios are some of the most difficult test points to execute (i.e., full Block 3F capabilities and flight envelope). This course of action adds risk if the JPO does not properly execute and close out SDD with applicable data, sufficient analytical rigor, and statistical confidence. This would likely result in problem discoveries in IOT&E that may require additional corrections and FOT&E.
  - Finally and most importantly, the program will likely deliver Block 3F to the field with shortfalls in capabilities the F-35 needs in combat against current threats.
- The program planned to provide full Block 3F capability, as defined in program schedules and the Test and Evaluation Master Plan (TEMP), with the first Lot 10 aircraft delivery in January 2018. As required by the National Defense Authorization Act (NDAA) for FY16, the Secretary of the Air Force certified to Congress in September 2016 that these aircraft will have full combat capability, as determined as of the date of the enactment of the NDAA, with Block 3F hardware, software, and weapons carriage. Although the program made good progress in CY17 and will deliver Lot 10 F-35A aircraft in early CY18 with Block 3F hardware, software, and a flight

clearance for carrying weapons, these aircraft will not yet have the full planned Block 3F capability due to the following shortfalls:

- Envelope limitations may restrict carriage and employment of the planned Block 3F missiles, bombs, and gun well into 2018, if not later.
- A set of five mission data loads (MDLs) is required to be built for the final version of Block 3F; each of these MDLs is optimized for a geographically specific area of responsibility (AOR) around the world, including one MDL designed for operational testing and training in the United States. The MDL for operational testing and training is scheduled to be delivered in July 2018 to support Block 3F IOT&E. However, the full set of MDLs required for real-world operations will not be completely developed, tested, and verified until the end of 2019. One of the remaining four is scheduled for release in December 2018, a second in May 2019, and the final two in November and December 2019, presuming the current schedule holds. This extended timeline is due to ongoing delays with Block 3F and the program's failure to provide the necessary equipment and adequate software tools for the U.S. Reprogramming Laboratory (USRL).
- Even after delivery, the initial set of MDLs will not be fully tested and optimized to deal with the full set of threats present in operational test, let alone in actual combat.
- As of late October 2017, the program had 263 Block 3F unresolved high-priority (Priority 1 and Priority 2) performance deficiencies, the majority of which cannot be addressed and verified prior to the Lot 10 aircraft deliveries, with only 88 of these 301 deficiencies being actively worked.
- The program has many known and acknowledged failures to meet the contract specification requirements. The program intends to seek relief from the SDD contract due to the lack of time and funding remaining.
- The JPO projects that dozens of contract specifications and requirements will be open or unmet going into FY18.
- The program estimates Block 3F mission systems testing will extend into early 2018, confirming estimates by DOT&E and the Office of Cost Assessment and Program Evaluation (CAPE) that delivery of full capability in January 2018 is not possible.
- The developmental and operational test teams continue to discover deficiencies and will discover more before and during IOT&E.
- ALIS version 3.0 is necessary to provide full combat capability. However, the program will likely not field ALIS 3.0 until early 2018 due to delays with ALIS 2.0.2.4. The program deferred to ALIS 4.0 capabilities previously designated for ALIS 3.0. ALIS 4.0 is scheduled for release in late 2018, but this schedule is high risk. Newer versions of ALIS software fielded during IOT&E will be evaluated, if possible.
- Finally, IOT&E, which provides the most credible means to predict combat performance, likely will not be completed until the end of 2019, at which point over 600 aircraft will already have been built.
- DOT&E assesses the proposed C2D2 plan is not executable for several reasons:
  - DT resources are insufficient, lacking enough test aircraft and software integration labs for each F-35 configuration, and adequate time for flight test.
  - The proposed rigid 6-month software cycle timeline does not align with required updates to ALIS, mission data, technical orders, training courseware and simulators, airworthiness envelope releases, and modifications for new hardware and weapons, which typically take longer to field.
  - It is unclear how a software production cycle of 6 months will merge with a fielding cycle that is currently 2-3 years on other aircraft, such as the F/A-18 and F-22.

Static Structural and Durability Testing

- Structural durability testing activity
  - Testing of the F-35A and F-35C ground test articles (AJ-1 and CJ-1, respectively) continued into their third lifetime – one lifetime is 8,000 equivalent flight hours (EFH). The JPO suspended testing of the F-35B ground test article (BH-1) after completing only the second lifetime of testing in February 2017.
  - The F-35A durability test article began the third lifetime of testing on March 11, 2016, and completed in October 2017. The test article is currently in teardown and analysis.
  - The F-35B durability test article completed the second lifetime of testing on February 1, 2017. Due to the significant amount of modifications and repairs to bulkheads and other structures, the program declared the F-35B ground test article was no longer representative of the production aircraft, so the JPO deemed it inadequate for further testing. On February 17, 2017, the program canceled the testing of the third lifetime with BH-1 and made plans to procure another ground test article, but has not yet done so.
  - The F-35C durability test article completed the second lifetime of testing (16,000 EFH) on October 29, 2016. The testing for the third lifetime began on April 4, 2017, and reached 17,606 EFH as of August 8, 2017. The JPO projects that lifetime testing on CJ-1 will be completed by December 2018.
- Structural durability testing assessment
  - For all variants, this testing led to discoveries requiring repairs and modifications to production designs and retrofits to fielded aircraft.

- To date, the JPO has not funded or put on contract a new ground test article. The program should complete contract actions for another F-35B ground test article as soon as possible to begin additional durability testing.
- The effect of the discoveries and failures during testing on the service life certification of the F-35B is yet to be determined. It may be less than the planned 8,000 hours designed for all variants, even with extensive modifications to strengthen the aircraft.

Mission Data Load Development and Testing

- F-35 effectiveness in combat relies on MDLs, which are compilations of the mission data files (MDFs) needed for operation of the sensors and other mission systems. The MDLs work in conjunction with the avionics software and hardware to drive sensor search parameters so that the F-35 can identify and correlate sensor detections, such as threat and friendly radar signals.
  - The contractor team produces an initial set of MDFs for each software version to support DT during SDD.
  - The USRL creates, tests, and verifies operational MDLs – one for operational test and training, plus one for each potential major geographic area of operation. Operational test aircraft and fielded aircraft use the USRL-generated MDLs.
- The testing of the USRL MDLs is an operational test activity, as arranged by the JPO after the program restructure that occurred in 2010, and consists of laboratory as well as flight testing on OT aircraft.
- Because MDLs are essential software components of F-35 mission capability, the Department must have a reprogramming lab that is capable of rapidly creating, testing, and optimizing MDLs, as well as verifying their functionality under stressing conditions representative of real-world scenarios. This is necessary to support the proper functioning of F-35 mission systems and the aircraft's operational effectiveness in IOT&E, training, and combat. The reprogramming lab must also be able to rapidly modify existing MDLs when intelligence data changes, but this capability has not yet been achieved.
- Although the USRL has the capability to create functioning MDLs for Block 3F and earlier blocks, it does not have a sufficient number of radio frequency (RF) signal generators, which are used to stimulate the F-35 Electronic Warfare (EW) system and the EW functions of the radar, nor are the signal generators able to test and optimize the MDLs under conditions stressing enough to ensure adequate performance against current and future threats.
  - The current reprogramming hardware and software tools are cumbersome, requiring several months for the USRL to create, test, optimize, and verify a new MDL; a time period that delays getting MDLs to operational units. The USRL began creating Block 3F MDFs in the summer of 2017; it will take approximately 12-15 months to deliver the first verified MDL for IOT&E and for fielded Block 3F aircraft. The USRL will then release verified MDLs for the remaining areas of responsibility at approximately 3-month intervals.
- The JPO and Lockheed Martin have yet to complete necessary funding and contracting actions to fully address shortfalls in signal generation capability within the USRL.
  - The Department clearly identified the need for improved USRL capabilities in 2012 and programmed $45 Million in the FY14-15 budgets to address the need.
  - The JPO sponsored a gap analysis study of USRL capabilities, completed in 2014, to determine the lab upgrade requirements at the engineering level before beginning contracting actions. The study concluded that the USRL would need between 16 and 20 upgraded RF signal generator channels for each of the USRL's two test lines, in order to adequately create and test MDFs for the fielded threats examined in the study, using realistic scenarios and threat densities.
  - After considering upgrade proposals from Lockheed Martin, the USRL recently elected to procure eight new RF signal generator systems known as Advanced Pulse Generators (APGs) for each of two USRL test lines, directly from the APG vendor. The USRL recently contracted with the vendor for their installation and checkout, expected to be competed in fall 2018, which will be late to need to support IOT&E. This is the only USRL upgrade that is funded. The installation was delayed until the JPO placed Lockheed Martin on contract in November 2017 to conduct the security certification, accreditation, and configuration management processes necessary to obtain authority to operate in the new, upgraded configuration. Even when this interim upgrade is complete, the USRL will still not have enough signal generators to simulate a realistic threat laydown with multiple modern surface-to-air missile threats and the supporting air defense system radars that make up the signal background in the laydown.
- The program began delivering production aircraft in the Block 3F configuration in September 2017. These aircraft are being delivered with a previous version of Block 3F software and an early, partially tested, and unverified MDL, resulting in an undetermined level of risk if used in combat prior to operational testing.
- To provide the necessary and adequate Block 3F mission data development capabilities for the USRL, the JPO must immediately fund and expedite the contracting actions for the necessary hardware and software modifications, including an adequate number of additional RF signal generator channels and the other required hardware and software tools. Although these actions are already late to need for Block 3F fielding and IOT&E, the capabilities are still urgently needed to support operational Block 3F aircraft.
- Significant additional investments are also required now to upgrade the USRL to support F-35 C2D2 MDL development.
  - The C2D2 plan includes new Technical Refresh 3 processors and other new hardware. Concurrency in development and production during SDD has resulted in

multiple fielded F-35 configurations that will continue to need to be supported long after the development program enters the C2D2 phase. During C2D2 the program will require the USRL, or an additional reprogramming lab, to have the capability to simultaneously create and test MDLs for different avionics hardware and software configurations, including not only whatever ones emerge from the various stages in C2D2 but also all prior active configurations. These different configurations include Technical Refresh 1 (Block 2B), Technical Refresh 2 for Block 3F, new electronic warfare equipment planned for C2D2, an improved display processor, and a new Technical Refresh 3 open avionics architecture for later increments in C2D2.
  - Although the C2D2 hardware upgrades for the USRL should already be on contract, the reprogramming requirements for C2D2 have yet to be fully defined. According to a study conducted by Lockheed Martin, three of the Block 4 capabilities will affect at least one of the models used in the reprogramming laboratory. The JPO must expeditiously undertake the development of those requirements and plan for adequate time and resources in order to ensure the USRL is able to meet C2D2 and MDL requirements.
- As part of IOT&E, the USRL will complete an "Urgent Reprogramming Exercise (URE)." This will evaluate the ability of the USRL, with its hardware and software tools, to respond to an urgent request from a Service to modify the mission data in response to a new threat or new mode of an existing threat.
  - During a URE at the USRL in 2016, the total hours recorded were double the Air Force standard for rapidly reprogramming a mature system. The JOTT identified several key process problems, including the lack of necessary hardware, analysis tools that were not built for operational use, and missing capabilities, such as the ability to quickly determine ambiguities in the mission data.
  - The JPO must correct these problems in order to bring the ability of the USRL to react to new threats up to the identified standards routinely achieved on legacy aircraft. However, the problems will not be addressed by the time IOT&E is projected to start in late CY18.
- In addition to resolving the deficiencies described above, involving overall laboratory capabilities, and the deficiencies in the tools used to develop MDLs, the program must also properly sustain the USRL to ensure a high state of readiness, particularly if the Services have an urgent reprogramming requirement, which could happen at any time for the fielded aircraft. To meet these tasks, the USRL must have all necessary equipment in a functioning status, similar to aircraft availability, which will require a sufficient number of Field Service Engineers (FSE) to assist in maintenance and operation of the lab equipment, and adequate training for laboratory personnel. Also, the USRL requires adequate technical data for lab equipment and enough spare parts and/or supply priority to quickly repair key components.

Weapons Integration and Demonstration Events

Block 3F Weapons Delivery Accuracy and Weapons Integration and Certification

- Activity
  - The table below depicts DT Weapons Delivery Accuracy (WDA) events for Block 3F weapons integration, including those accomplished during this reporting period. The JSF weapons team plans to complete the remaining gun events by the end of CY17.
  - Each WDA event has an overall assessment rating for meeting the weapons integration success criteria to verify compliance with the JSF contract specification.
    - Prerequisite engineering and characterization missions continued to discover deficiencies with mission systems software and hardware for all weapon types.
    - These discoveries of deficiencies in the fire control thread and fusion functionality, as well as the corresponding correction to deficiencies and fix verification, were the pacing items for accomplishment of the weapons events.
  - As shown in the event table, multiple versions of Block 3F software have been required to complete the events, with many created specifically to address deficiencies preventing the next event from proceeding.
  - Most of the AMRAAM events were completed using work-arounds to mitigate limitations induced by outstanding deficiencies that compromised the combat capability of the weapons employment. The JPO, contractor, Services, and JOTT are assessing these weapons integration deficiencies so that problems can be addressed prior to entry into IOT&E and subsequent fielding.
  - Detailed descriptions of technical and weapons employment problems, along with corresponding fixes required to ensure combat performance, are classified.
  - The JPO is also pursuing a structured, combined developmental and operational test strategy for the GBU-49 variant of Raytheon's PaveWay series of bombs.
    - The JPO agreed to integrate the GBU-49 weapon into Block 3F as requested and funded by the Air Force. This additional weapon integration on the F-35A is intended to provide the combat air forces with a more robust moving ground target kill capability.
    - The JPO will include this weapon as an update to the SDD requirement for GBU-12 integration and performance.
    - At the time of this report, the test center had performed one initial captive carry flight to verify safe integration and assess the controls and displays to the pilot. The JOTT, in conjunction with the 53rd Wing at Nellis AFB, is planning six additional GBU-49 weapons delivery events to confirm functionality and weapons integration. The JOTT will augment this by flying a number of IOT&E profiles and weapons events to sufficiently demonstrate and evaluate the operational capability in the IOT&E weapons delivery events.

BLOCK 3F WEAPONS DELIVERY ACCURACY (WDA) EVENTS				
WDA Event	**Weapon(s)**	**Mission Systems Software**	**Date Accomplished**	**Summary Assessment**
105	AMRAAM	3FR6.21	Jul 17	Successful
301	AMRAAM	3FR5.03	Jul 16	Successful
302	AMRAAM+AIM-9X	3FR5.03	Jul 16	Successful
303	AMRAAM	3FR5.03	Aug 16	Partially Successful
306	2 X AMRAAM	3FR6.21	Aug 17	Successful
307	2 X AMRAAM	3FR5.03	Aug 16	Partially Successful
308	AMRAAM + SDB	3FR5.06	Nov 16	Successful
309	2 X AMRAAM	3FR6.21	Jul 17	Successful
311	2 X AMRAAM	3FR5.03	Jul 16	Unsuccessful
314	UK ASRAAM	3FR6.12	Jun 17	Analysis in Progress
315	UK ASRAAM	3FR6.01	Feb 17	Analysis in Progress
316	AIM-9X	3FR5.03	Jul 16	Successful
317	AIM-9X	3FR5.03	Aug 16	Successful
318	AIM-9X BLOCK 2	3FR5.06	Dec 16	Successful
319	GBU-12	3FR6.11	Mar 17	Successful
320	GBU-31	3FR5.03	Jul 16	Successful
321	GBU-31	3FR5.03	Jul 16	Successful
322	2 X GBU-31	3FR5.03	Aug 16	Successful
323	4 X GBU-39	3FR5.05	Oct 16	Successful
324	2 X GBU-39	3FR5.03	Aug 16	Successful
325	SDB	3FR5.03	Jul 16	Successful
327	JSOW	3FR6.22	Oct 17	Successful
328	UK PW-4	3FR5.05	Oct 16	Successful
329	2 X UK PW-4	3FR6.01	Mar 17	Successful
330	A/A GUNNERY	3FR6.22	In Progress	*See note below
331	A/S GUNNERY	3FR6.22	Oct 17	*See note below
332	A/S GUNNERY	3FR6.22	Oct 17	*See note below
333	A/S GUNNERY	3FR6.22	In Progress	*See note below
334	NIGHT GUNFIRE	3FR6.3	In Progress	*See note below

* Flight testing of the different gun systems on the F-35 (internal gun for F-35A and external gun pods for the F-35B and F-35C) revealed problems with effectiveness, accuracy, pilot controls, and gunsights displayed in the Helmet Mounted Display System (HMDS). The synopsis and assessment of specific HMDS problems are classified. The gun profiles include the testing and qualification of four separate 25 mm rounds in the two gun types. The F-35A internal gun testing includes the PGU-23 training round, PGU-47 Armor Piercing High Explosive Incendiary round, and the PGU-48 Frangible Armor Piercing round. The F-35B and the F-35C variants external gun pod testing is limited to the PGU-32 Semi-Armor Piercing High Explosive Incendiary round used by the Marine Corps.

- Assessment
  - The JOTT is assessing three events as candidates to be repeated with additional follow-on OT shots.
    - Events WDA-303 and WDA-307 were partially successful due to control room work-arounds that compromised the operationally representative profiles necessary to support later-planned IOT&E weapons delivery events.
    - Event WDA-311 was unsuccessful due to the combination of weapon performance and the inability of the F-35 to effectively employ the weapon in the planned scenario.
  - The WDA events also provide much of the evidence needed for operational weapons flight clearance certifications.
    - The initial plan for weapons integration and operational stores certifications involved conducting the WDAs on the early Block 3F software versions. The data analyses and certification processes are extensive and lead to a recommendation from the weapon vendors and Lockheed Martin to the Service's flight clearance authorities. Successful tests and analyses would have endorsed the specific weapon and suspension and release equipment for the operational stores certifications that

are required for the military flight release for fielding and IOT&E.
  - Due to limited or problematic test data, the weapon vendors and Service flight clearance authorities have determined that the expected flight clearances for full carriage and employment of the F-35 Block 3F weapons suite may have significant limitations.
  - The JPO is reviewing the problems that may require limitations in the flight clearance. The JOTT will evaluate the effects of potential restrictions to the weapon carriage and release envelopes, including limitations on flight hours and stores combinations. As the technical details and effects of these problems unfold, DOT&E will monitor and assess how any limitations may affect the adequacy of planned IOT&E profiles and the performance of the F-35 in IOT&E and in combat.

Gun Testing

- Gun Activity
  - All three F-35 variants add gun capability with Block 3F. The F-35A gun is internal; the F-35B and F-35C each use an external gun pod. Differences in the outer mold-line fairing mounting make the gun pods unique to a specific variant (i.e., an F-35B gun pod cannot be mounted on an F-35C aircraft).
  - AF-31, the only Block 3F mission systems-capable F-35A test aircraft configured for gun testing, completed the first air-to-ground gun firing at Naval Air Weapons Station (NAWS) China Lake, California, in February 2017.
    - Helmet Mounted Display System (HMDS) alignment problems identified during the test event prevented further weapons demonstration activities with the gun until corrections were developed and tested. The test team accomplished a risk reduction test flight in March while awaiting resolution of the HMDS alignment and line-of-sight problems.
    - AF-31 completed an air-to-ground live fire accuracy event on September 27, 2017, and a gun lethality mission on October 5. Additional testing was ongoing at the time of this report.
  - BF-1 completed the first F-35B airborne gun firing on February 21, 2017. BF-1 then attempted more gun testing in March, but gun pod problems, weather, and range availability prevented the completion of the initial set of scheduled events.
    - BF-1 resumed testing in April, but gun pod seal problems and cracks at the FS 346.5 frame further delayed testing. BF-1 completed airborne gun firing in May to complete the flight sciences testing of the gun pod on the F-35B.
    - BF-17, the only Block 3F mission systems-capable test aircraft configured for gun accuracy testing, completed a gun lethality mission on September 12, 2017.
  - CF-3 performed the first F-35C airborne gun firing on June 6, 2017, and continued more gun testing throughout the month. It completed flight sciences testing with the gun pod in July.
- Gun Assessment
  - F-35A gun accuracy testing on AF-31 demonstrated uncharacterized bias toward long and right of the target. Also, the gunsight display in the HMDS was cluttered and slow to stabilize.
  - The initial F-35B strafing results with the gun pod have been better than those for the F-35A. The aim-point projection through the HMDS was more stable and the F-35B does not appear to have significant angular bias errors like the F-35A. The program will complete accuracy assessments; however, because the program used just a single aircraft per variant to assess compliance with specification requirements, the JPO will make more assessments with OT aircraft before and during IOT&E.
  - F-35C accuracy results with the gun pod to date have been consistent with those observed with the F-35B.
  - The JOTT and the Services will need to develop shot-kill criteria, possibly for each variant, to assess the effectiveness of simulated gun employment during training and test mission trials in IOT&E. Ongoing delays in completing the remaining gun testing and correcting gun-related deficiencies within SDD, especially for the F-35A, are adding risk to the IOT&E schedule.

Air-to-Ground Weapons Demonstration Events

- Air-to-Ground Weapons Activity
  - In 2016, the JOTT and the associated Service OT squadrons conducted 18 GBU-31 and GBU-32 Joint Direct Attack Munition (JDAM) weapon demonstration events (WDEs) and 28 GBU-12 laser guided bomb (LGB) WDEs on range complexes at NAWS China Lake and MCAS Yuma. The number of events accomplished exceeded the number of planned events. A summary of the events appears in the following table.
  - The JOTT planned all of the WDEs as part of operationally representative scenarios constructed to characterize the radial miss distance of air-to-ground weapons employed by the F-35 and to identify any problems in completing the find, fix, track, target, engage, and assess kill chain.
    - Aircraft were loaded with either Block 2BS5.2 or 2BS5.3 (the final Block 2B software).
    - Scenarios included a representative mix of target cueing via voice communications, Variable Message Format (VMF) digital messages, and shoot-list sharing via Multifunction Advanced Data Link (MADL).
    - LGB target designation was performed via self-lasing, airborne buddy-lasing, or lasing by the ground tactical control party. JDAM targeting was accomplished with coordinates generated either by the Electro-Optical Targeting System (EOTS) laser or a synthetic aperture radar (SAR) map.
  - Twenty-two of 28 LGB events and 15 of 18 JDAM events were valid for scoring miss distance. Invalid events include those in which the weapon failed, the scenario was

Weapon Type		Events Planned	Events Conducted					Events Valid for Scoring
			Total	Inert/Live		Variant		
				Inert	Live	F-35A	F-35B	
LGB	GBU-12	16	28	25	3	21	7	22
JDAM	GBU-31	8	15	7	8	15	0	13
	GBU-32	4	3	3	0	0	3	2

not operationally representative (i.e., range restrictions precluded accurate execution of a scenario), or mission systems problems disrupted the kill chain (i.e., a failure to generate target coordinates for JDAM employment or the laser designation wandered off the target during LGB employment). The invalid events for accuracy scoring still provided opportunities to identify kill chain problems.

- Air-to-Ground Weapons Assessment
  - The radial miss distance of these air-to-ground weapons when delivered by the F-35 is consistent with that of legacy platforms. Specific details are classified.
  - Mission systems problems affected the delivery of air-to-ground weapons. A preliminary assessment of these problems appeared in the FY16 Annual Report. Additional details appear below.
  - The Dynamic Launch Zone (DLZ), the aircraft-generated indication of the JDAM launch acceptability region (LAR) in the cockpit, was not consistent with the shoot cue, an indication generated by the actual JDAM in-weapon LAR.
    - The DLZ is based on an outdated LAR model.
    - The DLZ consistently reported being in-range (i.e., that the bomb could reach the target) or in-zone (i.e., that the bomb could reach the target and achieve pilot selected impact conditions) at a greater range than the shoot cue. It also disagreed with the shoot cue at weapon release in 7 of 17 WDEs.
  - The F-35 Block 2B cockpit displays did not allow the pilot to confirm the coordinates passed to the JDAM. The inability to confirm coordinates reduced pilot and ground controller confidence in weapon steering and contributed to the employment of two weapons on the wrong targets during the demonstration events.
    - Rules of engagement in operational areas sometimes require that pilots confirm the coordinates to the ground controller before receiving clearance to drop weapons.
    - For Block 3F, the pilot is now able to see what coordinates are sent to the bomb, but is still not able to see what coordinates are actually loaded in the bomb. The Services are assessing if this correction meets the requirements directed by the rules of engagement in specific areas of operation.
  - The EOTS presented several problems during the air-to-ground WDEs.
    - The EOTS slews rapidly and erratically when passing through the gimbal limit directly out the bottom of the aircraft. During this time, there is a period of seeker de-rotation along the aircraft flight path in which the EOTS cannot be controlled, leading to loss of target track during critical portions of the kill chain, including weapons employment, dive recovery, and battle damage assessment. Even though the pilots were trained to avoid the limit, the problem occurred during several of the WDEs and resulted in two failed attacks.
    - The responsiveness of the Cursor Slew Switch (CSS), which moves the cursor on the Panoramic Cockpit Display, precluded pilots from manually designating moving targets per Air Force tactics, techniques, and procedures.
    - EOTS point tracks were generally stable, but pilots observed cases in which the point track had difficulty differentiating between the target, background clutter, and the target shadow, causing track to occasionally transfer from moving targets to infrared-significant clutter.
    - The EOTS does not provide any lead-point-compute or lead-laser guidance to engage moving targets. The CSS slews the cursor at only one rate, regardless of the degree of displacement of the switch, and does not support manual moving target designation. To engage moving targets, pilots were forced to use simple rules of thumb which may not be effective or allowable in combat, depending on the rules of engagement and the target's speed.
  - Failures of the Fuselage Remote Interface Unit (FRIU), which provides the interface between the aircraft avionics and weapons stations, frequently disrupted missions.
    - If an FRIU failure occurs during an attack, pilots must reset the FRIU to clear the fault and regain communications with the weapon, and then re-attack the target. Several FRIU failures occurred during the WDEs and required minutes-long resets of the Integrated Core Processor.
    - The program has addressed these FRIU failures and recent weapons events demonstrated improved FRIU reliability.
  - Pilots frequently chose to manually enter mission planning data in the cockpit, versus using the Offboard Mission Support workstation, due to the excessive time required to transfer the data from the Portable Memory Device to the aircraft.
    - Manual entry is prone to error and led to inappropriate or incorrect radar mode presets, weapon overlays, steerpoints, sequences, pre-planned target coordinates, communication presets, Link 16 and MADL

assignments, and weapon and fuze settings during WDEs.
  - Although the program has improved load times with updated transfer devices, Portable Memory Device loading still takes too long and is often problematic.
- The lack of a video datalink or the capability to automatically compute a time-on-target (TOT) degrades the close air support (CAS) mission.
  - The lack of a video datalink required pilots to correlate targets with ground controllers via voice communications, extending the time required for targeting during CAS missions. The poor fidelity of EOTS video further extended the targeting time.
  - The lack of automatic TOT computation increased pilot workload, compared to legacy aircraft. Because pilots had to manually calculate TOTs during the CAS engagements, ground controllers either requested attacks with a time window for weapon impact or an immediate attack with no specified TOT in the majority of events. Of the five events in which a precise TOT was coordinated, two occurred more than 30 seconds from the acknowledged TOT; these attacks would have been aborted doctrinally.
  - The inability to calculate a TOT limits the ability of the F-35 to participate in complex combined arms environment. The program developed a fix to allow the pilot to compute a TOT, but as of the writing of this report, it has not been tested.

Air-to-Air Weapons Demonstration Events

- Air-to-Air Weapons Activity
  - The JOTT, with the Air Force 53rd Wing and the Marine Corps VMX-1 OT flying units, used the range complex over the Gulf of Mexico at Eglin AFB, Florida, to evaluate the ability of Block 2B and Block 3i aircraft to employ the AIM-120 Advanced Medium Range Air-to-Air (AMRAAM) missile in operationally representative scenarios.
    - These scenarios were designed to evaluate the ability of the F-35A and F-35B to accurately find and identify the target, track and engage a simulated hostile aircraft, and support the missile to a kill.
    - The Air Force supported the effort with six F-35A aircraft configured with IOC Block 3iR6.01 mission systems software. The Marine Corps supported the effort with three F-35B aircraft configured with IOC Block 2BS5.3 mission systems software. Both of these mission systems software versions reflected the Service's initial fielding configuration and capabilities.
  - The effort consisted of two CY16 deployment periods: the Air Force deployed in May 2016 and the Marine Corps deployed in August 2016.
    - The two units employed a total of six AIM-120 missiles at the Gulf Test and Training Range Complex against full-scale and sub-scale drone targets simulating combat configurations and flight profiles. These missile shots supported the JOTT test requirements as approved by DOT&E and the combat unit tactics development to support IOC fielding for both Services.
    - The deploying units used the initial deployment quick-look information to update and refine tactics development.
    - Technical problems with validation of the telemetry data stream delayed until 2017 the delivery of missile data required for detailed analysis. Once the technical data problems were resolved, the JOTT performed the required detailed analysis to evaluate the missile shots.
  - The six missile shots supported five OT events. The Marine Corps unit fired one of those missile shots against a specific target profile required by the Marine Corps for initial F-35 tactics development. All six shots were accomplished per the DOT&E-approved test plan and the combat scenarios used the most current tactics as outlined in the applicable tactics manuals. This initial set of OT events yielded tactics observations and identification of key technical deficiencies in the ability of the F-35 to employ the AIM-120 weapons.
- Air-to-Air Weapons Assessment
  - The assessment revealed several problems with the employment of air-to-air missiles in the Block 2B and Block 3i configurations. The test team discovered several classified missile integration problems as well as pilot-identified deficiencies with the controls and displays that affected the combat capability of the F-35 to support the kill chain. The teams also identified problems with the off-board mission planning and debriefing system that hindered effective planning and timely debriefing.
  - The test teams documented these problems in deficiency reports and submitted them via the monthly deficiency review board at the Edwards Integrated Test Force.

LFT&E

F-35 Ballistic Testing and Vulnerability Analyses

- In mid-FY17, the F-35 LFT&E program completed its final ballistic vulnerability test series at the Weapons Survivability Laboratory, NAWS China Lake, California, using the F-35C full-scale structural test article.
  - These tests demonstrated the structural tolerance of the F-35C against realistic ballistic threats, but also showed the probability of threat-induced fires was greater than previously anticipated. Consequently, the JPO revised the fire predictions used in its final analysis of F-35 ballistic threat vulnerability.
  - This test series completed the testing defined under the DOT&E-approved LFT&E Alternative Test Plan that provides the information needed to assess F-35 vulnerability to the prescribed threats.
- Lockheed Martin completed final ballistic vulnerability analyses for all three F-35 variants against four likely threats. DOT&E is in the process of evaluating the results to assess F-35 vulnerabilities.

- The Lockheed Martin assessment compares F-35 vulnerabilities against two sets of requirements: the JSF contract specifications and the JSF ORD.
  - All three F-35 variants met JSF contract specifications in the Prevent Pilot Escape (i.e., damage or injury that prevents ejection) category for three of the four threats. No variant met the Prevent Pilot Escape requirements against one of the threats.
  - For their ability to sustain damage and return to the Forward Line of Troops (FLOT), the F-35A and the F-35C met requirements against two of the four threats (one type of missile warhead fragment and Man-Portable Air Defense System (MANPADS) missiles). No variant met the Return-to-FLOT requirements against two of the threats. The F-35B did not meet the Return-to-FLOT requirements against three of the threats.
  - In comparing against the F-16C in similar configurations, all variants of the F-35 were better than the F-16 in the Prevent Pilot Escape and Return-to-FLOT categories for three of the four threats. None of the F-35 variants could meet the requirements against the fourth threat in either category, nor could the F-16.

Vulnerability to Unconventional Threats

- The full-up, system-level chemical-biological decontamination test on BF-40, a low-rate initial production (LRIP) F-35B aircraft, demonstrated the efficacy of the Hot Air Decontamination equipment and processes. Additional developmental work is required to field an operational decontamination capability. A 2QFY16 event demonstrated that a modified system process and a better insulated shelter could maintain adequate temperature and humidity control inside the shelter, even in a cold-weather environment.
- The program test plan to assess chemical and biological decontamination of pilot protective equipment remains inadequate.
  - Compatibility testing of protective ensembles and masks showed that the materials survive exposure to chemical agents and decontamination materials and processes, but the program has neither tested nor provided plans for testing the fielded Gen III and Gen III Lite versions of HMDS.
  - Gen II HMDS compatibility analysis compared HMDS materials with those in an extensive DOD aerospace materials database. The program plans similar analysis for the Gen III HMDS design. Even if the program understands the material compatibilities, it does not plan to demonstrate a process that could adequately decontaminate either HMDS from chemical and biological agents.
- The Navy evaluated an F-35B against the electromagnetic pulse threat level defined in Military Standard 2169B, but the data and report have not yet been provided to DOT&E. Follow-on tests on other variants of the aircraft, including a test series to evaluate any Block 3F hardware or software changes, are ongoing.

Gun Ammunition Lethality and Vulnerability

- The 780th Test Squadron at Eglin AFB, Florida, completed ground-based lethality tests of three 25 mm gun round variants against armored and technical vehicles, aircraft, and personnel-in-the-open targets. The rounds tested were:
  - PGU-32/U Semi-Armor Piercing High Explosive Incendiary
  - PGU-47/U Armor Piercing High Explosive Incendiary with Tracer (APEX)
  - PGU-48/B Frangible Armor Piercing
- Ground-based lethality tests for the APEX round correlated well with pre-test predictions for round penetrations, but the 780th Test Squadron discovered potential problems with fuze functioning when impacting rolled homogeneous armor at high obliquity.
  - Nammo, the Norwegian manufacturer, conducted additional testing to identify the cause of the dudded rounds during the ground tests and subsequently modified the fuze design to increase reliability.
  - DOT&E will include the effect of the ground-based lethality test data in the ammunition lethality assessment. No additional testing will be conducted.
- The weapons integration characterization of the gun and sight systems for the air-to-ground gun strafe lethality tests commenced in September 2017 and is ongoing at the Naval Air Warfare Center Weapons Division (NAWCWD) at NAWS China Lake. Strafe targets include small boats, light armored vehicles, technical vehicles (pickup trucks), and plywood manikins for each round type tested (similar to targets used in ground-based lethality tests).

Operational Suitability

Activity

- The program continued to deliver aircraft to the U.S. Services and international partners throughout CY17 in production Lot 9. As of the end of September, 235 operational aircraft had been delivered to the U.S. Services and international partners, and assigned to units. These aircraft are in addition to the 14 aircraft dedicated to developmental testing.
- As of the end of September, the U.S. fleet of F-35s accumulated 80,815.5 flight hours
- The following assessment of operational suitability is based on sets of data collected from the operational and test units and provided by the JPO. The assessment of aircraft availability is based on data provided through the end September 2017. Reliability and maintainability assessments in this report are based on data covering the 12-month period ending May 31, 2017. Data for reliability and maintainability include the records of all maintenance activity and undergo an adjudication process by the government and contractor teams, a process which creates a lag in publishing those data. The variety of data sources and processes are the reasons the data have different dates and appear to be delayed.

Assessment

The operational suitability of the F-35 fleet remains at a level below Service expectations and is dependent on work-arounds that would not be acceptable in combat situations. Over the previous year, most suitability metrics have remained nearly the same or moved only within narrow bands, which are insufficient to characterize a trend of performance.

Overall fleet-wide monthly availability rates remain around 50 percent, a condition that has existed with no significant improvement since October 2014, despite the increasing number of new aircraft. One notable trend, however, is an increase in the percentage of the fleet that cannot fly while awaiting replacement parts – indicated by the Not Mission Capable due to Supply (NMC-S) rate – for the entire fleet. The increase in the NMC-S rate is due to inadequate supply support. Concurrency of production and development, lower-than-expected reliability for parts, inadequate fault isolation, and early program decisions to not adequately fund procurement of spares have contributed to the increased NMC-S rate.

Reliability growth has stagnated, as reported in the FY16 DOT&E Annual Report. It is highly unlikely that the program will achieve the ORD threshold requirements at maturity for the majority of reliability metrics. Most notably, the program will likely not meet the Mean Flight Hours Between Critical Failures threshold without redesigning aircraft components, improving Prognostic Health Management (PHM) accuracy, or some combination of both.

- F-35 Fleet Availability. Aircraft availability is determined by measuring the percent of time individual aircraft are in an "available" status, aggregated monthly over a reporting period. The program-set availability goal is modest at 60 percent, and the fleet-wide availability discussion below uses data from the 12-month period ending September 2017.
  - Availability is determined by measuring the combined non-availability rate across three status categories: Not Mission Capable for Maintenance (NMC-M), Depot (in the depot for modifications or repairs beyond the capability of unit-level squadrons), and NMC-S.
    - The average monthly NMC-M rate was 15 percent, compared to the goal of not more than 15 percent. The monthly NMC-M rate exhibited little trend up or down, indicating stable performance. The F-35B variant was down for maintenance more than the F-35A or F-35C, averaging an 18 percent NMC-M rate compared to a 13 percent rate for the F-35A and a 14 percent rate for the F-35C.
    - The average monthly Depot rate was 14 percent, compared to the goal of not more than 13 percent. The monthly Depot rate varied from as high as 24 percent to a low of 11 percent. The depots, along with depot-level repair teams sent to operating sites, repaired or modified the most aircraft in October 2016, largely driven by one-time repairs to faulty insulation of fuel lines on a select number of F-35A aircraft. After that period the depot rate stabilized in the low teens, ranging from 15 percent to 11 percent.
    - The average monthly NMC-S rate was 21 percent, compared to the goal of not more than 12 percent. The NMC-S rate was the primary driver of non-availability, ranging from 16 to 25 percent.
      - The NMC-S rate displayed a slight worsening trend over this period, never falling below 20 percent from February to September 2017, and reaching the highest value in the period of 25 percent in September 2017.
      - Several factors contribute to the high NMC-S rate.
        - Concurrency of production and development has caused the program to build a spares pool based on engineering assessments of reliability, vice actual failure data.
        - The program initially purchased spares to a 20 percent NMC-S rate estimate, which has proven to be optimistic.
        - The program has been late to stand up organic depot capabilities to repair existing parts that have failed but can be refurbished instead of being replaced with new parts, a capability that would reduce the strain on suppliers to produce more spare parts.
        - An immature PHM system (see PHM section later this report for more detail) detects failures which cause removal of parts which actually have not failed. However, these parts are sent back to the original equipment manufacturer and then returned to the supply chain as being "Re-Test OK" (RTOK). These actions add additional backlog to an already overloaded repair system.
  - The average monthly fleet availability rate was 50 percent. The availability rate ranged from 44 percent to 55 percent. Individual operating sites, particularly those with later lot aircraft, surpassed the 60 percent goal in select months over this period. At no point did the overall fleet, nor did the average of any specific variant persistently exceed 60 percent availability; although the F-35C variant surpassed 60 percent availability in three months, with a high of 70 percent in one of these 3 months.
    - This availability rate range was the same as reported in the FY16 DOT&E Annual Report, indicating a stable rate of availability with no trend of improvement.
    - Fleet availability has changed little over the past 3 years. The availability rate first reached 50 percent in October 2014 and has since achieved a maximum 56 percent on two separate occasions.
  - Variant-specific average monthly availability rates were relatively consistent for this period as well, at 51 percent for the F-35A, 46 percent for the F-35B, and 54 percent for the F-35C.
    - In previous reporting periods, F-35B availability was significantly lower than that of the F-35A and F-35C, largely due to a disproportionately high number of

F-35B aircraft going through depot modifications in order to support the Marine Corps declaration of IOC.
  - Starting late fall 2017, a disproportionately large number of F-35C aircraft are scheduled to receive depot modifications. As a result, that variant's monthly availability will likely fall significantly, relative to the other variants, through at least the winter to spring of 2018.
- The table below summarizes F-35 aircraft availability by operating site. The number of aircraft assigned at the end of the reporting period is an indicator of potential variance in availability.

F-35 AVAILABILITY FOR 12-MONTH PERIOD ENDING SEPTEMBER 2017 [1]

Operating Site	Average	Max	Min	Aircraft Assigned [2]
Whole Fleet	50%	55%	44%	235
Eglin F-35A	38%	49%	30%	25
Eglin F-35C	57%	69%	46%	12
Yuma F-35B	60%	70%	45%	10
Edwards F-35A	51%	70%	13%	8
Edwards F-35B	35%	58%	18%	7
Edwards F-35C	41%	73%	28%	7
Nellis F-35A	53%	67%	46%	16
Luke F-35A	50%	55%	44%	60
Beaufort F-35B	38%	52%	27%	28
Hill F-35A	70%	81%	22%	27
Amendola F-35A [3]	60%	80%	29%	4
Iwakuni F-35B [4]	58%	71%	42%	16
Lemoore F-35C [4]	54%	92%	18%	8
Nevatim F-35A [5]	45%	45%	45%	7

Footnotes
1. Data represent fielded aircraft and do not include SDD test aircraft.
2. Aircraft assigned at the end of September 2017.
3. Amendola F-35A operations began December 2016.
4. Iwakuni F-35B, and Lemoore F-35C operations began January 2017.
5. Nevatim F-35A operations began September 2017.

- To account for the performance of the aircraft that are in the field and not in Depot status, the program tracks Mission Capable (MC) and Fully Mission Capable (FMC) rates. The MC rate indicates the proportion of all fielded aircraft not in depot that are capable of flying at least one mission of the F-35 mission set, while the FMC rate reports the proportion that can fly all defined F-35 missions. Both the fleet-wide and variant-specific rates for MC and FMC appeared stable.
  - The average monthly MC rate was 58 percent, ranging from 56 to 64 percent, with the F-35A achieving 59 percent, the F-35B at 54 percent, and the F-35C at 63 percent.
  - The average monthly FMC rate was 26 percent, ranging from 21 to 31 percent. This was for a fleet almost entirely in the Block 2B/3i configuration; the fleet did not yet have any aircraft in the Block 3F "full warfighting" configuration. The F-35A FMC rate of 34 percent was significantly higher than other variants, with the F-35B at 14 percent and the F-35C at 15 percent.
- The average monthly utilization rate measures flight hours per aircraft per month. The utilization rate was 16.5 flight hours, reflecting the stable but low availability rate. The F-35A fleet averaged 18.0 flight hours, while the F-35B and F-35C fleets averaged 14.1 and 15.1, respectively.
  - The utilization rate has been relatively constant; the overall rate is similar to the average monthly utilization rate of 16.8 flight hours reported in the FY16 DOT&E Annual Report.
- The stagnant availability and utilization rates continue to prevent the Services from achieving their programmed fly rates, which are the basis of flying hour projections and sustainment cost models. As of April 3, 2017, the fleet had flown 72,019 hours. This amounted to 71 percent of the roughly estimated 100,800 hours from the original beddown plan the Services originally programmed for, or 84 percent of the most recent "modeled achievable" 85,882 flight hours.
- To help increase aircraft availability rates and reduce time waiting for spare parts, the program, in coordination with the Services, should stand up intermediate-level maintenance capability as soon as possible, particularly to support deployed aircraft and ship-borne operations.
- A separate analysis of availability of the OT-instrumented fleet, using data from the 12-month period ending September 2017, is important to consider as the program prepares for IOT&E. This analysis shows similar availability for the F-35A, but less availability for the F-35B and F-35C. The numbers below account only for the aircraft assigned to the OT fleet at the end of September 2017 (8 F-35A, 7 F-35B, 7 F-35C). There was little change in the availability trend of the F-35B and F-35C OT fleets.
  - The average monthly availability rate for F-35A OT aircraft was 51 percent, ranging from 13 to 70 percent. F-35A OT aircraft achieved or exceeded 60 percent availability at the beginning of the period. Availability declined precipitously from June 2017, reaching 13 percent in September 2017. This was primarily due to the Distributed Aperture Sensor (DAS) windows. The program established damage limits for the DAS windows in summer 2017, leading to closer inspections and a fleet-wide surge of demand for replacements for damaged windows. Although the aircraft with damaged windows are airworthy, they are not FMC. In fact, the Air Force does not report them as mission capable at all; but rather NMC-A, or Non-Mission Capable for Low Observable capabilities. Alternatively, the Department of the Navy reports such aircraft as PMC.
  - The average monthly availability rate for F-35B OT aircraft was 35 percent, ranging from 18 to 58 percent.

  - The average monthly availability rate for F-35C OT aircraft was 41 percent, ranging from 28 to 73 percent. Ongoing modifications of the F-35C fleet affected availability during this period.
  - Because the OT aircraft were produced in earlier production lots, they require many modifications to be production-representative of the Block 3F aircraft being delivered in Lot 9. Although later-lot aircraft have shown higher availability rates, they are still well below the planned 80 percent availability needed to efficiently execute IOT&E, especially for consistently launching variant-specific four-ship flights for many of the mission trials.
- F-35 Fleet Reliability
  - Aircraft reliability assessments include a variety of metrics, each characterizing a unique aspect of overall weapon system reliability.
    - Mean Flight Hours Between Critical Failure (MFHBCF) includes all failures that render the aircraft unsafe to fly, along with any equipment failures that would prevent the completion of a defined F-35 mission. It includes failures discovered in the air and on the ground.
    - Mean Flight Hours Between Removal (MFHBR) indicates the degree of necessary logistical support and is frequently used in determining associated costs. It includes any removal of an item from the aircraft for replacement. Not all removals are failures; some removed items are later determined to have not failed when tested at the repair site, and other components can be removed due to excessive signs of wear before a failure, such as worn tires.
    - Mean Flight Hours Between Maintenance Event Unscheduled (MFHBME_Unsch) is a reliability metric for evaluating maintenance workload due to unplanned maintenance. Maintenance events are either scheduled (e.g., inspections or planned part replacements) or unscheduled (e.g., failure remedies, troubleshooting, replacing worn parts such as tires). MFHBME_Unsch is an indicator of aircraft reliability and must meet the ORD requirement.
    - Mean Flight Hours Between Failure, Design Controllable (MFHBF_DC) includes failures of components due to design flaws under the purview of the contractor, such as the inability to withstand loads encountered in normal operation.
  - The F-35 program developed reliability growth projection curves for each variant throughout the development period as a function of accumulated flight hours. These projections compare observed reliability with target numbers to meet the threshold requirement at maturity (200,000 total F-35 fleet flight hours, made up of 75,000 flight hours each for the F-35A and F-35B, and 50,000 flight hours for the F-35C). As of May 31, 2017, the date of the most recent set of reliability data available, the fleet and each variant accumulated the following flight hours, with the percentage of the associated hour count at maturity indicated as well:
    - The complete F-35 fleet accumulated 86,233 flight hours, or 43 percent of its maturity value.
    - The F-35A accumulated 48,752 hours, or 65 percent of its maturity value.
    - The F-35B accumulated 26,374 hours, or 35 percent of its maturity value.
    - The F-35C accumulated 11,107 hours, or 22 percent of its maturity value.
  - The program reports reliability and maintainability metrics for the three most recent months of data. This rolling 3-month window dampens month-to-month variability while providing a short enough period to distinguish current trends.
  - The following tables for MFHBCF, MFHBR, MFHBME_Unsch, and MFHBF_DC compare the most recently reported and projected interim goal values with associated flight hours. July 2016 values (used in the FY16 DOT&E Annual Report) are included for reference. The tables also include projected values for each ORD metric at maturity, based on updated reliability growth analyses through May 2017.

F-35 RELIABILITY: MFHBCF (HOURS)

Variant	ORD Threshold		Values as of May 31, 2017					Values as of July 2016	
	Flight Hours	MFHBCF	Cumulative Flight Hours	Interim Goal to Meet ORD Threshold MFHBCF	Observed MFHBCF (3 Mos. Rolling Window)	Observed Value as Percent of Goal	Reliability Growth Projection at Maturity	Cumulative Flight Hours	Observed MFHBCF (3 Mos. Rolling Window)
F-35A	75,000	20	48,752	18.8	8.0	43%	8.5	32,358	8.0
F-35B	75,000	12	26,374	10.4	4.6	44%	N/A	20,256	4.6
F-35C	50,000	14	11,107	11.5	8.0	70%	N/A	7,648	4.2

F-35 RELIABILITY: MFHBR (HOURS)									
Variant	ORD Threshold		Values as of May 31, 2017					Values as of July 2016	
	Flight Hours	MFHBR	Cumulative Flight Hours	Interim Goal to Meet ORD Threshold MFHBR	Observed MFHBR (3 Mos. Rolling Window)	Observed Value as Percent of Goal	Reliability Growth Projection at Maturity	Cumulative Flight Hours	Observed MFHBR (3 Mos. Rolling Window)
F-35A	75,000	6.5	48,752	6.1	4.9	80%	5.3	32,358	4.7
F-35B	75,000	6.0	26,374	5.2	2.9	56%	3.8	20,256	2.8
F-35C	50,000	6.0	11,107	4.9	3.7	76%	N/A	7,648	2.3

F-35 RELIABILITY: MFHBME (HOURS)									
Variant	ORD Threshold		Values as of May 31, 2017					Values as of July 2016	
	Flight Hours	MFHBME	Cumulative Flight Hours	Interim Goal to Meet ORD Threshold MFHBME	Observed MFHBME (3 Mos. Rolling Window)	Observed Value as Percent of Goal	Reliability Growth Projection at Maturity	Cumulative Flight Hours	Observed MFHBME (3 Mos. Rolling Window)
F-35A	75,000	2.0	48,752	1.88	1.56	83%	1.54	32,358	1.36
F-35B	75,000	1.5	26,374	1.30	1.03	79%	1.75	20,256	1.08
F-35C	50,000	1.5	11,107	1.20	0.83	69%	1.14	7,648	0.74

F-35 RELIABILITY: MFHBF_DC (HOURS)								
Variant	JSF Contract Specification Requirement		Values as of May 31, 2017				Values as of July 2016	
	Flight Hours	MFHBF_DC	Cumulative Flight Hours	Interim Goal to Meet Threshold MFHBF_DC	Observed MFHBF_DC (3 Mos. Rolling Window)	Observed Value as Percent of Goal	Cumulative Flight Hours	Observed MFHBF_DC (3 Mos. Rolling Window)
F-35A	75,000	6.0	48,752	5.57	6.1	110%	32,358	5.8
F-35B	75,000	4.0	26,374	3.37	3.8	113%	20,256	4.1
F-35C	50,000	4.0	11,107	3.12	5.0	160%	7,648	3.3
MFHBF_DC is a contract specification, so its JSF contract specification requirement is shown in lieu of an ORD threshold. Since this measure does not have an ORD requirement, no "reliability growth projection at maturity" was computed.								

- Overall F-35 reliability has changed little compared to July 2016. Most changes are nominal and within the natural variability of 3-month moving averages for the F-35. The exceptions are F-35A MFHBME, F-35C MFHBCF, and F-35C MFHBR reliability metrics; all three of these ORD reliability metrics show improvement over the past year. Nonetheless, all ORD reliability metrics for all variants fall short of their interim goals.
- Later production lot aircraft have tended to have higher reliability values than earlier lot aircraft. An analysis of MFHBR values by lot showed a significant increase in reliability for F-35A aircraft for Lots 6 and later compared to aircraft from Lots 5 and earlier. However, most aircraft within F-35A Lots 6 and later had similar reliability values. This lot-by-lot improvement trend was much less pronounced for the F-35B variant. The F-35C was not investigated due to the small number of aircraft in the fleet, and thus very small numbers of F-35C in each lot, making statistically significant evaluation difficult.
- The program should review reliability and maintenance data from test and operations and provide an updated sustainment cost estimate based on actual data and trends. This updated estimate should include assessments of sustaining aircraft in older configurations vice modifying them to current configurations.
- In addition to reporting the MFHBCF values above, the JPO has recently adopted a second, alternative approach for reporting MFHBCF which only counts critical failures that take 8 hours or more to remedy. This approach presumably supports modeling of Sortie Generation Rate (SGR), a Key Performance Parameter in the ORD.
  - Based on recent data sets, this alternative approach does not account for approximately three quarters of all critical failures, resulting in a higher MFHBCF estimate. For example, for the 3 months ending in April 2017, the JPO reports the F-35A MFHBCF rate using this alternate approach as 27.4 hours versus 7.7 hours when counting all critical failures; the F-35B MFHBCF rate

as 17.2 hours versus 4.6 hours when counting all critical failures; and the F-35C MFHBCF rate as 35.6 hours versus 8.5 hours.
    - DOT&E disagrees with this approach because failures that take less than 8 hours to remedy can still affect SGR. Also, it is not consistent with the widely accepted definition of the MFHBCF measure.
- F-35 Reliability Growth
  - DOT&E updated a reliability growth analysis from the FY16 Annual Report, based on the Army Materiel Systems Analysis Activity (AMSAA)-Crow Projection Model and using cumulative flight hour and failure data from the start of flying for each variant through May 2017. The AMSAA-Crow model is used to estimate system reliability and is able to project the impact of corrective actions on system reliability.
  - This updated, long-term analysis shows flat or negative reliability growth for F-35B MFHBCF, F-35C MFHBCF, and F-35C MFHBR. Although both F-35C MFHBCF and MFHBR have improved over the last year, they have not improved enough to overcome the trend based on historical data from prior years. As a result, these three metrics have no projection at maturity. Sustained improvement is needed for positive reliability growth to become apparent in future long-term analyses.
  - For the remaining six ORD metrics, only one, F-35B MFHBME, is on track to surpass its threshold requirement by maturity.
- Maintainability
  - The amount of time needed to repair aircraft and return them to flying status has changed little over the past year, but remains higher than the requirement for the system when mature. The program assesses this time with several measures, including Mean Corrective Maintenance Time for Critical Failures (MCMTCF) and Mean Time To Repair (MTTR) for all unscheduled maintenance. Both measures include "active touch" labor time and cure times for coatings, sealants, paints, etc., but do not include logistics delay times, such as how long it takes to receive shipment of a replacement part.
    - MCMTCF measures active maintenance time to correct only the subset of failures that prevent the F-35 from being able to perform a specific mission. It indicates the average time for maintainers to return an aircraft from NMC to MC status.
    - MTTR measures the average active maintenance time for all unscheduled maintenance actions. It is a general indicator of the ease and timeliness of repair.
  - The program reports maintainability metrics for the three most recent months of data. The tables provide MCMTCF and MTTR values for the 3-month period ending May 31, 2017, the date of the most recent maintainability report available, and compare those values to the ORD threshold.
    - All mean repair times are longer, some up to more than twice as long, as their ORD threshold values for maturity, reflecting a heavy maintenance burden on fielded units.
    - July 2016 values used in the FY16 DOT&E Annual Report are included for reference. No significant change or trend can be determined between data from July 2016 to May 2017.

F-35 MAINTAINABILITY: MCMTCF (HOURS)

Variant	ORD Threshold	Values as of May 31, 2017 (3 Mos. Rolling Window)	Observed Value as Percent of Threshold	Values as of July 2016 (3 Mos. Rolling Window)
F-35A	4.0	12.3	308%	10.6
F-35B	4.5	11.9	264%	13.2
F-35C	4.0	11.7	293%	10.1

F-35 MAINTAINABILITY: MTTR (HOURS)

Variant	ORD Threshold	Values as of May 31, 2017 (3 Mos. Rolling Window)	Observed Value as Percent of Threshold	Values as of July 2016 (3 Mos. Rolling Window)
F-35A	2.5	7.4	296%	6.3
F-35B	3.0	7.7	257%	7.3
F-35C	2.5	4.7	188%	4.9

  - The JPO, after analyzing MTTR projections to maturity, acknowledged that the program would not meet the MTTR requirements defined in the ORD. The JPO is seeking relief from the original MTTR requirements and has proposed new values of 5.0 hours for both the F-35A and F-35C, and 6.4 hours for the F-35B. This will affect the ability to meet the ORD requirement for Sortie Generation Rate (SGR), a Key Performance Parameter.
  - The amount of time spent maintaining the low observable (LO) properties of the aircraft, particularly those repairs involving cure times with the LO coatings and seals, is greater than requirements, but an improvement over earlier generations of LO aircraft. The MTTR for LO-related maintenance events was 12.4 hours for the F-35A, 17.1 hours for the F-35B, and 14.7 for the F-35C. These metrics are based on maintenance data from March 2012 through February 2017. Higher-than-planned replacement rates for blade seals (designed to cover gaps between structural surfaces), canopy boots and wingtip light lens covers have contributed to extend LO repair times. Improved versions of these components have been designed with anticipated lower failure rates, and should lower the overall LO maintenance burden in the fleet once incorporated. The improved versions have not yet proliferated to all fielded aircraft. In CY17, the Air Force created a new reporting status, designated NMC-A, for tracking aircraft that are NMC due to excessive degradation of LO capabilities, and asked the JPO to track this category for fleet metrics. This status is based on the rating provided by the Low Observable Health Assessment

System (LOHAS) module of ALIS, where the LO status of the aircraft is assessed and tracked based on LO defects and LO maintenance activity completed.
- Air-Ship Integration and Ship Suitability Testing
  - Dawn Blitz, a large combined Navy-Marine Corps exercise, included F-35B aircraft flying from the USS *Essex* off the coast of Southern California. The exercise ran from October 20-30, 2017, but full analysis of all collected data was not complete at the time of writing this report. However, DOT&E personnel on the USS *Essex* made three significant observations:
    - Initial aircraft reliability and availability were immediately problematic, with 7 of 8 planned aircraft arriving and only 3 of 7 available to fly by the second day of flying. Although the aircraft completed most of their planned missions, usually consisting of a four-aircraft requirement, it would have been challenging to achieve equal success with only six aircraft, as normally assigned, and with a longer logistics burden, as would be the case in a deployed theater.
    - The ship's electrical power, from wall outlets in the hangar bay and on the flight deck used for aircraft maintenance, appeared to damage electrical components in two of the aircraft. This damage made the aircraft NMC on day two of the exercise. From that day forward, maintainers only applied power to aircraft using F-35 specific Support Equipment (SE).
    - The F-35 has large, unique SE that is not compatible with the common SE for the other aircraft on the USS *Essex*. As a result, large areas of the hangar deck were taken up by the two sets of SE, which may make it difficult to efficiently conduct maintenance with a full complement of aircraft onboard for an actual deployment.

Autonomic Logistics Information System (ALIS)

ALIS Activity

- ALIS 2.0.2.4 was originally scheduled for release in 2016, but delays in development pushed the initial fielding into 2017.
- The program focused on testing and fielding ALIS software version 2.0.2.4 throughout CY17. Testing included the following new major capabilities:
  - Life Limited Parts Management, which includes propulsion data integration and Production Aircraft Inspection Requirements (PAIRs). PAIRS includes the first eight prognostics-based algorithms for the program.
  - Sub-squadron reporting, which relays the status of detached aircraft back to the home squadron Standard Operating Unit (SOU).
  - Limited direct SOU-to-SOU communications, to improve deployed operations.
  - Deployment planning tool.
- The program conducted initial testing of ALIS 2.0.2.4 with field data at two venues.
  - Testing with OT aircraft occurred on the Operationally Representative Environment (ORE) at Edwards AFB from February 1-24, 2017. The ORE consists of production-representative ALIS hardware in a closed network. This venue is designed for testing ALIS software using data downloaded from OT aircraft.
  - Testing with SDD aircraft occurred at the Air Force Test Center at Edwards AFB from February 7-24, 2017.
  - Because of limitations associated with the hardware versions of the ALIS equipment used to support the SDD aircraft and the ORE, the program could not conduct complete operationally representative testing of new ALIS software versions in either venue.
- The program completed verification testing of ALIS 2.0.2.4 at Nellis AFB. This testing showed that the migration to ALIS 2.0.2.4 at the fielded units would require an extensive effort to ensure that all the data for the aircraft, propulsion systems, spare parts, and support equipment migrated accurately into the more restrictive data structures within ALIS 2.0.2.4.
  - The program allocated 2 weeks for each operating site to complete the migration in an attempt to minimize the effect on flying operations, projecting 8 months to complete all units.
  - After four sites completed migration, VMFA-211, one of the two operational F-35B units at MCAS Yuma, discovered that ALIS was not properly tracking life usage on engine components and suspended flying operations in June 2017.
  - The program ceased migration of remaining sites to ALIS 2.0.2.4 in order to identify root causes and corrective actions and then developed and tested software fixes in another version of ALIS software – version 2.0.2.4.4.
- The program conducted initial testing of ALIS 2.0.2.4.4 on the ORE at Edwards AFB. Validation testing occurred at MCAS Yuma in September 2017.
  - Based on the late discovery of problems at MCAS Yuma, the Air Force required ALIS 2.0.2.4.4 to undergo further testing at Nellis AFB before allowing fielding to other Air Force sites.
  - Deficiencies discovered during the testing of ALIS 2.0.2.4.4 at Nellis AFB in September 2017 required the program to make more software corrections before the Air Force would permit fielding to operational units proceed.
  - The Air Force restarted fielding ALIS 2.0.2.4.4 at Eglin AFB, Florida, in November 2017, to be followed by Luke AFB, Arizona, in January 2018.
- The program expected to begin testing ALIS 2.0.2.5 in October 2017 at the Air Force Test Center at Edwards AFB, and expects to field this update in December 2017. ALIS 2.0.2.5 is intended to address deficiencies and usability problems, upgrade the browser to Internet Explorer 11, and include a filtering function to decrease false alarms in the

Prognostic Health Management (PHM) System. It will include no other new capabilities.
- ALIS 3.0 began regression testing at the Lockheed Martin facility in Orlando, Florida. Major new capabilities include support for lightning protection, improvements to the LOHAS, security enhancements, an initial parts identification and location (IDLO) capability, and corrections to existing deficiencies. The IDLO capability is intended to facilitate maintaining the aircraft which usually have a unique "as maintained" configuration due to the concurrency of production and development and the complex modification program.

ALIS Assessment
- ALIS is designed to bring efficiency to maintenance and flight operations, but it does not yet perform as intended due to several unresolved deficiencies. For example:
  - Most capabilities function as intended only with a high level of manual effort by ALIS administrators and maintenance personnel. Manual work-arounds are often needed to complete tasks designed to be automated. Maintainers frequently must manually enter missing or incorrect Electronic Equipment Logbook data, which accompany spare parts, so they can be accepted and tracked by an SOU.
  - Configuration management of ALIS software and data products remains complex and time-consuming.
  - ALIS incorrectly reports the status of aircraft as Not Mission Capable in the Squadron Health Management application based on Health Reporting (fault) Codes. Meanwhile, a separate application – Customer Maintenance Management System, which relies on the Mission Essential Function List (MEFL) – reports the same aircraft as mission capable. A logistics test and evaluation report for ALIS version 1.0.3A3 in December 2012 first noted this problem.
- Initial testing of ALIS 2.0.2.4 uncovered deficiencies requiring corrections. The Air Force Test Center recommended that the program field ALIS 2.0.2.4 after developing software fixes for the most serious deficiencies. Validation testing demonstrated no problems beyond those noted at the ORE and logistics test and evaluation.
- ALIS 2.0.2.4 does not address many unresolved deficiencies and the program has not yet allocated an appropriate level of funding in SDD to resolve them. The existing unresolved deficiencies will continue to negatively affect aircraft availability and sortie generation rate. The program does not have sufficient resources to simultaneously develop new required capabilities and reduce unresolved deficiencies.
- The ALIS 2.0.2.4.4 validation testing at MCAS Yuma discovered problems related to propulsion data management and life usage tracking. Smaller problems with Portable Maintenance Aid synchronization and the transfer of air vehicle data between SOUs were also discovered. Testing showed improved Portable Memory Device download times compared to earlier versions of ALIS software.
- The program deferred many of the remaining planned capabilities for SDD out of ALIS 3.0. Despite these deferrals, the schedule for ALIS 3.0 is at risk. Delays associated with completing and testing ALIS 2.0.2.4 have contributed to this risk.
  - In late July 2017, the program noted that if ALIS 2.0.2.4.4 was not in flight test by the end of September 2017, the ALIS 3.0 flight test would not occur until 2018. ALIS 2.0.2.4.4 did undergo flight test before the end of September 2017, but the program found deficiencies that were addressed before fielding to operational units resumed in November 2017. As of the end of September 2017, the program had not allocated funding for the rollout of ALIS 3.0 nor made plans for the migration.
  - Resource availability will continue to affect the ALIS 3.0 schedule and will likely affect the schedule and fielding of ALIS 4.0, which has most of the remaining capabilities planned for SDD. The program noted in September 2017 that the margin built into the ALIS development and release schedule will not be sufficient to cover the delays already projected, so the ALIS 4.0 schedule is high risk.
  - It is unlikely that ALIS 3.0 will be fielded and available for use in any carrier deployments planned for IOT&E.
- Assessment of the testing regimen for ALIS.
  - The program relies too heavily on the results of laboratory testing of ALIS software, which does not resemble operational conditions in several ways, including the amount of data processed and external connections. This non-operationally representative method of testing leads to delays in finding and fixing deficiencies, often after the software is fielded. The program should develop an adequate ALIS test venue to ensure ALIS capabilities are well-tested prior to fielding to operational units.
  - The investigation into shortcomings in the conduct of ALIS 2.0.2.4 testing showed that fleet personnel used ALIS in ways that laboratory testers did not.
  - Developmental testing should include the use of a variety of personnel from different Services and experience levels to increase the chances of finding problems early.
  - ALIS testing, architecture, operation, and fielding each absorb a disproportionate amount of time, manpower, and funding.

Prognostic Health Management
- The program developed and is testing an Advanced Filter and Correlate (AFC) 1.0 capability, which is part of the PHM System. AFC 1.0 is intended to mitigate:
  - The number of false alarm Health Reporting Codes (HRCs)
  - Sympathetic HRCs, which result in a single failure generating multiple HRC Work Orders
  - Conditional nuisance HRCs, which are false alarms triggered only by certain, non-operationally representative aircraft configurations, such as test aircraft or aircraft

maintained in a unique configuration (i.e., caused by the concurrency of production and development)

- ALIS 2.0.2.4 includes the first seven prognostic algorithms in PHM which involve monitoring of fuel, oil, and hydraulic fluid. The personnel who initially use these algorithms will collect data that will be used to mature the servicing and remaining life predictions.
- The program moved from reporting PHM metric performance in 6-month rolling windows to 3-month rolling windows. The following table shows the most recent data available. Compared to last year's Annual Report, nearly every fault detection and isolation metric has improved for both Block 2B and 3F with the exception of the two non-electronic fault isolation metrics for Block 3F, which decreased 7 to 9 percent.
- PHM diagnostic performance shows improvement overall with two of five metrics meeting threshold requirements in this rolling window. DOT&E will need more formally adjudicated data before determining if PHM maturation is sufficient to meet any of its threshold requirements.
- The small improvements in false alarm metrics noted in the last three Annual Reports indicate the program will not meet false alarm threshold requirements. The program expects AFC 1.0 to improve PHM false alarm performance, but DOT&E estimates the improvements will be insufficient for the program to meet requirements.

METRICS OF DIAGNOSTIC CAPABILITY
(3-month rolling window, as of February 2017. Data provided by the F-35 Joint Program Office are preliminary; they have not completed the formal adjudication by the data review board.)

Diagnostic Measure	Threshold Requirement	Demonstrated Performance	
		Block 2B	Block 3F
Developmental Test and Production Aircraft			
Fault Detection Coverage (percent mission critical failures detectable by PHM)	N/A	90	96
Fault Detection Rate (percent correct detections for detectable failures)	98	90	96
Fault Isolation Rate (percentage): Electronic Fault to One Line Replaceable Component (LRC)	90	84	75
Fault Isolation Rate (percentage): Non-Electronic Fault to One LRC	70	83	77
Fault Isolation Rate (percentage): Non-Electronic Fault to Three or Fewer LRC	90	92	92
Production Aircraft Only			
Mean Flight Hours Between False Alarms	50	0.71	1,03 [1]
Mean Flight Hours Between Flight Safety Critical False Alarms	450	878	430 [1]
Accumulated Flight Hours for Measures	N/A	2,634	430 [1]
Ratio of False Alarms to Valid Maintenance Events	N/A	14:1	33:1 [1]

1. False alarm activity may be underreported due to flight test activity (i.e., the control room may be able to tell the pilot that a fault indication is a false alarm that would otherwise have been reported in the field)

Cybersecurity Operational Testing

Activity

- The JOTT continued to accomplish testing based on the cybersecurity strategy, approved by DOT&E in February 2015, with some modifications due to test limitations. The JOTT assessed the Autonomic Logistics Information System (ALIS) version 2.0.2.4 at all three levels of operation:
  - Autonomic Logistics Operating Unit (ALOU)
  - Central Point of Entry (CPE)
  - Squadron Kit (SQK), comprised of the Standard Operating Unit (SOU), the Mission Planning and Support Boundary (MPSB), and the Low Observable Maintenance Boundary (LOMB)
- In 2017, the JOTT conducted Cooperative Vulnerability and Penetration Assessments (CVPAs) of ALIS 2.0.2.4 at three locations in partnership with certified cybersecurity test organizations and personnel:
  - The Navy's Operational Test and Evaluation Force cyber testers assessed the ALOU at Lockheed Martin, Fort Worth, Texas.
    - Unanticipated DOD policy changes for classified equipment security requirements prevented any testing of the classified segment of the ALOU.
  - The 92nd Cyber Operations Squadron assessed the CPE at Eglin AFB and assessed the SQK at Edwards AFB.
    - Unanticipated changes in classified equipment security requirements based on a new DOD policy memorandum disrupted the pace of cyber testing on the SQK.
    - Edwards AFB had not yet received the most recent version of the Low Observable Health Assessment System (LOHAS) workstation and the JOTT decided not to test the available, non-operationally representative older system. The JOTT only became aware of this limitation onsite during the test. The JOTT still tested the operationally representative LOHAS server.
    - Administrative delays with the SOU, caused by pre-coordination problems with the contractors who administer the Edwards SOU, reduced the time available for penetration testing.
- In 2017, the JOTT conducted Adversarial Assessments (AAs) of ALIS 2.0.2.4 at three locations in partnership with certified cybersecurity test organizations and personnel. The AAs did not conclude as originally planned because U.S. Cyber Command (USCYBERCOM) issued and subsequently extended a Period of Non-Disruption (POND), directing all DOD Red Teams to halt activities during the last week of the planned test period.
  - The Marine Corps Information Assurance Red Team (MCIART) assessed the ALOU at Lockheed Martin, Fort Worth.
    - MCIART completed testing of the unclassified ALOU; however, it did not test the classified ALOU due to the USCYBERCOM POND direction to temporarily cease AA testing.
  - The 57th Information Aggressor Squadron (IAS) assessed the CPE at Eglin AFB.
    - As a result of the USCYBERCOM POND, the 57th IAS did not conduct an AA against the classified CPE.
    - The test team also did not complete its assessment of the unclassified CPE.
    - The Eglin AFB unit commander approved a white card physical access assessment of the CPE, which consisted of 57th IAS personnel holding a guided discussion with key CPE personnel.
  - The 177th IAS assessed the SQK at Hill AFB, Utah.
    - The 177th IAS completed testing of the SOU and the MPSB.
    - Due to the USCYBERCOM POND, the test team did not conduct an AA against the LOMB.
    - The Hill AFB unit commander declined permission to undertake the planned close access team assessment of the SQK.
- In response to the DOT&E recommendation to conduct active intrusion discovery and forensics, referred to as a Blue Hunt, on ALIS, the JOTT has scheduled Blue Hunt events for SQK, CPE, and ALOU in CY18.
- Due to the USCYBERCOM POND guidance, full end-to-end cybersecurity testing of the ALIS architecture, from the operational ALOU to the air vehicle, which was planned for 2017, remains to be completed. The JOTT is planning assessments of ALIS 3.0, the air vehicle, the Full Mission Simulator (FMS), the U.S. Reprogramming Laboratory (USRL), and the Operationally Representative Environment (ORE) in 2018 as part of IOT&E. The JOTT is also exploring testing opportunities to complete portions of the AA not undertaken or partially completed.

Assessment

- Cybersecurity testing in 2017 showed that some of the vulnerabilities identified during earlier testing periods still had not been remedied.
- More testing is needed to assess the cybersecurity structure of the air vehicle and supporting logistics infrastructure system (i.e., ALOU, CPE, SQK) and to determine whether, and to what extent, vulnerabilities may have led to compromises of F-35 data. The JOTT has scheduled this testing in CY18.
- The JOTT should expand the scope of cybersecurity testing to include fielded aircraft and other systems required to support the fielded aircraft, such as the Multifunction Analyzer Transmitter Receiver Interface Exerciser (MATRIX). MATRIX is a troubleshooting computer system used by contractor maintenance technicians to detect and isolate faults and is more capable than the Portable Maintenance Aid used by Service maintenance personnel.
- The program should fully complete end-to-end cybersecurity testing on all three levels of ALIS for each of the planned updates to ALIS software and all other systems associated

with the F-35 program, including the USRL, software integration labs, MATRIX, etc.
- Testing to date has identified vulnerabilities that must be addressed to ensure secure ALIS operations. The program should immediately address all identified cyber vulnerabilities from previous rounds of cybersecurity testing.
- According to the JPO, the air vehicle is capable of operating for up to 30 days without connectivity to ALIS. In light of current cybersecurity threats and vulnerabilities, along with peer and near-peer threats to bases and communications, the F-35 program and Services should conduct testing of aircraft operations without access to ALIS for extended periods of time.

IOT&E Readiness

The JPO, Lockheed Martin, and JOTT continued to make preparations for IOT&E. Despite significant effort and progress since the FY16 DOT&E Annual Report, the readiness criteria will not be met until late CY18 to allow formal IOT&E to start. Besides the delays in completing development, producing a verified MDL, and completing ALIS 3.0 development and fielding, this section addresses additional challenges the program must overcome to ensure IOT&E readiness.

Aircraft modifications

- Up to 155 modifications per aircraft are required to bring the early lot OT aircraft into the production-representative configuration required for IOT&E.
- Despite a significant effort by the JPO, JOTT, and Lockheed Martin to minimize delays, modification to all of the 23 IOT&E aircraft will not be complete until August 2018, at the soonest. This challenge is further complicated because some of the IOT&E aircraft were loaned for use by DT, delaying the start of their modification process until their work assisting DT is complete.

Instrumentation

- Test instrumentation requirements will likely not be met until integration and testing is complete in the third quarter of CY18.
- Air-to-Air Range Infrastructure system, version 2 (AARI 2) is undergoing integration and testing with the F-35 aircraft and mission systems software. It is required for mission test trials on the Nevada Test and Training Range (NTTR).
- The Data Acquisition Recording and Telemetry (DART) pod must be certified to the same flight envelope as the internal weapons are for Block 3F, including weapons bay door opening during simulated weapon launches.
- Air Warfare Battle Shaping (AWBS), which can host AARI 2 on the Navy's Pacific Sea Test Range (STR) and China Lake test range, must complete integration and testing to support mission test trials.
- Integration and testing of range threat emitters, which will be used on both the NTTR and STR, must be complete before they can support open air mission trials.

Joint Simulation Environment

- The Joint Simulation Environment (JSE) is a man-in-the-loop simulator. It runs the F-35 operational flight program (mission systems software) and is intended for use in IOT&E to conduct scenarios with modern threat types and densities that are not able to be replicated in open air. Originally slated to be operational by the end of 2017, delivery of the JSE is now planned for late 2018 with accreditation in 2019, near the end of planned IOT&E trials.
- Development of the JSE, although late, made good progress this year with one exception: Integration of the critical F-35 model has lagged behind the development of other parts of the simulation due to contractual difficulties. Until resolved, this problem will continue to increase the risk to delivering the JSE in time for use as an IOT&E venue.
- The JSE's physical facilities (cockpits, visuals, and buildings) and synthetic environment (terrain, threat, and target models) are nearing completion. The JSE version 0.5 configuration included most of the necessary environment, but not the F-35 model, and was successfully delivered in early October 2017, passing all verification testing.
- The JSE validation process has continued to lag development and is now the schedule driver for successful delivery of the simulation. Contractual problems, the lack of a working F-35 simulation, and an inability to harvest needed reference data from the F-35 flight test effort have all contributed to continuing delays in validation and hence accreditation for use in IOT&E.
- Successful completion of the F-35 model contract and increased productivity of the validation team may lead to a usable resource for IOT&E, but both are extremely high risk. The JOTT, per DOT&E direction, continues to plan to execute IOT&E without this resource. However, if the JSE becomes ready and accredited in time, it will be used during IOT&E. Without the JSE, the IOT&E will be limited in assessing the F-35 against complex threats, resulting in risk for operational use. If still not completed by the time IOT&E ends, the JSE should be a valuable test resource for follow-on F-35 testing and possibly for testing of other platforms.

Unresolved Technical Deficiencies

- Deficiency Reporting and Fix Prioritization
  - The JPO, Services, and operational test units continued the process of sorting, adjudicating by severity, and coordinating the hardware and software fixes needed to resolve the backlog of open and newly discovered deficiencies. This effort supports the JSF contract specification verification process the program must complete to finish SDD, the readiness criteria to enter IOT&E, and the delivery of the combat capability required by the Services and partner nations.
  - As of mid-November 2017, the JSF development program was monitoring a total of 2,769 deficiency reports.

Of these, 1,748 have been closed via the review processes now in place. To meet "closure" criteria, these deficiency reports were either determined to no longer be relevant (i.e., they originated in older software versions), or they were deferred to follow-on development (C2D2), corrected and verified, or combined with other relevant deficiency reports. An additional 29 deficiency reports were canceled. The Services and JOTT have reviewed the remaining 992 active deficiency reports for operational effects and meeting readiness criteria for beginning IOT&E. This review created a Service priority list of 301 Priority 1 and 2 deficiencies deemed necessary for the program to address for combat effectiveness and operational testing. However, only 88 of the 301 Priority 1 and 2 deficiencies were in-work, with the remaining 213 unresolved. These deficiencies must either be corrected or have Service-approved, operationally acceptable work-arounds. These deficiencies affect target kill chains, weapons integration, combat survivability, shipboard operations, maintenance/operational documentation, mission planning, ALIS functionality, operational test instrumentation, and cybersecurity.

- Pilot Escape System
  - In May 2017, the Air Force and Navy announced that they were lifting restrictions on lightweight pilots flying F-35s because the fixes that were put in place to address ejection seat problems were working.
  - The JPO provided DOT&E with the F-35 System Safety Risk Assessment (SSRA) it conducted on the additional risk-reducing actions to the pilot escape system during recent testing. The JPO SSRA was informed by modeling and simulation of ejections in off-nominal conditions, along with limited ground subsystem testing with a manikin and the Head Support Panel (HSP), to assess the overall risk of injury as "Low." The testing showed that the changes incorporated into the seat and provided to the pilot's equipment have generally reduced the risk of neck injury to the pilot under the normal ejection conditions.
  - The JPO also provided DOT&E with an SSRA supplement from the U.S. Air Force Technical Airworthiness Authorities (TAA). In that document, due to a lack of test data in off-nominal conditions, the TAA assessed that the level of risk of injury to lighter-weight pilots (103 to 135 pounds with the Gen III Lite helmet, and 136 to 150 pounds with any Gen II/III/III Lite helmet) was categorized as "Serious" due to the absence of test data with the new changes to the ejection system and the potential for head and neck injury during off-nominal ejections at airspeeds less than 190 knots. The TAA determined that it may be possible for the head to miss the HSP for these lighter weight pilots and the result could be either death or total disability. However, the risk was reduced sufficiently during the ejection testing in nominal conditions for the Air Force to remove the restriction preventing pilots weighing less than 136 pounds from flying the F-35.
  - The program began retrofitting fielded F-35s with the modifications to the ejection seats in 2017 and plans to deliver aircraft with the upgraded seat in Lot 10, starting in January 2018. The Gen III Lite helmets will be included with the Lot 10 aircraft delivery, and will be delivered starting in November 2017. If these delivery timelines are met, the Air Force may open F-35 pilot training to lighter-weight pilots (i.e., below 136 pounds) as early as December 2017.
  - Part of the weight reduction to the Gen III Lite HMDS involved removing one of the two visors (one dark, one clear). As a result, pilots that need to use both visors during a mission (e.g., during transitions from day to night), will have to store the second visor in the cockpit. However, there is no designated storage space in the cockpit for the visor; the program is working a solution to address this problem.
  - The program has yet to complete additional testing and analysis needed to determine the risk of pilots being harmed by the Transparency Removal System (TRS), which shatters the canopy first, allowing the seat and pilot to leave the aircraft) during ejections in other than ideal, stable conditions (such as after battle damage or during out-of-control situations). Although the program completed an off-nominal rocket sled test with the TRS in CY12, several aspects of the escape system have changed since then, including significant changes to the helmet, which warrant additional testing and analyses. DOT&E recommends the program complete these tests, in a variety of off-nominal conditions, as soon as possible, so that the Services can better assess risk associated with ejections under these conditions.
- Physiological Incidents
  - Multiple pilot physiological events were reported in 2017, with the majority of them from Luke AFB, Arizona. No common root cause has been identified. The program is investigating the possibility of onboard oxygen generation system (OBOGS) degradations in the fleet. At the time of this report, testing of a new algorithm to control the oxygen generator within the OBOGS was in progress at Wright Patterson AFB, Ohio.
- Production Line Quality Lapses
  - The program recently discovered corrosion in an F-35A at Hill AFB, possibly due to Lockheed Martin not properly treating fastener holes with primer after drilling during production. At the time of this report, the program was still investigating, but it appears to be a production line quality lapse which may affect all variants. In 2016, the program had a well-publicized quality lapse with insulation on fuel tubes within F-35A fuel tanks which required extensive, intrusive depot-level modifications to repair the affected aircraft.
  - F-35A and F-35C fuel valve couplings within the fuel system may require a one-time inspection. This problem appears to be another quality lapse.

- F-35B Tires
  - The program has struggled to find a tire for the F-35B that is strong enough for conventional high-speed landings, soft enough to cushion vertical landings, and still light enough for the existing aircraft structure. Average F-35B tire life is below 10 landings, well below the requirement for 25 conventional full-stop landings. The program is still working this problem, which will not be resolved within SDD.
- Night Vision Camera (NVC)
  - The NVC used with the Gen III helmet has several deficiencies, including inadequate acuity for low-illumination operations (i.e., during a cloudy night with no stars, moon, or cultural lighting). As a result, F-35B pilots were losing situational awareness during night landings on an aircraft carrier. At the time of this report, incremental software solutions had been demonstrated in the lab and were planned for flight test. Further improvement is dependent on improved imaging technology with a prototype expected in 2019.
- F-35B and F-35C Air Refueling Restrictions
  - Both variants use an air refueling probe which is designed with an intentional weak link to protect the probe. The probe tips are breaking too often, resulting in squadrons imposing restrictions on air refueling. The program is still investigating this problem.

Full Mission Simulator

- The program experienced delays developing and fielding the Block 3i Full Mission Simulator (FMS) (i.e., pilot training simulator), with Block 3i aircraft being delivered to most locations well prior to the Block 3i FMS. The Block 3i FMS delays, along with ongoing Block 3F flight test delays, are also delaying development of the Block 3F FMS.
- As a result, the program plans to field an interim "Block 3FR1" version of FMS software in 2018 with partial Block 3F functionality. The Block 3FR1 FMS is based on an earlier Block 3F software version (Block 3FR6.01), to support the pilots flying Block 3F aircraft which are already being delivered. The program then plans to release a "Block 3FR2" version, based on Block 3FR6.3, with full Block 3F functionality between late CY18 through CY19.
  - All versions of FMS software to date, including the Block 3F FMS, are based on Lockheed Martin mission data loads (MDL) which are intended for use in DT flight test, not for realistic operational training or combat.
  - The utility of the Block 3F FMS for IOT&E training will depend on operational MDLs, developed by the USRL, being integrated with the FMS virtual threat environment. The existing FMS software development and integration processes will take about 24 months to incorporate a USRL MDL, once it is available.
  - Based on the timelines above, the Block 3F FMS will not be available to support IOT&E training, even with partial functionality using the DT MDL. A version of Block 3F FMS software with a fielded USRL MDL will likely not be available until 2020.
  - As a result, IOT&E pilots will need to rely on available aircraft, along with the Verification Simulator and JSE, for Block 3F training and spin-up (i.e., test mission rehearsals). This will place a heavier demand on the IOT&E aircraft from late 2017 through most of 2018, at a time when many of the aircraft will be undergoing modifications to be production-representative.
  - The JPO plans to change the FMS architecture in C2D2 to decrease the long software development and integration timelines while enabling rapid incorporation of operational mission data for more realistic training and mission rehearsals.

Pre-IOT&E Events

- As the program and JOTT continue to prepare for IOT&E, early releases of Block 3F software and mission data (i.e., Level 3 MDL) may allow the OT squadrons to train and conduct some spin-up activities prior to meeting formal spin-up entrance criteria.
- The JOTT plans to conduct operationally representative Pre-IOT&E events (i.e., weapons delivery events, cold weather deployment). Prior to seeking DOT&E approval of these events, the JSF Program Executive Officer will certify that the program is ready for the specific event(s) and will coordinate with the Defense Acquisition Executive for authorization to accomplish them. These Pre-IOT&E events will not interfere with preparations (i.e., modifications and spin-up) for formal IOT&E entrance planned for later in CY18.
- DOT&E will observe the execution of the Pre-IOT&E events and assess whether each event was operationally representative and adequate to meet IOT&E requirements. This may allow the program to apply data from select Pre-IOT&E events toward formal IOT&E assessment.

Recommendations

- Status of Previous Recommendations. The program adequately addressed 4 of the 17 previous recommendations. The following recommendations remain valid:
  1. The program should complete all necessary Block 3F baseline test points. If the program uses test data from previous testing or added complex test points to sign off some of these test points, the program must ensure the data are applicable and provide sufficient statistical confidence prior to deleting any underlying build-up test points.
  2. The program should ensure adequate resources remain available (personnel, labs, flight test aircraft) through the completion of IOT&E to develop, test, and verify corrections to deficiencies identified during flight testing.
  3. The program should address the deficiency of excessive F-35C vertical oscillations during catapult launches within SDD to ensure catapult operations can be conducted safely during IOT&E and during operational carrier deployments. (The program made progress working this problem, but testing of potential fixes is not complete.)
  4. The JPO must immediately fund and expedite the contracting actions for the necessary hardware and software

modifications to provide the necessary and adequate Block 3F mission data development capabilities for the USRL, including an adequate number of additional RF signal generator channels and the other required hardware and software tools.

5. The program should address the JOTT-identified shortfalls in the USRL that prevent the lab from reacting to new threats and reprogramming mission data files consistent with the standards routinely achieved on legacy aircraft.
6. The program should ensure Block 3F is delivered with capability to engage moving targets, such as that provided by the GBU-49, or other bombs that do not require lead laser guidance. (GBU-49 is being integrated on the F-35A and C, but is not funded for integration and testing on the F-35B.)
7. The program should complete additional testing and analysis needed to determine the risk of pilots being harmed by the Transparency Removal System during ejections in other than ideal, stable conditions. The program should complete these tests as soon as possible, with the new equipment, including the Gen III Lite helmet in a variety of off-nominal conditions, so that the Services can better assess risk associated with ejections under these "off-nominal" conditions.
8. The Navy and the JPO should investigate alternatives for determining the operational effect of an engine removal and install while conducting carrier air wing operations at sea.
9. The Navy and Marine Corps should conduct an analysis, such as an operational logistics footprint study, which simulates flight deck and hangar bay aircraft placement with a full Air Combat Element (ACE) onboard, using data from the DT-III ship trials to determine what the effect of an engine removal and installation would be on integrated ship and ACE operations with a full ACE onboard. (The Navy has provided historical operational logistics footprint reports to DOT&E and the JOTT has provided data collected during Exercise Dawn Blitz 2017 to DOT&E; analysis is ongoing).
10. The program and the Navy should investigate if the heavy power module container should be redesigned for better usability at sea.
11. The program and the Navy should investigate potential options to improve ship-based communications bandwidth dedicated to ALIS connectivity off-ship, such as increasing the priority of ALIS transmissions, or reserving low-use times of the day for handling large volumes of ALIS message traffic.
12. The Navy should investigate any efficient, multi-use opportunities for F-35 support equipment (SE) such as using legacy SE on the F-35 or F-35 SE on legacy aircraft.
13. The Navy should investigate options for increasing the number of wall power outlets in CVN hangar bays to help facilitate simultaneous maintenance on multiple F-35Cs, or the ability to interconnect multiple pieces of support equipment from a single outlet to permit simultaneous operations.

- FY17 Recommendations.
  1. The program should re-plan C2D2 to have a more realistic schedule and content that include adequate test infrastructure (labs, aircraft, and time) and modifications while aligning the other fielding requirements, like mission data, training simulators, and airworthiness.
  2. For the USRL, the program must:
     - Immediately provide adequate resources within the FY19 DOD program review cycle to fully equip the USRL with software tools and hardware lines, including enough signal generators, to support new C2D2 capabilities and the many fielded configurations with timely and validated mission data.
     - Complete end-to-end cybersecurity testing of the laboratory test lines
     - Provide the USRL with adequate technical data for lab equipment and enough spare parts and supply priority to quickly repair key components.
  3. The program should complete contract actions for another F-35B ground test article as soon as possible to begin additional durability testing.
  4. The program, in coordination with the Services, should stand up intermediate-level maintenance capability as soon as possible, particularly to support deployed aircraft and ship-borne operations.
  5. The program should review reliability and maintenance data from test and operations and provide an updated sustainment cost estimate based on actual data and trends. This updated estimate should include assessments of sustaining aircraft in older configurations vice modifying them to current configurations.
  6. For ALIS, the program should:
     - Develop an adequate ALIS test venue to ensure ALIS capabilities are well-tested prior to fielding to operational units
     - Fully complete end-to-end cybersecurity testing on all three levels of ALIS.
  7. The program should immediately address and seek to remediate all identified cyber vulnerabilities from previous rounds of cybersecurity testing and expand test venues to include software integration labs and maintenance aids (e.g., MATRIX).
  8. The program and Services should conduct testing of "unplugged" aircraft operations without access to ALIS for extended periods of time in light of current cybersecurity threats and vulnerabilities, along with peer and near-peer threats.
  9. The program should complete testing of all required aircraft instrumentation, including integration with the test ranges prior to the formal start of IOT&E. This include the Air-to-Air Range Infrastructure system, Air Warfare Battle Shaping system, and flight certification for the Data Acquisition Recording and Telemetry pod. These instrumentation capabilities are required for test adequacy during IOT&E.

Global Command and Control System - Joint (GCCS-J)

Executive Summary

- In FY17, the Defense Information Systems Agency's (DISA) development of Global Command and Control System – Joint (GCCS-J) focused on the major components of GCCS-J: GCCS-J Global and Joint Operation Planning and Execution System (JOPES).

Global

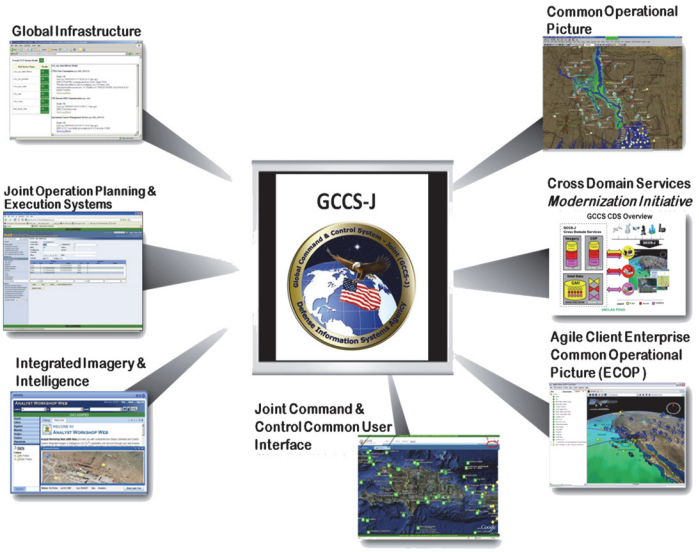
- The program manager corrected all significant defects discovered during the August 2016 operational assessment (OA), except three that affected the Joint Targeting Toolbox (JTT). The Program Executive Officer (PEO) Services Development approved Global v6.0 and Agile Client Release 7 v5.1.0.1 for limited fielding without the JTT component.
- The program manager used incremental Maintenance Releases (MRs) to develop Global v6.0, completing four Global v6.0 MRs in FY17. The Joint Interoperability Test Command (JITC) observed and reported on the Global v6.0 MR level I operational tests. Operational testing in FY17 confirmed that the program manager implemented the majority of new capabilities and defect fixes successfully. In cases where testers found defects, the program manager removed the defective capability or component prior to deploying the MR to users. DOT&E will evaluate Global v6.0 and Agile Client operational effectiveness and operational suitability once the program manager delivers a more complete set of capabilities.
- The program manager deployed Global v6.0.0.3 MR on July 5, 2017, and Agile Client Release 8, v5.2.0.1 on July 19, 2017.
- Global v6.0.0.3 MR and Agile Client Release 8, v5.2.0.1 survivability is undetermined. The program manager should complete a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) and Adversarial Assessment (AA) on the fielded version of Global and Agile Client to enable a survivability determination.

JOPES

- JITC operationally tested JOPES v4.2.0.3 MR4 in FY17, and found it operationally effective and operationally suitable.
- JOPES v4.2.0.3 MR4 cyberspace survivability is undetermined. The program manager should complete a cybersecurity CVPA and AA on the fielded version of JOPES to enable a survivability determination.

System

- GCCS-J consists of hardware, software (both commercial off-the-shelf and government off-the-shelf), procedures, standards, and interfaces that provide an integrated, near real-time picture of the battlespace that is necessary to conduct joint and multi-national operations. Its client/server architecture uses open systems standards and government-developed military planning software. Global and JOPES are two of the baseline systems that comprise the operational environment of GCCS-J.



Global (Force Protection, Situational Awareness, and Intelligence applications)

- Global v4.3 Update 1 Emergency Release 1 is the currently fielded version. DISA developed Global v4.3 Update 1 to implement high-priority intelligence mission updates to the Theater Ballistic Missile correlation systems, JTT, and Modernized Integrated Database. Emergency Release 1 resolved an operational deficiency discovered in the fielded Global v4.3 Update 1 software and included some of the improvements originally planned for the canceled Global v5.0.
- Global v6.0.0.3 and Agile Client Release 8, v5.2.0.1 are currently fielded at a limited number of sites. Global v6.0.0.3 is intended to provide back-end services, databases, and system administration functions. Agile Client Release 8, v5.2.0.1 with Agile Client core services and the Agile Client plug-in, is intended to provide visualization and presentation of GCCS-J mission applications and functionality to the user.
- The program manager is using agile development to evolve Global v6.0, releasing incremental MR packages to expand capabilities available to the warfighter. DISA is developing GCCS-Joint Enterprise (JE) to replace Global v4.3 Update 1 Emergency Release 1, Global v6.0, and Agile Client Release 8 v5.2.0.1. GCCS-JE is intended to provide situational awareness using a data subscription service, ending the current dependence on a local software instantiation of GCCS-J Global. The Services and

Combatant Commands will need to modify their command and control systems to interface with the new GCCS-JE data service.

JOPES (Force Employment, Projection, Planning, and Deployment/Redeployment applications)

- JOPES v4.2.0.3 MR4 is the currently fielded version. JOPES v4.2.0.3 MR4 supports migration to 64-bit applications, Public Key Infrastructure implementation on web servers, security enhancements, and resolves 25 problem reports.
- DISA is developing Joint Planning and Execution Services (JPES) to replace JOPES v4.2.0.3 MR4. One component of JPES, referred to as the JPES Solution, provides the user interface, presentation services, search capabilities, and mobile device support. The other component of JPES, referred to as the JPES Framework (JFW), provides the software infrastructure, permissions management, core data services, business logic, and interfaces to Authoritative Data Sources. DISA plans to start moving external interfaces from JOPES to the JPES Solution and the JFW during FY18.

Mission

- Joint Commanders utilize the GCCS-J to accomplish command and control.

Global

- Commanders use Global to:
  - Link the National Command Authority to the Joint Task Force, Component Commanders, and Service-unique systems at lower levels of command
  - Process, correlate, and display geographic track information integrated with available intelligence and environmental information to provide the user a fused battlespace picture
  - Provide integrated imagery and intelligence capabilities (e.g., battlespace views and other relevant intelligence) into the common operational picture and allow commanders to manage and produce target data using the joint tactical terminal
  - Provide a missile warning and tracking capability
- Air Operations Centers use Global to:
  - Build the air picture portion of the common operational picture and maintain its accuracy
  - Correlate or merge raw track data from multiple sources
  - Associate raw electronics intelligence data with track data
  - Perform targeting operations

JOPES

- Commanders use JOPES to:
  - Translate policy decisions into operations plans that meet U.S. requirements to employ military forces
  - Support force deployment, redeployment, retrograde, and e-posturing
  - Conduct contingency and crisis action planning

Major Contractors

- Government Integrator: DISA – Fort Meade, Maryland
- Software Developers:
  - Northrop Grumman – Arlington, Virginia
  - Leidos – Arlington, Virginia
  - Pragmatics – Arlington, Virginia
  - CSRA – Falls Church, Virginia

Activity

Global

- The DISA PEO Services Development Office approved the limited fielding of Global v6.0 and Agile Client v5.1.0.1 in January 2017.
- The program manager conducted and JITC observed and reported on an operational test of Global Version (v) 6.0.0.1 during the Coalition Warrior Interoperability eXploration, experimentation, examination, exercise (CWIX) 2016 and at the DISA laboratory facility at Fort Meade, Maryland, from February 15-21, 2017. In accordance with DOT&E policy, this low-risk upgrade warranted a level I operational test, which did not require a DOT&E-approved test plan.
- The program manager conducted and JITC observed and reported on a level I operational test of Global v6.0.0.2 at the DISA laboratory from March 6-16, 2017, and Global v6.0.0.3 at U.S. Transportation Command at Scott AFB, Illinois, and the DISA laboratory from June 5-13, 2017.
- The program manager approved Global v6.0.0.3 MR for release on July 5, 2017.
- The program manager approved Agile Client Release 8, v5.2.0.1 for release on July 19, 2017.
- The program manager commenced a level I test of Global v6.0.0.5 MR and Agile Client Release 9, v6.0.0.0, with JITC observation, at the DISA and JITC laboratories from August 14 through November 8, 2017.

JOPES

- Following the JITC-conducted JOPES v4.2.0.4 operational test in September and October 2016, DISA worked to resolve critical Deliberate and Crisis Action Planning and Execution System and Joint Flow and Analysis System for Transportation interface problems. In accordance with DOT&E policy, this moderate-risk release warranted a level II operational test, which did not require a DOT&E-approved test plan.
- DISA changed the JOPES version from v4.2.0.4 to v4.2.0.3 MR4 on May 11, 2017. System functionality remained unchanged.

- JITC conducted a JOPES v4.2.0.3 MR4 operational test from May 22 through September 5, 2017. U.S. Army Forces Command, Fort Bragg, North Carolina; Headquarters Air Force, Pentagon, Washington, District of Columbia; U.S. Transportation Command, Scott AFB, Illinois; DISA, Fort Meade, Maryland; and Joint Service Support Center, Pentagon, Washington, District of Columbia participated in the operational test.

Assessment

Global

- The program manager corrected all significant Global v6.0 and Agile Client Release 7 v5.1.0.1 defects discovered during the August 2016 OA, except three that affected the JTT. The PEO Services Development Office approved Global v6.0 and Agile Client v5.1.0.1 for limited fielding without the JTT component.
- The program manager updated Agile Client Imagery Transformation Services and Integrated Imagery and Intelligence (I3) Imagery Plug-ins in Global v6.0.0.1 MR. Following testing, the program manager removed the Automated NATO Database Interface Agile Client plug-in due to a security concern. All other fixes worked correctly and Agile Client performed as expected.
- The program manager updated Joint Effects Model components in Global v6.0.0.2 MR. The program manager and JITC confirmed 22 of 23 defects were resolved. One low-priority defect remained unresolved, but the mission impact is limited due to a user validated operational workaround.
- The program manager updated the Common Operational Picture Transportation Interface and Integrated Command, Control, Communications, Computers, and Intelligence System Framework components in Global v6.0.0.3 MR. The program manager and JITC confirmed that 22 of 22 defects were resolved. Global v6.0.0.3 MR performed as expected.
- The program manager added Agile Client Release 9, v6.0.0.0 to the Global baseline, implemented 28 new capabilities, and fixed 28 defects in Global v6.0.0.5 MR. The Global v6.0.0.5 MR level I test results were not available for inclusion in this report.
- DOT&E will evaluate Global v6.0 and Agile Client effectiveness and suitability once the program manager delivers a more complete set of capabilities.
- Global v6.0.0.3 MR and Agile Client Release 8, v5.2.0.1 cyberspace survivability is undetermined. The program manager should complete a cybersecurity CVPA and AA on the fielded version of Global and Agile Client to allow DOT&E to make a survivability determination.
- As part of the GCCS-JE development, the program manager is drafting a Test and Evaluation Master Plan (TEMP) for DOT&E approval. The pace of system development has slowed the program manager's TEMP progress.

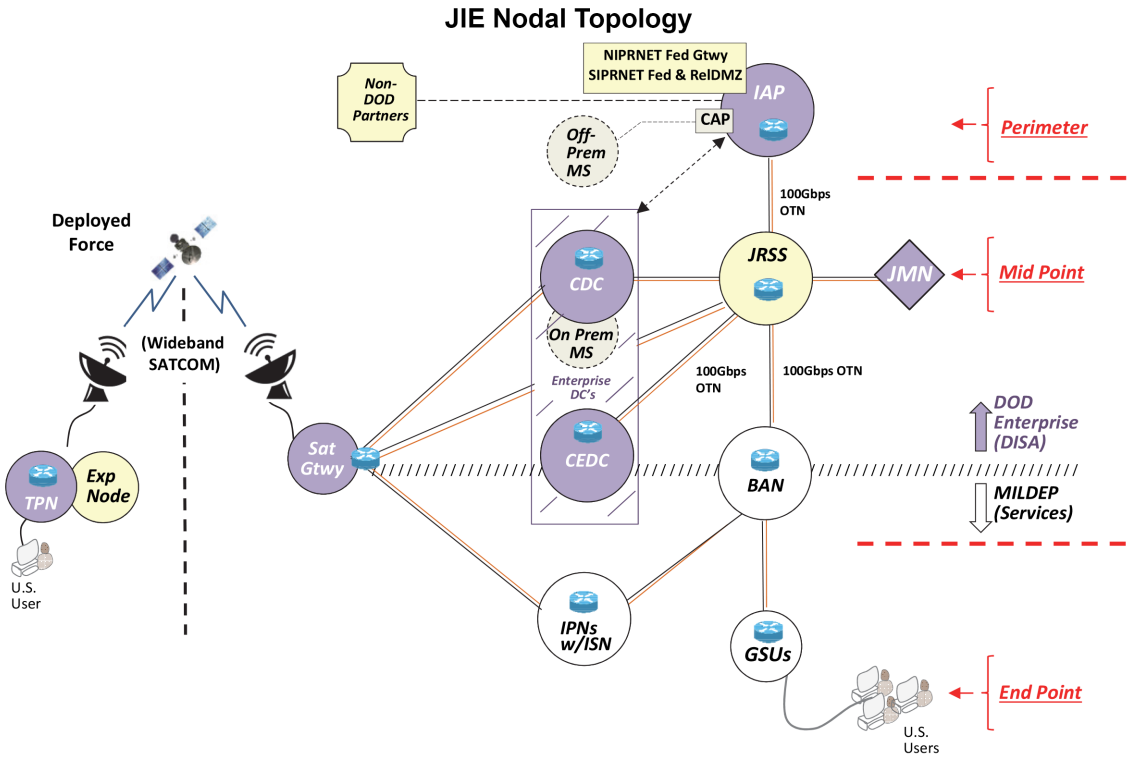
JOPES

- During the JOPES v4.2.0.3 MR4 operational test, JITC assessed transition and installation activities in the operational environment and validated correction of previously identified defects. JITC identified new high severity data exchange defects during testing. However, the program manager resolved these and JITC validated correction of all defects by the completion of testing.
- JOPES v4.2.0.3 MR4 is operationally effective. JOPES users successfully created operational plans and force requirements; sourced, updated, and validated force requirements; and scheduled and moved forces. The program manager resolved all previously identified defects or identified user validated operational workarounds.
- JOPES v4.2.0.3 MR4 is operationally suitable. System administrators installed and configured the system using the available documentation. JOPES system administrators successfully transitioned to v4.2.0.3 MR4, with no loss of data or system capabilities. The test system was available 624 of 624 hours throughout the test. Both the test and operational system exceeded the availability Key Performance Requirement threshold of 99.7 percent. There was no degradation of performance or usability compared to the currently fielded version.
- JOPES v4.2.0.3 MR4 cyberspace survivability is undetermined. The program manager has not yet completed a cybersecurity CVPA and AA on the fielded version of JOPES.

Recommendations

- Status of Previous Recommendations. DISA addressed three of the five previous FY16 recommendations. However, DISA still needs to complete a cybersecurity CVPA and AA on the fielded versions of Global v6.0 and JOPES.
- FY17 Recommendation.
  1. DISA should complete the GCCS-JE TEMP for DOT&E approval.

Joint Information Environment (JIE)



BAN - Base Area Network
CAP - Cloud Access Point
CDC - Core Data Center
CEDC - Component Enterprise Data Center
DCs - Data Centers
DISA - Defense Information Systems Agency
DMZ - Demilitraized Zone
Exp - Expeditionary
Fed - Federal
Gbps - Gigabits per second
GSUs - Geographically Separated Unit

Gtwy - Gateway
IAP - Internet Access Point
IPNs - Installation Processing Node
ISN - Installation Service Node
JMN - Joint Management Network
JRSS - Joint Regional Security Stack
MILDEP - Military Department
MS - Materiel Solution
NIPRNET - Non-classified Internet Protocol Router Network

Off-Prem - Off premises
On-Prem - On premises
OTN - Optical Transport Network
Prem - Premises
RelDMZ - SIPRNET Releasable DMZ
Sat - Satellite
SATCOM - Satellite Communications
SIPRNET - Secret Internet Protocol Router Network
TPN - Tactical Processing Node

Executive Summary

- The Joint Information Environment (JIE) Executive Committee (EXCOM) approved 10 JIE capability objectives in January 2017 that prioritize JIE capability development and integration efforts for the DOD.
- DOT&E worked with the DOD Chief Information Officer (CIO) to develop a Mission Partner Environment – Information System (MPE-IS) Test and Evaluation Strategy in March 2017. MPE-IS integration, developmental testing, and rehearsals coincide with Exercises Steadfast Cobalt and Bold Quest 2017 to support and inform a DOD independent study report due in 2018.

Capability and Attributes

- In August 2012, the Joint Chiefs of Staff (JCS) approved the JIE concept as a secure environment, comprised of a single security architecture, shared information technology (IT) infrastructure, and enterprise services.
- JIE consists of multiple subordinate programs, projects, and initiatives managed by the Defense Information Systems Agency (DISA) and the Services.
- The DOD CIO established 10 JIE capability objectives that include the following:
  - Modernize Network Infrastructure, to include optical carrier upgrades, multi-protocol label switching, satellite communication gateway modernization, and Internet Protocol (IP) version 6 implementation
  - Enable Enterprise Network Operations, to include establishing global and regional operations centers, a JIE out-of-band management network, and converging IT service management solutions
  - Implement Regional Security, to include the Joint Regional Security Stacks (JRSS), and the Joint Management System for JRSS

  - Provide MPE-IS for coalition/partner information sharing, to include virtual data centers, services, and Mission Partner Gateways
  - Optimize Data Center Infrastructure
  - Implement Consistent Cybersecurity Architecture/Protections, to include DOD enterprise perimeter protection, endpoint security, mobile endpoint security, data center security, cybersecurity situational awareness analytic capabilities, and identity and access management (previously referred to as the Single Security Architecture in older JIE documentation)
  - Enhance Mobility for unclassified and classified capabilities
  - Standardized IT Commodity Management, to include enterprise software agreements, license agreements, hardware agreements, and IT asset management
  - Establish End-User Enterprise Services, to include the Enterprise Collaboration and Productivity Services (ECAPS) and converged voice and video services over IP
  - Provide Hybrid Cloud Computing Environments, to include Commercial Cloud, Cloud Access Points, and milCloud
- The JCS envision JIE as a shared information technology construct for DOD to reduce costs, improve and standardize physical infrastructure, increase the use of enterprise services, improve IT effectiveness, and centralize the management of network defense. The Joint Staff specifies the following enabling characteristics for JIE capability objectives:
  - Transition to centralized data storage
  - Rapid delivery of integrated enterprise services (such as email and collaboration)
  - Real-time cybersecurity awareness
  - Scalability and flexibility to provide new services
  - Use of common standards and operational techniques
  - Transition to the JIE Cybersecurity Architecture
- JIE is not a program of record and does not have a traditional milestone decision authority, program executive organization, and project management structure that would normally be responsible for the cost, schedule, and performance of a program.
- The DOD CIO leads JIE efforts with support from the JIE EXCOM – chaired by the DOD CIO, U.S. Cyber Command, and Joint Staff J6. The EXCOM provides JIE direction and objectives. DISA is the principal integrator for JIE services and testing.

Activity

- For reporting on the JRSS, see the separate article on page 69.
- The JIE EXCOM approved 10 JIE capability objectives in January 2017 that prioritize JIE capability development and integration efforts for the DOD.
- The DOD CIO developed an MPE-IS Test and Evaluation Strategy in March 2017. MPE-IS integration, developmental testing, and rehearsals coincide with Exercises Steadfast Cobalt and Bold Quest 2017 to support and inform a DOD-directed independent study for future funding in 2018.
- The JIE EXCOM approved the JIE Architecture and Engineering Security Classification Guide in May 2017, and the strategy document, Achieving the JIE Vision, in August 2017.
- The DOD CIO began development of a JIE Capabilities Test and Evaluation, and Assessment Concept whitepaper in June 2017.
- The JIE Capabilities Test and Evaluation Working Group is developing a JIE Test and Evaluation Strategy.
- The USD(AT&L) commenced acquisition strategy development for the Defense Enterprise Office Solution and the ECAPS components of JIE in February 2017.
- The DOD CIO, Joint Staff, Combatant Commands, Services, and DOD Agencies continued efforts to develop and build the JIE Cybersecurity Architecture.

Assessment

- The DOD CIO, DISA, and Services intend to achieve the JIE goals through implementation of initiatives aligned under the JIE EXCOM-approved capability objectives.
- The JIE EXCOM has started efforts to monitor JIE capability performance factors; however, the EXCOM does not place high priority on developmental and operational test information when making capability fielding decisions.
- The JIE EXCOM utilizes schedule-driven management but should adopt event-driven decision processes supported by developmental and operational test reporting.

Recommendations

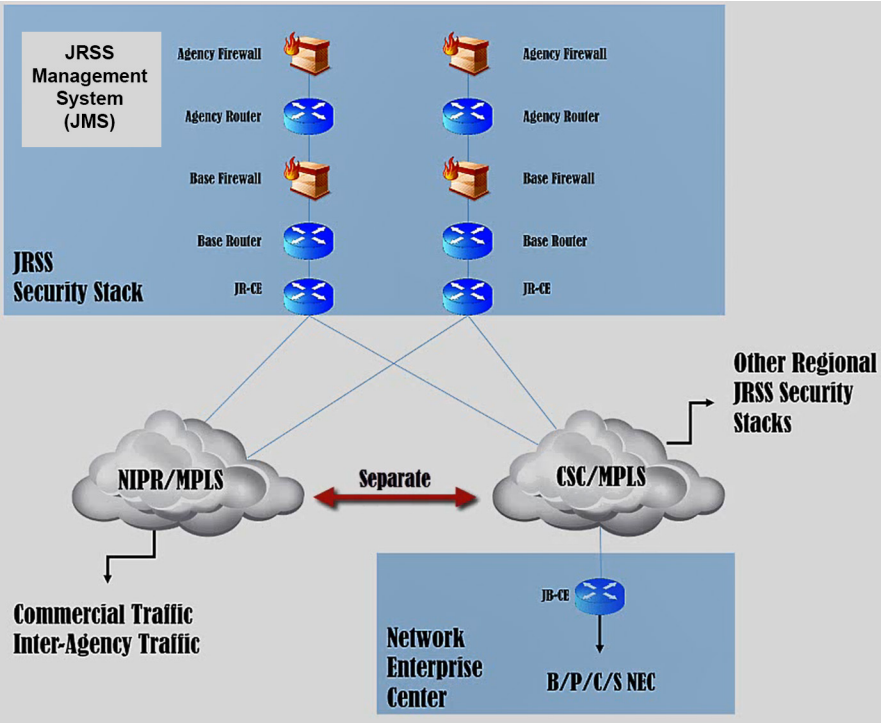
- Status of Previous Recommendations. The DOD CIO, JIE EXCOM, and Director of DISA satisfactorily addressed two of the previous non-JRSS specific FY16 recommendations. The following remain:
  1. Establish an overarching JIE program executive to integrate the system efforts and oversee cost, schedule, and performance.
  2. Complete, adopt, and implement the JIE Test and Evaluation Strategy.
- FY17 Recommendations. The DOD CIO, JIE EXCOM, and Director of DISA should:

1. Use operational test information to inform JIE capability fielding decisions.
2. Update the MPE-IS Test and Evaluation Strategy to reflect full delivery and test schedule upon completion of the independent study and DOD funding decision.
3. Develop a test and evaluation strategy for ECAPS and more generally for each JIE capability objective with funded initiatives.
4. Conduct thorough cybersecurity testing of JIE capabilities.

Joint Regional Security Stack (JRSS)

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted an operational assessment (OA) that demonstrated that the Joint Regional Security Stack (JRSS) Version 1.5, as fielded by the Air Force, is unable to help network defenders protect the network against operationally realistic cyber-attacks. This is because integration of the disparate commercial technologies is complex and the JRSS training and standard operating processes are not yet mature enough to take advantage of the capabilities offered by the equipment.
- In accordance with DOD Chief Information Officer (CIO) guidance, the Army, Air Force, and other DOD components continue to deploy JRSS to operational DOD networks, despite testing that demonstrates JRSS technology integration, training, and Service and agency processes are not able to protect networks from cyber-attacks.
- The Air Force JRSS operators state that JRSSs are undermanned; Defense Information Systems Agency (DISA) Global is staffed for four stacks but manages nine, and the Air Force is at 50 percent manning for JRSS. DISA and the Services need to ensure that fielding and JRSS training are synchronized to overcome shortfalls.
- The Senior Advisory Group (SAG) for JRSS wisely delayed the IOT&E until 2QFY19 to assure test adequacy and Red Team availability for the cybersecurity Adversarial Assessment.



B/P/C/S - Base, Post, Camp, Station
CSC - Carrier Supporting Carrier
JB-CE - Joint Base - Customer Edge
JR-CE - Joint Router- Customer Edge
JRSS - Joint Regional Security Stack
MPLS - Multi-Protocol Label Switching
NEC - Network Enterprise Center
NIPR - Non-classified Internet Protocol Router Network

Capability and Attributes

- As a component of the Joint Information Environment (JIE), JRSS is a suite of equipment intended to perform firewall functions, intrusion detection and prevention, enterprise management, and virtual routing and forwarding, as well as provide a host of network security capabilities. Neither JIE nor JRSS is a program of record.
- The JRSS is intended to centralize and standardize network security into regional architectures instead of locally distributed, non-standardized architectures at different levels of maturity and different stages in their lifecycle at each military base, post, camp, or station.
- Each JRSS includes racks of equipment, which allow DOD components to intake, process, and analyze large sets of network data.
- The Services and DISA intended to deploy JRSS on both the Non-classified Internet Protocol Router Network (NIPRNET (N-JRSS)) and SECRET Internet Protocol Router Network (SIPRNET (S-JRSS)).
- DISA is the designated approving and certification authority for both JRSS equipment and multiprotocol label switching (MPLS) equipment.
- MPLS is part of a modernization effort to upgrade the bandwidth capacity of the Defense Information Systems Network (DISN). DISA will implement MPLS/JRSS-enabling technology to increase network speed and manage the traffic flows.
- A key component of JRSS is the Joint Management System (JMS) that provides centralized management of cybersecurity services required for DOD Information Network (DODIN) operations.

Mission

DISA and the Services intend to use JRSS to enable DOD cyber defenders to continuously monitor and analyze the DODIN for increased situational awareness to minimize the effects of cyber threats while ensuring the integrity, availability, confidentiality, and non-repudiation of data.

Vendors

DISA is the lead integrator for JRSS. The tables below lists the current Original Equipment Manufacturers (OEMs) of the JRSS capabilities.

OEM	OEM Location
A10	San Jose, California
Argus	Houston, Texas
Axway	Phoenix, Arizona
Bivio	Pleasanton, California
BMC	Houston, Texas
Bro	Berkeley, California
Cisco	San Jose, California
Citrix	Fort Lauderdale, Florida
CSG International	Alexandria, Virginia
Dell	Round Rock, Texas
EMC	Santa Clara, California
F5	Seattle, Washington
Fidelis	Bethesda, Maryland
Gigamon	Santa Clara, California
HP	Palo Alto, California
IBM	Armonk, New York
InfoVista	Ashburn, Virginia
Juniper	Sunnyvale, California

OEM	OEM Location
Micro Focus	Rockville, Maryland
Microsoft	Redmond, Washington
Niksun	Princeton, New Jersey
OPSWAT	San Francisco, California
Palo Alto	Santa Clara, California
Quest	Aliso Viejo, California
Raritan	Somerset, New Jersey
Red Hat	Raleigh, North Carolina
Red Seal	Sunnyvale, California
Riverbed	San Francisco, California
Safenet	Belcamp, Maryland
Symantec	Mountain View, California
Trend Micro	Irving, Texas
Van Dyke	Albuquerque, New Mexico
Veeam	Columbus, Ohio
Veritas	Mountain View, California
VMWare	Palo Alto, California

Activity

- DISA and JITC conducted an OA of N-JRSS version 1.5 in July 2017 in accordance with a DOT&E-approved test plan.
- Also in July 2017, the DOD CIO approved and signed the JRSS Test and Evaluation Strategy version 1.14.
- In August 2017, U.S. Cyber Command (USCYBERCOM) signed the JRSS Concept of Operations, which provides the foundational concepts and operational framework for the integration and synchronization of joint Cyberspace Operations that leverage JRSS.
- The JIE Executive Committee approved the "JRSS Operations Training Requirements Document" in April 2017; the purpose of the document is to codify training requirements that will "lead to a future JIE state of enterprise training standardization."
- In September 2017, the JRSS SAG deferred the JRSS IOT&E to 2QFY19 with the following conditions:
  - Conduct another OA of N-JRSS version 1.5 in 2QFY18 to establish N-JRSS version 1.5 operational performance, after addressing the shortfalls discovered during the July 2017 OA.
  - Conduct an OA of N-JRSS version 2.0 in 1QFY19 that will include participants from the Army, Air Force, Navy, DISA Global, and potentially other DOD components.
- The JRSS SAG deferred the IOT&E for the following reasons:
  - To alleviate a test adequacy concern: not all planned traffic (email) would have traversed JRSS during the IOT&E because the Air Force would not have retired the associated Gateways. One of the purposes of the IOT&E is to help inform the Air Force of the risk of retiring all of their legacy Gateways, which currently provide some cybersecurity capability.
  - Lack of available cyber Red Teams to conduct the test.
  - A USCYBERCOM scheduled Period of Non-Disruption, which would have prevented a failover test.
  - To provide time for the Services and DISA to mitigate problems identified in the OA.

Assessment

- The OA demonstrated that the JRSS, as fielded by the Air Force, is unable to help network defenders protect the network against operationally realistic cyber-attacks. This is because integration of the disparate commercial technologies is complex and the JRSS training and standard operating processes are not yet mature. The following shortfalls contributed to poor JRSS cybersecurity performance:
  - Although the JRSS uses mature, commercial-off-the-shelf technologies, JRSS operator training lags behind JRSS deployment, and is not sufficient to prepare operators to

effectively integrate and configure the complex, room-sized suite of JRSS hardware and associated software.
  - The Services, DISA, and USCYBERCOM have not codified JRSS joint tactics, techniques, and procedures to ensure unity of defensive effort and enhance defensive operations.
  - Air Force JRSS operators state that JRSSs are undermanned; DISA Global is staffed for four stacks but manages nine, and the Air Force is at 50 percent manning for JRSS.
- DOT&E intends to publish a classified report on the OA results in January 2018.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendations.
  1. The CIO and the Services should discontinue deploying JRSS until the JRSS demonstrates that it is capable of helping network defenders to detect and respond to operationally realistic cyber-attacks.
  2. Because of the lack of trained personnel, DISA and the Services should conduct training and deployment analysis to ensure sufficient trained personnel are available to meet fielding schedules.
  3. The JRSS Program Office should use operationally realistic testing results to improve current JRSS configurations, training, procedures, and inform future JRSS fielding decisions.
  4. The JRSS Program Office should work closely with JITC to schedule and fund adequate FOT&E of future incremental versions of both N-JRSS and S-JRSS.
  5. DISA and the Services should conduct periodic cyber assessments of the JRSS, using a threat representative Persistent Cyber Opposing Force, to discover and address critical cyber vulnerabilities.

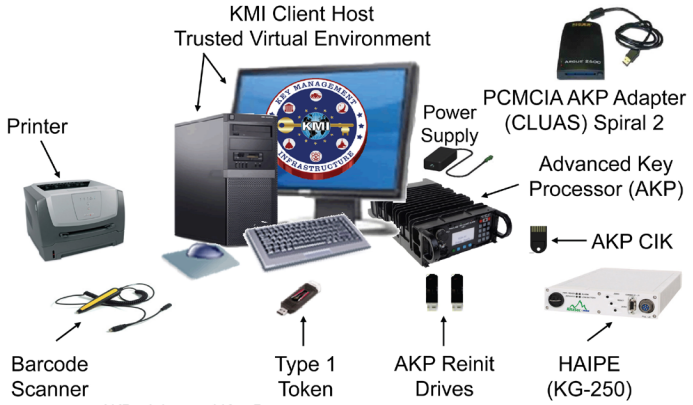
Key Management Infrastructure (KMI) Increment 2

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted an adequate Limited User Test (LUT) of Key Management Infrastructure (KMI) Spiral 2, Spin 2 capabilities in June/July 2017 in accordance with a DOT&E-approved test plan.
- DOT&E published its KMI Spiral 2, Spin 2 LUT Report in late September 2017 that found KMI to be operationally effective and operationally suitable for day-to-day operations, but not suitable for long-term sustainment.
- The KMI Program Management Office (PMO) should address the seven Priority 2 defects discovered during the LUT.
- Sustainment, manpower, KMI Training System (KMITS), configuration management, and documentation problems prevent KMI from being operationally suitable for long-term sustainment.
- The KMI PMO plans to eliminate some late Increment 2 requirements and interfaces (e.g., the Enterprise Service Bus that interoperates with the Dynamic Product Catalog, automating the Legacy Catalog Manager function for symmetric key generation requests). The KMI PMO should delay the KMI Increment 2 FOT&E until the system architecture, critical Spin 3 functionality, and interfaces are ready for test.

System

- KMI is intended to replace the legacy Electronic Key Management System (EKMS) to provide a means for securely ordering, generating, producing, distributing, managing, and auditing cryptographic products (e.g., encryption keys, cryptographic applications, and account management tools).
- KMI consists of core nodes that provide web operations at sites operated by the National Security Agency (NSA), as well as individual client nodes distributed globally, to enable secure key and software provisioning services for the DOD, the Intelligence Community, and other Federal agencies.
- KMI combines substantial custom software and hardware development with commercial off-the-shelf computer components. The custom hardware includes an Advanced Key Processor for autonomous cryptographic key generation and a Type 1 user token for role-based user authentication.



The commercial off-the-shelf components include a client host computer with monitor and peripherals, High Assurance Internet Protocol Encryptor (KG-250), printer, and barcode scanner.

Mission

- Combatant Commands, Services, DOD agencies, other Federal agencies, coalition partners, and allies will use KMI to provide secure and interoperable cryptographic key generation, distribution, and management capabilities to support mission-critical systems, the DOD Information Networks, and initiatives such as Cryptographic Modernization.
- Service members will use KMI cryptographic products and services to enable security services (confidentiality, non repudiation, authentication, and source authentication) for diverse systems such as Identification Friend or Foe, GPS, Advanced Extremely High Frequency Satellite System, and Warfighter Information Network – Tactical.

Major Contractors

- Leidos – Columbia, Maryland (Spiral 2 Prime)
- SafeNet – Belcamp, Maryland
- L3 Communications – Camden, New Jersey

Activity

- JITC conducted an operational assessment (OA) of KMI Spiral 2, Spin 2 capabilities in January/February 2017 in accordance with a JITC-approved test plan. JITC approved the test plan in accordance with delegated authority in the DOT&E policy memorandum, "Guidelines for OT&E of Information and Business Systems," September 14, 2010.

To support agile acquisition and fielding approaches, DOT&E delegates test plan approval on an assessment of moderate or low overall risk to mission accomplishment of new software integration. The KMI Spiral 2, Spin 2 OA was assessed as low risk.

- DOT&E published its KMI Spiral 2, Spin 2 OA Report in early April 2017.
- The KMI PMO received new Model H KMI tokens in 2017 that need to be integrated and tested.
- JITC conducted a LUT of KMI Spiral 2, Spin 2 capabilities in June/July 2017 in accordance with a DOT&E-approved test plan.
- DOT&E published its KMI Spiral 2, Spin 2 LUT Report in late September 2017.
- During the LUT, JITC examined new KMI capabilities and enhancements for supporting:
  - F-22 Raptor
  - Advanced Extremely High Frequency and Mobile User Objective System satellite systems
  - Benign fill (a cryptographic key wrapped within an encryption key known only between the device wrapping it and the end unit)
  - Secure Terminal Equipment enhanced cryptographic cards
  - Site failover
  - EKMS and KMI client workstation transition procedures
- The KMI PMO and JITC plan to conduct a Spin 3 OA and an Increment 2 FOT&E in early FY18; however, some externally provided critical interfaces will not be ready to support this schedule.
- The KMI Program Manager deferred Window 10 client migration until after the projected KMI Increment 2 Full Deployment Decision projected for late March 2018.

Assessment

- KMI Spiral 2, Spin 2 builds upon the existing KMI operational baseline, and automates some key management and delivery actions. The Spin 2 software incorporates NSA-approved specifications and protocols that will allow commercial developers to create new KMI-aware devices with increased security to protect key material from compromise.
- KMI Spin 2 provides a Non-classified Internet Protocol Router Network capability that will allow the Service and agency key managers to complete the transition from the legacy EKMS to KMI for remote user sites.
- The KMI Program Manager delayed the start of the KMI Spiral 2, Spin 2 OA to correct deficiencies found during earlier developmental testing. The KMI team's troubleshooting efforts during the brief delay yielded a stable KMI client software baseline, notably reduced defects, and improved JITC's ability to accomplish all of the OA goals.
  - During the OA, all Spin 2 capabilities and enhancements performed as required, although JITC assessed some of the transformational capabilities using developer-provided emulators that JITC has not independently validated.
  - JITC discovered only three Priority 2 defects during the Spin 2 OA; none precluded KMI software deployment for the Spin 2 LUT. The positive OA results demonstrated that the KMI Spiral 2, Spin 2 software baseline was mature and posed low risk to operations to deploy into the production environment for the June 2017 LUT.
  - The KMI Spin 2 OA demonstrated that the KMI PMO did not adequately maintain the KMI Test Infrastructure, which the NSA uses for both system development and software maintenance testing, at the same level as the NSA does for the operational KMI system. This sustainment lapse led to unnecessary test interruptions and delays, with some users experiencing problems with system access because of a lack of reverification of their KMI roles. Because the NSA will use the KMI Test Infrastructure to test maintenance releases throughout the KMI system lifecycle, it is important from a sustainment perspective that the NSA give the same attention to configuration management for both the operational and test instantiations of the KMI system.
- The LUT demonstrated that KMI Spiral 2, Spin 2 is operationally effective and operationally suitable for day-to-day operations, but not suitable for long-term sustainment.
- JITC evaluated all of the new Spin 2 capabilities during the LUT that did not require the use of an emulator. All KMI capabilities in previous releases continued to function to support the operational missions. JITC discovered seven Priority 2 defects during the LUT.
- The LUT showed that sustainment, manpower, KMITS, configuration management, and documentation problems still exist that hamper long-term sustainment.
  - Service and agency Regional Sparing Warehouses are not yet fully established and provisioned as defined in published Service sustainment plans.
  - KMI staffing, especially at the alternate site and civil support facilities, is not sufficient to support all existing and planned new capabilities, networks, and users.
  - KMITS availability is insufficient to support user training because of excessive unplanned downtime. All Services reported KMITS availability shortfalls ranging from hours to days per 2-week class.
  - KMI did not have accurate universal key installation procedures and system configuration management to support asymmetric key ordering.
  - The KMI PMO was 2 months late in providing the Services with proper network change requests and KMI-related Authority to Operate documentation.
- The KMI PMO plans to eliminate some late Increment 2 requirements and interfaces (e.g., the Enterprise Service Bus that interoperates with the Dynamic Product Catalog, automating the Legacy Catalog Manager function for symmetric key generation requests). This will delay delivery of critical functionality, and leave the system architecture in an incomplete state for the Increment 2 FOT&E as currently scheduled by the PMO. The KMI PMO currently does not have plans to operationally test changes to the KMI system architecture and any NSA-deferred Increment 2 requirements and interfaces for the Services.
- KMI has 4 operational test events in 13 months from January 2017 through January 2018. The PMO is exhausting

the Service users and test team, trying to achieve a March 2018 Full Deployment Decision. Normally, two operational test events in a year is a major endeavor. The KMI PMO is not ready for the Increment 2 FOT&E, and it is deferring critical capabilities to maintain schedule.

Recommendations

- Status of Previous Recommendations. The KMI PMO satisfactorily addressed one of three previous FY16 recommendations. The following remain:
  1. Ensure shared test resources are synchronized with competing NSA program and sustainment efforts, and continue to maintain an overall schedule that is executable with coordinated Service support and participation.
  2. Improve KMITS connectivity, software updating, and sustainment support for KMI courses and student training.
- FY17 Recommendations.
  1. The KMI PMO should:
     - Resolve all Priority 2 defects and verify acceptability to users prior to Spin 2 full deployment.
     - Maintain the KMITS to the same degree as the operational environment to support Service and agency training schedules.
     - Continue to improve token reliability and production quality control.
     - Provide network change and coordinating documentation to the Services with enough lead time for the Services to make those changes without using crisis management processes to support KMI efforts, particularly as it pertains to universal changeover.
     - Delay the KMI Increment 2 FOT&E until the system architecture, critical Spin 3 functionality, and interfaces are ready for test.
     - Plan for JITC to conduct a post-Increment 2 OA and LUT to evaluate KMI client upgrades to Windows 10, since the PMO delayed integrating that operating system until beyond Spin 3.
     - Establish a more realistic timeline for future KMI capability testing that supports revised milestone decisions, while managing expectations of those with KMI equities.
  2. NSA's KMI Operations should:
     - Improve KMI configuration management and develop procedures for loading universal keys for asymmetric key generation.
     - Reassess KMI Operations staffing to ensure that it can support all existing and planned new capabilities, networks, sites, and users.
  3. Services and agencies should:
     - Establish and provision Regional Sparing Warehouses per their sustainment plans to meet client availability and Administrative and Logistics Delay Time requirements.
  4. JITC should:
     - Determine how and under what conditions transformation capabilities will be tested in a live operational environment.
     - Evaluate the new Model H KMI token for reliability during Spin 3 OA and Increment 2 FOT&E.

Next Generation Chemical Detector (NGCD)

Executive Summary

- The Services and National Guard Bureau intend for the Next Generation Chemical Detector (NGCD) program to provide chemical detection and identification systems to detect and identify chemical warfare agents (CWA), non-traditional agents, and toxic industrial chemicals (TIC) in various physical states to support force protection decisions, situational awareness, and battle management decisions.
- The Services conducted Early Operational Assessments of prototype systems to assess the potential contribution of the NGCD detection and identification technologies in various operational mission scenarios to inform operational requirements and entry into the Milestone B Engineering Manufacturing Development phase of the acquisition program.
- The NGCD prototype systems demonstrated poor performance in the areas of detection, automated algorithm identification, reliability, and operator usability.
- In October 2017, the program manager made the decision to extend the Technology Maturation and Risk Reduction phase of the NGCD Increment 2 acquisition program based on the poor demonstrated technical and operational performance.

System

- The NGCD program consists of four increments of capability to detect and identify CWA, non-traditional agents, and TIC hazards in different physical states in support of the Joint Forces and the National Guard Bureau Civil Support Teams.
- The Services and the National Guard Bureau intend for:
  - NGCD Increment 1 to detect CWA and TIC in aerosol and vapor form, and alert personnel to an attack to support post-attack actions, such as reconnaissance, surveillance, and decontamination operations.
  - NGCD Increment 2 to detect and identify CWA and non-traditional agents in liquid and solid states to characterize threats on various surfaces to support hazard warning, force protection, situational awareness, and battle management decisions.
  - NGCD Increment 3 to collect samples, transfer the samples to a chemical analysis capability, and analyze and characterize the sample to determine the presence of target chemicals.
  - NGCD Increment 4 to be a wearable detector to alert personnel to the presence of chemical vapors and explosive atmospheres that present an immediate hazard. The Increment 4 program will be initiated upon completion of research and development efforts.

Mission

Commanders of Joint Forces and the National Guard Bureau Weapons of Mass Destruction Civil Support Teams intend to employ the NGCD systems to detect, characterize, and identify chemical hazards in order for the force to take protective measures and mitigating actions to continue military operations.

Major Contractors

- NGCD Increment 1:
  - Smiths Detection, Inc. – Edgewood, Maryland
  - Chemring Sensors and Electronic Systems, Inc. – Charlotte, North Carolina
  - Signature Science, LLC – Austin, Texas
- NGCD Increment 2:
  - Smiths Detection, Inc. – Edgewood, Maryland
  - Chemring Sensors and Electronic Systems, Inc. – Charlotte, North Carolina
  - Nomadics, Inc. – Stillwater, Oklahoma
  - ChemImage Bio Threat, LLC – Pittsburgh, Pennsylvania
- NGCD Increment 3:
  - Bruker Detection Corporation – Billerica, Massachusetts
  - Chemring Sensors and Electronic Systems, Inc. – Charlotte, North Carolina
  - Battelle Memorial Institute – Columbus, Ohio

Activity

- The Army Operational Test Command conducted a Multi-Service Early Operational Assessment of the NGCD at Fort Hood, Texas, from October 24-27, 2016.
- The Navy's Operational Test and Evaluation Force conducted an Early Operational Assessment of the NGCD aboard the USS *Bataan* (LDH 5) in port at the Naval Station Norfolk, Virginia, from November 14-17, 2016.
- The Early Operational Assessments were conducted in accordance with the DOT&E-approved test plan.
- The Edgewood Chemical and Biological Center conducted Final Prototype Testing of the NGCD Increment 1 from 4QFY16 through 1QFY17 in Edgewood, Maryland.
- The Edgewood Chemical and Biological Center conducted Final Prototype Testing of the NGCD Increment 3 from 1QFY17 to 2QFY17.
- In October 2017, the program manager extended the Technology Maturation and Risk Reduction phase of the NGCD Increment 2 program based on the poor technical and operational performance demonstrated.

Assessment

NGCD Increment 1

- The NGCD Increment 1 prototype systems demonstrated detection performance that was many orders of magnitude short of the operational requirement for some agents during prototype agent testing. The false alarm rate of the detectors could not be assessed due to poor detector sensitivity.
- The demonstrated vapor detection capability for traditional chemical agents was generally worse than, and in one case no better than, that of the currently fielded Joint Chemical Agent Detector.
- Prototype system reliability was poor and hindered the ability to collect planned test data in some instances.
- The size and weight of the prototype systems reduced operators' ability to effectively employ the systems during some missions.

NGCD Increment 3

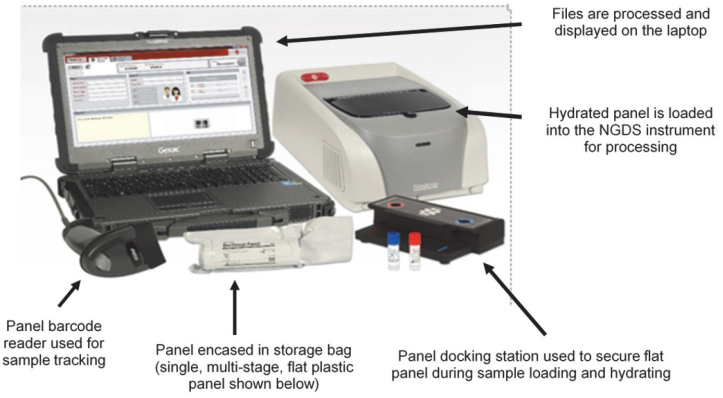
- Prototype systems were able to identify chemical agents at or near the required limit of identification or sensitivity for liquids and solids.
- The systems experienced significant false identification of chemical agents in samples.
- Prototype system reliability was poor during the Early Operational Assessment.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendations. The program manager should:
  1. Conduct additional technology development to improve detection and identification performance and plan false detection testing in concert with agent testing.
  2. Implement a reliability growth program and continuously assess progress.

Next Generation Diagnostic System (NGDS) Increment 1

Executive Summary
- The Next Generation Diagnostics System (NGDS) is a polymerase chain reaction analytical instrument to aid in the diagnosis of biological warfare agent (BWA)-related illnesses and environmental sample analysis to identify the presence of BWA in the operational environment.
- The NGDS is operationally effective and suitable for clinical use by deployable medical units to support the diagnosis and treatment of BWA associated illnesses.
- Emerging test results indicate that the NGDS provides a timely, accurate, and reliable capability to identify BWAs in environmental samples to support force protection decisions.



System
- The NGDS Increment 1 is the FilmArray 2.0 commercial off-the-shelf liquid sample polymerase chain reaction analytical instrument with automated sample preparation.
- The NGDS uses the Warrior Panel for BWA identification in clinical samples (e.g., blood, blood culture, and sputum) and the Sentinel Panel for BWA identification in environmental samples (e.g., air, soil, and water).
- The system includes a ruggedized computer, software, ruggedized transport case, optical handheld barcode scanner, optical mouse, power and communication cables, pouch loading module, consumable assays, and an operator's manual with sample protocols.
- The Services intend to use the NGDS Increment 1 in existing microbiology laboratories equipped with common laboratory support equipment such as Class II Biological Safety Cabinet, refrigerator, freezer, level work surfaces, line power sources, lighting, and appropriately trained laboratory personnel.

Mission
- Commanders intend to employ trained clinical laboratory technicians equipped with the NGDS Increment 1 to identify BWAs and infectious diseases in clinical specimens to support medical provider's clinical diagnosis and treatment decisions.
- Commanders intend to employ trained laboratory technicians equipped with NGDS to identify BWAs in environmental samples to confirm a potential BWA incident and support Force Health Protection decision-making.

Major Contractor
BioFire Defense, LLC – Salt Lake City, Utah

Activity
- The U.S. Army Medical Research Institute of Infectious Disease at Fort Detrick, Maryland, and Battelle Memorial Institute in Aberdeen, Maryland, conducted combined developmental/operational live agent testing of the NGDS Sentinel Panel and BioFire FilmArray device from April to December 2017.
- The Army Research Laboratory Survivability Lethality Analysis Directorate conducted a cybersecurity Cooperative Vulnerability and Penetration Assessment of the NGDS from July 11-12, 2017, at the Army Medical Department Center and School (AMEDDC&S) in San Antonio, Texas.
- The Army Threat Systems Management Office conducted a cybersecurity Adversarial Assessment of the NGDS from July 31 to August 4, 2017, at the AMEDDC&S.
- The Navy's Operational Test and Evaluation Force conducted IOT&E of the NGDS from August 21 to September 9, 2017, aboard USNS *Comfort* and USS *Gerald R. Ford* and at the Naval Environmental Preventive Medical Unit, Naval Station Norfolk, Virginia.
- The operational testing was conducted in accordance with DOT&E-approved test plans. DOT&E approved changes to the planned test dates and locations due to unanticipated Navy ship support to Hurricanes Harvey and Irma.

Assessment
- The NGDS is operationally effective in providing deployable medical units with timely clinical sample analysis to aid in the diagnosis of anthrax, plague, tularemia, Q fever, and the hemorrhagic fevers caused by Ebola and Marburg viruses, in response to a suspected or confirmed bioterrorism event or outbreak.
- The NGDS provides increased breadth of diagnostic coverage through compatibility with four FDA-approved commercially

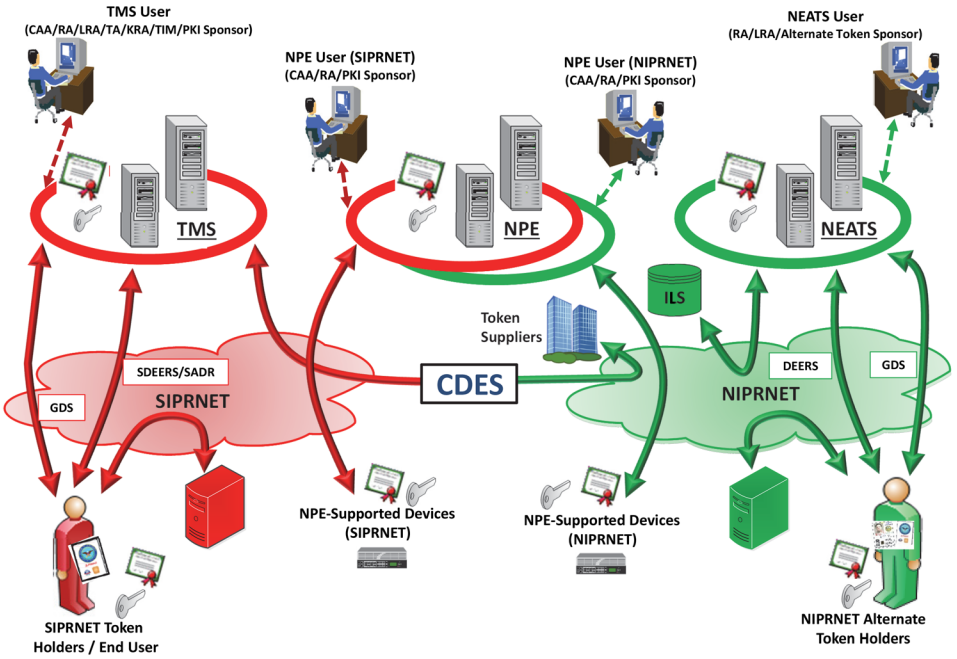
available common infectious diseases panels enabling day-to-day use of the system.
- Emerging results from the combined developmental/operational live agent testing of the NGDS Sentinel Panel indicate the system identifies BWAs present in environmental samples at similar or lower levels than the Joint Biological Agent Diagnostic Systems (JBAIDS), which the Services intend to replace.
- The NGDS is operationally suitable for clinical and environmental sample analysis. It is easy to use, demonstrated 98.6 percent probability of completing analysis of 5 samples without an operational mission failure, and has a smaller operational footprint that the JBAIDS.

Recommendations
- Status of Previous Recommendations. The Services have addressed the previous recommendations.
- FY17 Recommendations.
  1. The Services should develop and implement plans to educate medical providers at units receiving NGDS on the capabilities provided and the diversity of assays available to support medical diagnostics.
  2. The Program Office should provide sample preparation procedures on a single document to improve the logical flow of information.

Public Key Infrastructure (PKI) Increment 2

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted an FOT&E of the Increment 2 Spiral 3 Public Key Infrastructure (PKI) capabilities in August and September 2017 in accordance with a DOT&E-approved test plan.
- The Spiral 3 FOT&E examined enhancements to the Token Management System (TMS) including a new Central Management of Tokens (CMT) capability, end-user certificate rekey, an Advanced Reporting System (ARS), and the ability to terminate expired certificates in batches. The FOT&E also examined sustainability processes including help desk, system administration, failover, training, and documentation.
- Preliminary PKI FOT&E findings and observations indicate the Spiral 3 TMS, CMT, and ARS capabilities are working with a few problems pertaining to second source tokens, certificate rekey and revocation, and help desk processes.
- DOT&E published the PKI Spiral 3 FOT&E Report in December 2017.



System

- DOD PKI provides for the generation, production, distribution, control, revocation, recovery, and tracking of public key certificates and their corresponding private keys. DOD PKI supports the secure flow of information across the DOD Information Network as well as secure local storage of information.
- The primary purpose of the SECRET Internet Protocol Router Network (SIPRNET) TMS is to issue tokens and certificates to end users. The private keys are encoded on the token, which is a smartcard embedded with a microchip.
  - The National Security Agency (NSA) manages TMS with operational support from the Defense Information Systems Agency (DISA), which hosts the infrastructure and provides PK-enabling support for DOD. TMS uses the Defense Manpower Data Center's Secure Defense Enrollment Eligibility Reporting System (SDEERS) as the authoritative data source for personnel data and provides capabilities for token formatting, user registration, token enrollment, token personal identification number reset, token suspension and restoration, token revocation, and encryption private key escrow and recovery.
  - TMS uses commercial off-the-shelf hardware and software components using Linux-based operating systems hosted at the DISA Enterprise Service Centers in Mechanicsburg, Pennsylvania, and Oklahoma City, Oklahoma.
- The NSA deployed PKI Increment 1 on the Non-classified Internet Protocol Router Network (NIPRNET) with access control provided through Common Access Cards (CACs). The NSA is developing and deploying PKI Increment 2 in four spirals on SIPRNET and NIPRNET. The NSA deployed Spirals 1 and 2, while Spirals 3 and 4 will deliver TMS enhancements, inventory logistics tools, an enterprise-level alternate token issuance and management system (for system administrators) on the NIPRNET, and an enterprise-level Non-Person Entity (NPE) (e.g., workstations, routers, and web servers) for certificate issuance and system management.

Mission

- Commanders at all levels will use DOD PKI to provide authenticated identity management via personal identification number-protected CACs or SIPRNET tokens to enable DOD members, coalition partners, and others to access restricted websites, enroll in online services, and encrypt and digitally sign email.
- Military operators, communities of interest, and other authorized users will use DOD PKI to securely access,

process, store, transport, and use information, applications, and networks.
- Military network operators will use NPE certificates for workstations, web servers, and mobile devices to create secure network domains, which will facilitate intrusion protection and detection.

Major Contractors
- General Dynamics Mission Systems – Dedham, Massachusetts (Prime)
- 90Meter – Newport Beach, California
- SafeNet Assured Technologies – Abington, Maryland

Activity
- USD(AT&L) approved the fielding of the PKI Spiral 3, Release 4 TMS capabilities in January 2017 for DOD-wide use.
- The PKI Program Management Office (PMO) procured 566,500 second source Giesecke and Devrient (G&D) tokens for the DOD, that the Services and agencies later discovered were not interoperable with some thin and zero client environments.
- The PKI PMO developed a SIPRNET DISA Integration Lab (DIL) in March 2017 that provided limited system capacity and did not adequately represent the operational environment.
- The PKI PMO conducted a 2-week sustainment review in July 2017 to address problems with token failure tracking, help desk processes, token inventory logistics, and new token deployment processes.
- JITC conducted an FOT&E of the Spiral 3 PKI capabilities in August/September 2017 in accordance with a DOT&E-approved test plan. DOT&E published the PKI Spiral 3 FOT&E Report in December 2017.
- The Spiral 3 FOT&E examined enhancements to TMS including a new CMT capability, end-user certificate rekey, an ARS, and the ability to terminate expired certificates in batches. The FOT&E also examined sustainability processes including help desk, system administration, failover, training, and documentation.
- DOT&E approved the PKI Spiral 4 Test and Evaluation Master Plan (TEMP) Addendum in October 2017. The PKI Spiral 4 TEMP Addendum covers NPE automated device certificate issuance system and NIPRNET Enterprise Alternate Token System (NEATS).
- JITC plans to conduct a Spiral 4 operational assessment of NPE and NEATS in February 2018 and an Increment 2 FOT&E from May to June 2018.

Assessment
- CMT, ARS, and Nagios system health and monitoring capabilities operate properly but testing revealed that during routine failovers between the two TMS sites, ARS and CMT did not fail over correctly, requiring manual troubleshooting.
- The PKI PMO made improvements to training and documentation through classroom and on-demand, web-based training modules.
- The preliminary PKI Spiral 3 FOT&E findings are:
  - The Spiral 3 capabilities work. However, some deficiencies across the PKI capability set remain.
    - Registration Authorities successfully configured CMT to accept new tokens into their inventories, transfer tokens to affiliated sites, and place token orders. Token Inventory Managers confirmed that their inventories automatically updated as tokens transitioned between states (e.g., issued, blacklisted, and failed).
    - A small set of 50 end users demonstrated the ability to rekey their tokens within 60 days of expiration. However, in some cases, network configuration changes were required and Registration Authorities needed to confirm revocation of the users' original certificates.
    - An automated token termination server-side process terminated approximately 8,000 expired tokens in bulk, allowing Registration Authorities to reuse stacks of tokens without manually revoking each token individually.
    - Registration Authorities experienced sporadic problems revoking certificates, and end users with newly issued tokens experienced intermittent problems logging on, or digitally signing and encrypting emails.
    - The newly deployed second source G&D tokens do not work in many thin and zero client environments. The PKI PMO has been aware of the token problem since December 2016, but did not initiate a root cause analysis effort. Services and agencies only became aware of the problem when they employed the G&D tokens in the operational environment.
  - Some new Spiral 3 and long-standing Increment 2 deficiencies across the PKI capability set remain.
    - Token failure estimates as reported through TMS may prove to be inaccurate despite the inclusion of a token failure reporting mechanism. Services and agencies track internal failures and do not uniformly use the new TMS reporting process.
    - The PKI PMO piloted a new SIPRNET DIL in February 2017 to support developmental testing; however, the DIL lacked the necessary operational relevance to avert problems discovered after deployment.
    - A token reliability test, conducted using a sample of 365 users, concluded that second source tokens achieved a Mean Time to Failure (MTTF) of 26,605 hours whereas the SafeNet version 4.0c tokens achieved a MTTF of 1,175 hours at the 80 percent confidence level. Both tokens failed to meet the target MTTF of 43,000 hours, which assumes a 3-year life span and an 8-hour per day

usage profile. The existing requirement is in question because usage profiles of the sample population indicate tokens may be used for less than 1 hour per day for the majority of users and for much longer durations per day for a small subset of users. The data confirms that the G&D tokens can support the required 3-year life span given a 5-hour usage per day profile whereas the SafeNet 4.0c tokens can support approximately 13 minutes per day over the required 3 years.

- The PKI PMO deployed the second source token types without adequate beta testing in realistic operational environments resulting in interoperability findings with existing thin and zero clients across the DOD.
- Help desk processes remain inadequate because Registration Authorities continue to contact the PKI PMO directly for Tier III support, therefore losing the benefit of a trouble ticket tracking and reporting system.
- ARS is more widely used since the 2016 Limited User Test but remains difficult to use without assistance from experienced users.

Recommendations

- Status of Previous Recommendations. The PKI PMO satisfactorily addressed two of three previous FY16 recommendations. The PKI PMO still should provide periodic reports of token reliability, failure rates, and root cause analyses.
- FY17 Recommendations. The PKI PMO should:
  1. Implement a sustainable token reliability testing and certification process to ensure new tokens work in existing DOD thick, thin, and zero client environments.
  2. Establish an operationally representative DIL to properly examine TMS and NPE capabilities in a test environment. To support long-term sustainment, ensure the DIL is available for the Services and agencies to interconnect and test device and middleware variants.
  3. Establish an integrated product team to address sustainability problems through transition of the program to DISA.

Army Programs

Army Programs

Army Network Modernization

The FY16 National Defense Authorization Act directed the DOD to conduct a comprehensive assessment of the current and future capabilities and requirements of the Army's air-land, mobile tactical communications and data networks, including technological feasibility, suitability, and survivability. Taking into account the study findings, the Army conducted a comprehensive review of the entire network to assess the processes, reduce system vulnerabilities, redefine capability gaps, and improve the equipment needed in the force to "fight and win" today and to innovate to develop future systems.

The Army made the following decisions as a result of their comprehensive review:

- Cancel the Mid-tier Networking Vehicular Radio (MNVR).
- Cancel Command Post of the Future (CPOF).
- Limit procurement and fielding of Warfighter Information Network – Tactical (WIN-T) Increment 2.
- Rewrite the request for proposals for the Handheld, Manpack, Small (HMS) Form Fit Leader Radio to allow for competition of a more capable system.
- Establish an Information Technology Oversight Council to oversee integration of all network-related efforts in the Army.
- Designate lead organizations for network requirements and Army information technology integration.

- Propose an "adapt and buy" acquisition approach for network capabilities.
- Create and enforce a standards-based open architecture to include a unified transport layer and unified mission command suite of systems and applications.

NETWORK INTEGRATION EVALUATION (NIE)

The purpose of the NIEs is to provide a venue for operational testing of Army acquisition programs, with a particular focus on the integrated testing of tactical mission command networks. The Army intended the NIEs to serve as a venue for evaluating emerging capabilities. These systems, termed by the Army as "systems under evaluation," were not intended to be acquisition programs of record, but rather systems that may offer value for future development. That intent has evolved such that acquisition programs of record are using NIE as a venue for risk reduction testing of capabilities prior to formal operational test. The Joint Warfighting Assessment, which has replaced the second annual NIE, has become the primary venue for experimentation.

The Army's intended objective of the NIE – to test and evaluate network components in a combined event – remains sound. The NIE events allow for a more comprehensive evaluation of an integrated mission command network than is possible through piecemeal evaluations of individual network components. However, the benefit is predicated on aligning multiple operational tests with a single, annual, schedule-based event. This limits the flexibility of programs to adapt to schedule delays. Delays are amplified when a program must wait for the next scheduled NIE.

NIE 17.2

During NIE 17.2, the Army conducted an FOT&E for WIN-T Increment 2 Network Operations Security Center – Lite and Tactical Communications Node – Lite. The article providing an assessment of WIN-T can be found on page 129.

NETWORK MODERNIZATION ASSESSMENT

As a result of internal and external reviews, the Army decided to adjust its Network Modernization strategy by instituting cohesive governance, revamping its acquisition approach, halting select programs of record, and realigning the funds to more promising technology. Frequent program restructuring and program delays have translated into very few radios fielded to date. The timing for the change was opportune as three major tactical radio programs, MNVR, HMS Manpack Radio, and HMS Rifleman Radio (now Leader Radio), have re-entered source selection to allow for full and open competition. At a high level, the Army has developed the first principles, characteristics, requirements, and attributes to define the network it needs to operate in a congested and contested environment against current and future peer threats. This approach of defining the overarching

characteristics of the network represents a paradigm shift in what has been to date an overly prescriptive requirements process focused on technical specifications of individual systems. To realize the benefits of this approach the Army must flow down these concepts as threshold capabilities and critical operational issues in validated program requirements documents.

The Army defined the desired network as one that enables the warfighter to fight, shoot, move, communicate, protect, and sustain. The current network components, including mission command systems and elements of the transport layer, are very complex to use. The current capability of an integrated network to enhance mission command is diminished due to pervasive task complexity. It is challenging to achieve and maintain user proficiency. Units remain dependent upon civilian field service representatives to establish and maintain the integrated network. This dependency corresponds directly to network complexity of use. The Army defined its objective network as simple and intuitive with a single mission command suite. The Army desires the future state network to be operated and maintained by soldiers without need for civilian field service representatives. The Israeli Army does not support its communications with contractors deployed at every level. Simple and intuitive networks obviate the need for contractor support.

Governance. One significant change the Army made pertains to governance. The Army established the Information Technology Oversight Council, co-chaired by the Vice Chief of Staff of the Army and the Under Secretary of the Army. The Information Technology Oversight Council will integrate all activities across the network mission areas; warfighting, intelligence, enterprise information environment, and business. The Army Chief Information Officer/G6 was designated the lead integrator, responsible for establishing a standards-based architecture. The Mission Command Center of Excellence will be responsible for synchronizing all tactical network requirements. The Chief of Staff of the Army is the final approval authority responsible for reviewing and validating requirements with operational needs through the Army Requirements Oversight Council (AROC) process.

Acquisition Approach. Another significant change the Army proposed is to institute an acquisition approach for the network of "adapt and buy." The Army does not believe the acquisition process allows for "agile procurement" of the latest technology. The intent of the new approach is to leverage industrial, joint, or special operational forces (SOF) initiatives. The details of how this will be implemented are being developed.

One concept suggested by the Army is to stand up a cross functional team (CFT). The CFT will consist of representatives from the Training and Doctrine Command; Army Materiel Command; Assistant Secretary of the Army for Acquisition, Logistics and Technology; and Army Test and Evaluation Command (ATEC). The Army intends the CFT to support streamlining and horizontal integration of requirements. The CFT will support experimentation and demonstrations of emerging capabilities. Experimentation will be used to further refine requirements and aid in system development. The idea of experimentation is similar to the original intent of the NIE, which was to evaluate emerging capabilities. The lack of new technology offered and the gradual shift to program of record evaluations reduced the benefit of this approach in the NIE.

The Army believes the pivot to a development operations (DevOps) model constitutes a major shift to the approach to modernization. The DevOps model uses continuous experimentation and user feedback to refine requirements and acquisition decisions. The Army will need to carefully define the process by which they will refine the requirements based on experimentation results.

The new acquisition approach poses some challenges the Army should consider.

- Much of the goal for a standards-based open architecture, a universal transport layer, and a unified mission command suite is predicated on the Army's ability to define these standards in light of dozens of programs of record spread across multiple Program Executive Offices.
- Experimentation and demonstration generally do not provide adequate data to make a determination of operational effectiveness and suitability. A comprehensive integrated test plan would outline the data requirements needed from experimentation through operational test and could be used to reduce the amount of duplicative testing required.
- Given the difficulty the Army is having resourcing operational tests with test units, resourcing multiple experimentation events could be a problem.
- The Army is seeking "reciprocity" for testing conducted by SOF and joint partners. If the Army plans and coordinates with SOF and joint partners to collect adequate data, this could be possible.
- As the Army selects systems to "adapt and buy," there may be a reduction in full and open competition.

Programmatic Changes. The Army asked Congress for the ability to realign funding for FY18. It intends to halt procurement of the MNVR immediately. At the Milestone C decision in November 2016, the Defense Acquisition Executive directed the Army to conduct an Analysis of Alternatives for MNVR prior to awarding a low-rate initial production (LRIP) contract. At the time, the Army decided to field the 478 MNVR radios already on contract to outfit 4 brigade combat teams for "experimentation." Operational test results demonstrated that MNVR using the Wideband Networking Waveform was not effective at providing reliable communications at doctrinally required ranges. Cancellation of this program will allow the Army to redefine the requirements for communications between battalion and companies to better meet their operational needs.

The Army announced its intent to halt procurement of CPOF as part of the new strategy. CPOF was already intended for divestiture. The Command Post Computing Environment part of the Common Operating Environment was the planned replacement.

The Army intends to halt procurement of WIN-T Increment 2 at the end of FY18. That does not constitute the end of WIN-T Increment 2 fielding. The Army will field the light versions of Network Operations Security Center and Tactical Communications Node tested during NIE 17.2, to Infantry Brigade Combat Teams. The Army will complete fielding of WIN-T Increment 2 to Stryker Brigade Combat Teams by cascading the heavy versions of Network Operations Security Center and Tactical Communications Node from the Infantry Brigade Combat Teams and procuring additional Stryker Enhanced Point of Presence. The major change in strategy is that the Army no longer plans to field WIN-T Increment 2 to Armored Brigade Combat Teams. Implementation of the WIN-T network into the Armored Brigade Combat Team was dependent upon successful development and fielding of the Armored Multi-purpose Vehicle Mission Command variant.

In advance of releasing the request for proposals for the Leader Radio, the Army revised the requirements to enable industry to offer more technologically capable radios. This represents a significant change from the original acquisition strategy. The original Leader Radio requirements specified Soldier Radio Waveform (SRW) and Single Channel Ground and Airborne Radio System (SINCGARS) as the two required waveforms for the system. This represented a change from the Rifleman Radio that only required SRW. The requirement for a two-channel radio was added because the limited range provided by SRW did not support divestiture of the legacy SINCGARS radio. A two-channel radio would obviate the need for soldiers to carry two radios. The requirement for SRW is 20 years old. Industry innovation has surpassed the capability inherent in the SRW waveform producing waveforms with routing protocols that are inherently more scalable and power efficient. It will be possible for vendors to compete with multiband radios as the Army transitions from a "lowest cost technically acceptable" to a "best value" approach.

The Army awarded a contract for test articles for the HMS Manpack in July 2017. Unlike the Leader Radio, the strategy does not allow for additional capabilities with the delivered radios for IOT&E. The Full and Open Competition Manpack Radios are required to weigh less than the LRIP versions tested in 2014. The radios have the same threshold waveform requirements of SRW and SINCGARS. The Mobile User Objective System on Manpack was tested during Multi-Service Operational Test and Evaluation (MOT&E) in 2016. The radios to be tested at IOT&E do not represent an improved capability over what has already been tested. If multiband Leader Radios are competed, they will only be interoperable with Manpack over SRW and SINCGARS.

New Technology. The Army intends to use some of the reprogramed funds for experimentation with mature joint and SOF solutions. These include capabilities for coalition and joint radio gateways with access to a tactical datalink aimed at improving joint and Army interoperability with close air support. As mentioned previously in this article, the key to successful integration of these technologies into an overarching, cohesive strategy will be dependent on development and enforcement of open architecture standards for a unified transport layer and mission command suite.

NIE ASSESSMENT

NIE 17.2 was the eleventh such event conducted to date. NIEs have been an excellent venue for conducting operational tests of network acquisition programs.

Dedicated Test Unit. For the first time since NIE inception in July 2011, a dedicated test unit did not conduct the event. Having a dedicated test unit stationed at Fort Bliss, Texas, has been a critical element in successful operational testing conducted during NIEs. It has made the planning and execution of complex brigade-sized operational tests of Army networks much more effective than would be the case if new test units were selected for each event. Past experience demonstrates that having a dedicated test unit enables good operational testing. Due to its experience and the organizational learning that occurred over time, the dedicated NIE test brigade has shown that it is more attuned to incorporating new systems into its formation for testing than has been the case with one-off test units. As a result, the system undergoes efficient operational testing and receives a thorough evaluation.

A dedicated test unit is desirable in that it relieves the stress on the U.S. Army Forces Command (FORSCOM) to designate a test unit of appropriate size each time an operational test is on the schedule for a given program. Some tests require large-scale units, up to brigade in size and, in cases where the Army is testing command and control systems, sometimes even requiring a division headquarters element. Having a dedicated test unit of a mixed composition enables all of those requirements to be met at one place. FORSCOM has struggled resourcing the force requirements for several upcoming operational tests. For example, FORSCOM did not task a company-sized unit to conduct the Joint Light Tactical Vehicle MOT&E until 3 months before the planned execution. The delay has affected ATEC's ability to develop operationally relevant missions and ensure that the unit is trained, equipped, and manned to execute these missions.

The 2nd Brigade Combat Team, 101st Airborne Division conducted NIE 17.2 and provided frank feedback on the systems under test. As an airborne unit, it conducted sling load operations in a realistic manner. The systems being tested, Network Operations Security Center – Lite and Tactical Communications Node – Lite, did not represent a significant new capability over the heavy versions. As such, the expected benefit of a dedicated test unit's experience was not required.

The 2nd Brigade Combat Team, 101st Airborne Division recently returned from deployment and had finished its reset so many of

the personnel were new to that unit. The NIE was their first field exercise as a brigade since returning from deployment. As such, some soldiers were not familiar with the unit or the equipment. This might be mitigated by sending a unit after their combat training center rotation.

Another aspect of good operational testing is a capable opposing force (OPFOR). The dedicated test brigade has been very proficient in creating this OPFOR. Good operational testing requires an aggressive, adaptive threat unit intent on winning the battle in order to adequately stress the system under test and to fully understand its capabilities. A realistic demanding OPFOR requires capabilities that are not easily assembled and integrated. These capabilities include electronic warfare and cybersecurity threats as well as a mix of heavy and light forces.

One of the most significant benefits of NIEs has been the extensive incorporation of threat information operations, such as electronic warfare and computer network operations. The integration of electronic warfare and cyber capabilities into an OPFOR requires practice and is not easily replicated by new units tasked to portray the OPFOR in operational testing. The units permanently assigned to conduct the NIEs have, over time, demonstrated the ability to employ an effective OPFOR with a variety of combat multipliers. This OPFOR capability has grown increasingly sophisticated and can be readily adapted to reflect new real-world threat capabilities. As a result, NIEs have provided numerous insights with respect to operations in this type of threat environment. The Army has initiated efforts to enhance the cyber and electronic warfare capabilities of the OPFOR at the combat training centers. Lessons learned from NIE could be used as a model to employ those capabilities.

The OPFOR unit (1st Battalion, 502nd Infantry Regiment) was deployed from Fort Campbell, Kentucky, to support operations at Fort Bliss. It was able to overcome these challenges due to the discipline, skill, and motivation of its soldiers and leaders and the presence of an exceptionally competent electronic warfare non-commissioned officer in their tactical operations center (TOC). However, it was not until the middle of the record test that the majority of TOC personnel had a full understanding of all the systems, their capabilities, and how to effectively integrate them into both current and future OPFOR operations.

To provide realistic assessments of new capabilities, the Army should maintain a robust threat during network experimentation and testing. The shift from a single annual NIE event to multiple smaller events will increase resources required to bring these enablers to each venue.

Instrumentation and Data Collection. The Army should continue to improve its instrumentation and data collection procedures to support operational testing. ATEC should devote increased effort towards developing instrumentation to collect network data for dismounted radios, such as the Manpack radio. The Army needs to place greater emphasis on the use of Real-Time Casualty Assessment instrumentation – an essential component of good force-on-force operational testing – such as that conducted at NIEs. A Real-Time Casualty Assessment is intended to accurately simulate direct and indirect fire effects for both friendly and threat forces. Finally, the Army should continue to refine its methodology for the conduct of interviews, focus groups, and surveys with the units employing the systems under test.

Abrams M1A2 System Enhancement Program (SEP) Main Battle Tank (MBT)

Executive Summary

- In January 2017, the Army continued root cause analysis of Abrams M1A2 System Enhancement Program (SEP) main gun accuracy problems noted during the Software 4.6 user Beta Test in June 2016. The Army has excluded crew error and software as possible factors leading to inaccuracy and will focus future efforts on gun tube wear.
- The Army initiated testing in February 2017 to determine how round count and tube wear affect main gun accuracy. Testing was completed in October 2017. The Army will provide updated gun tube condemnation criteria to fielded units, which includes new equivalent full charge counts for service ammunition and revised tube inspection criteria.
- As of October 2017, the M1A2 SEPv3 has completed 80 percent of planned reliability testing. The system is exceeding the operational requirement for combat mission failures, but is below the requirement for system failures. Current M1A2 SEPv3 reliability exceeds that demonstrated by the M1A2 SEPv2.
- The Army conducted ballistic testing of the Abrams Reactive Armor Tiles (ARAT) I and II in FY17. The Army continued to characterize the performance of the M1A2 SEPv3 Next Evolutionary Armor (NEA) and is scheduled to begin full-up system-level (FUSL) live fire testing for the M1A2 SEPv3 in 2QFY18.

System

- The Abrams M1A2 Main Battle Tank (MBT) is a tracked, land combat, assault weapon system designed to possess significant survivability, shoot-on-the-move firepower, joint interoperability (for the exchange of tactical and support information), and a high degree of maneuverability and tactical agility. The Army intends the M1A2 SEP to enable the crew to engage the full spectrum of enemy ground targets with a variety of point- and area-fire weapons in urban and open terrain.
- The M1A2 SEPv2 is currently fielded. It upgrades the M1A2 SEP by providing increased memory and processor speeds; full color tactical display; digital map capability; compatibility with the Army Technical Architecture; improved target detection, recognition, and identification through incorporation of second-generation Forward Looking Infrared technology and electronics; and crew compartment cooling through the addition of a thermal management system.
- The Army integrated M153A1E1 Common Remotely Operated Weapon Station (CROWS)-Low Profile (LP) into the M1A2 SEPv2. The CROWS-LP incorporates upgraded software and addresses visibility concerns associated with the M153 CROWS II by relocating the sights and laser range finder to the side of the weapon and ammunition box rather than under the weapon. This reduces the system height by 10 inches.

Common Remotely Operated Weapon Station-Low Profile (CROWS-LP)

M1A2 SEP

- M1A2 SEPv3 fielding is planned for FY20. The M1A2 SEPv3 is an upgrade to the M1A2 SEPv2. The upgrades include the following:
  - Power generation and distribution to support the power demands of future technologies.
  - Network compatibility.
  - Survivability against multiple threats by incorporating NEA, a new underbody IED kit, and other vulnerability reduction measures to reduce the tank's vulnerability to IEDs. These measures include redesigned crew seating, additional floor stiffeners, hardware to provide lower limb protection, and changes in the material and dimensions of internal structural supports.
  - Lethality by providing the ability for the fire control system to digitally communicate with the new large caliber ammunition through use of an ammunition datalink.
  - Energy efficiency (sustainment) due to the incorporation of an auxiliary power unit.
- The M1A2 SEP MBT utilizes 120 mm main gun rounds to defeat enemy targets.
  - The XM1147 Advanced Multi-purpose (AMP) Round, currently in development, is a 120 mm munition fired utilizing an ammunition datalink-equipped Abrams MBT.

The round is optimized for use in urban environments in direct support of assaulting infantry. The Army intends the round to have three defeat modes including Point Detonate (PD), Point Detonate Delay (PDD), and airburst in order to defeat a combination of targets including anti-tank guided missile teams, dismounted infantry, double reinforced concrete walls, light armor, bunkers, obstacles, and armor.
- The M829A4 armor-piercing, 120 mm line-of-sight kinetic energy cartridge was fielded in 2014. It is the materiel solution for the Abrams' lethality capability gap against threat vehicles equipped with third-generation explosive reactive armor.

Mission
- Commanders employ units equipped with the M1A2 SEP MBT to close with and destroy the enemy by fire and maneuver across the full range of military operations.
- The Army intends the M1A2 SEP MBT to defeat and/or suppress enemy tanks, reconnaissance vehicles, infantry fighting vehicles, armored personnel carriers, anti-tank guns, guided missile launchers (ground and vehicle-mounted), bunkers, dismounted infantry, and helicopters.

Major Contractor
General Dynamics Land Systems – Sterling Heights, Michigan

Activity
- The Army conducted all testing in accordance with a DOT&E-approved test plan.
- In January 2017, the Army continued root cause analysis of the main gun accuracy problems noted in June 2016 when Abrams crews fired service M829A4 kinetic energy (KE) ammunition during the Software 4.6 user Beta Test.
- The Army initiated testing in February 2017 to determine how round count and tube wear affect main gun accuracy.
- The Army conducted ballistic testing of the ARAT I and II in FY17. The ARAT I and II characterization included 54 total shots along with behind-armor debris testing. DOT&E analysis is ongoing.
- The Army continued developmental and verification testing to characterize the performance of the M1A2 SEPv3 NEA against multiple operationally realistic threats. DOT&E is working with the Army to utilize data from ongoing test phases to support its FY20 final assessment of M1A2 SEPv3 survivability against existing and emerging threats.
- FUSL live fire testing for the M1A2 SEPv3 is scheduled to begin in 2QFY18.

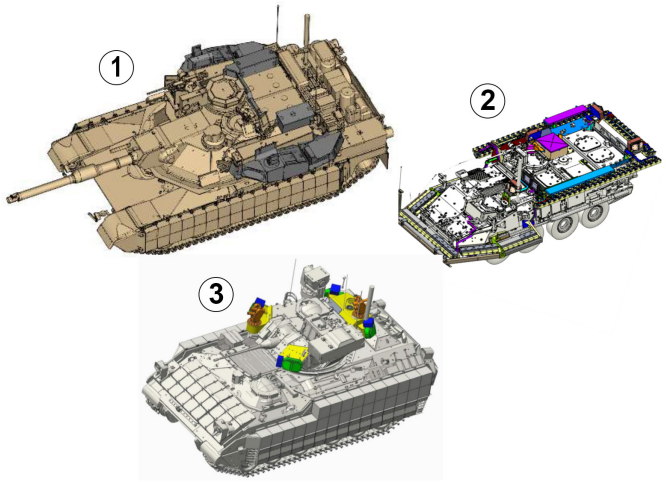
Assessment
- The Army excluded crew error and software as sources of the failure during its root cause analysis. The Army narrowed further testing to focus on how gun tube wear affects main gun accuracy. The Army identified that similar inaccuracy phenomena occurred during testing of the M829A3 KE round.
- After isolating the inaccuracy variables to gun tube wear, the Army acquired field-representative tubes for use during testing. Testing was completed in October 2017. The Army will provide updated gun tube condemnation criteria to fielded units, which includes new equivalent full charge counts for service ammunition and revised tube inspection criteria.
- As of October 2017, the M1A2 SEPv3 has completed 80 percent of planned reliability testing. The system is exceeding the operational requirement for combat mission failures, but is below the requirement for system failures. Current M1A2 SEPv3 reliability exceeds that demonstrated by the M1A2 SEPv2.
- DOT&E continues to assess data resulting from the Army's ongoing efforts to characterize the protection provided by NEA against expected, operationally realistic threats. DOT&E will leverage all relevant vulnerability test data from the armor characterization and underbody IED test phases and evaluate all modeling and simulation tools available to support an FY20 final assessment of the tank's survivability to current and expected threats.

Recommendations
- Status of Previous Recommendations. There are no previous recommendations.
- FY17 Recommendations. None.

Active Protection Systems (APS) Program

Executive Summary

- On October 12, 2016, in support of the European Deterrence Initiative, the Army G-8 issued a Directed Requirement to procure and rapidly field (by FY20) Non-Developmental Item (NDI) Active Protection Systems (APS) to one Armored Brigade Combat Team (Abrams and Bradley vehicles) of pre-positioned stocks and to one Stryker battalion task force.
- The Army intends for APS to improve the survivability of combat vehicles against anti-tank guided missile, rocket-propelled grenade, and recoilless rifle threats by using kinetic "hard kill" options to intercept and disrupt/defeat the incoming threat warhead.
- On February 18, 2017, the Army Acquisition Executive approved an Acquisition Decision Memorandum authorizing expedited installation and characterization of three NDI "hard kill" APS to assess maturity, performance, and integration risk. The following systems were selected: Rafael Trophy APS for the Army Abrams M1A2 and Marine Corps M1A1 tanks, the IMI Systems Iron Fist APS for the Bradley vehicles, and the Artis Iron Curtain for the Stryker vehicles.
- The Army divided APS testing into three phases: Phase 1 is the characterization phase, Phase 2 is the urgent material release (UMR) phase, and Phase 3 is the program of record phase.
- The Army completed Phase 1 Trophy testing in September 2017; Phase 1 Iron Curtain and Iron Fist testing is ongoing.
- Phase 1 Trophy live fire testing demonstrated the ability of the APS to successfully intercept two of the three class threats tested and the potential to provide improved protection against these threats when compared to the existing systems without APS. This capability was demonstrated under benign range conditions and simple threat scenarios inhibiting an assessment of the APS performance with confidence.
  - The Army performed the majority of the tests on a ballistic hull and turret asset that did not independently power the APS, nor have any internal operational features as they would in a fielded configuration.
  - The level of involvement and control of the foreign contractor, Rafael, was high. In many cases, the Army allowed Rafael to adjust the test events to be conducted, provide exclusion zones, and precondition systems with software fixes.
  - Expected software and potential hardware changes in Phase 2 may limit the applicability of Phase 1 results towards overall system evaluation.
- Phase 1 Trophy user testing identified a degradation in turret traverse performance resulting from an imbalance of the turret due to the additional weight of the Trophy system. Subsequent user testing identified several mitigations that reduce the effect of the imbalance enough for crews to conduct combat operations with the additional weight.
- Given the Phase 1 testing limitations, a more operationally realistic testing effort will be required in Phase 2 to support the UMR.



1 - Abrams with Trophy APS
2 - Stryker with Iron Curtain APS
3 - Bradley with Iron Fist APS

System

- The APS solutions consist of multiple components and subsystems that enable the system to detect and declare a threat, deploy countermunitions, and disrupt/defeat the threat. A successful APS intercept of a threat does not imply the absence of residual damage.
- The Army selected Rafael Trophy APS to be installed and characterized on the Army Abrams M1A2 and Marine Corps M1A1 tanks. The Trophy system engages incoming threats with a kinetic projectile intended to destroy the threat or cause early initiation. The Abrams base armor is expected to be able to absorb threat residuals. The Trophy APS adds approximately 5,000 pounds to the platform. In addition to the installation of the Trophy system onto the tank, the Army has incorporated limited integration of the Trophy system into the tank's situational awareness system.
- The Army selected the IMI Systems Iron Fist to be installed and characterized on the Bradley. The Iron Fist engages incoming threats with an explosive projectile intended to destroy or divert the threat, and adds approximately 450 pounds to the platform. The fielded Bradley A3 does not generate sufficient power to operate the APS. The Bradley A4, which is currently under development, does generate sufficient power, so power components from the Bradley A4 must be integrated into the APS test asset.

- The Army selected the Artis Iron Curtain to be installed and characterized on the Stryker. The Iron Curtain engages incoming threats with a kinetic projectile intended to prevent function of the warhead. The Iron Curtain adds approximately 5,700 pounds to the Stryker vehicle.

Mission
- Army and Marine units intend to use Abrams main battle tanks equipped with the Trophy APS to close with and destroy the enemy by fire and maneuver across the full range of military operations.
- Army units use Bradley vehicles equipped with the Iron Fist APS to provide protected transport of soldiers; provide overwatching fires to support dismounted infantry and suppress an enemy; and to disrupt or destroy enemy military forces and control land areas.
- Army commanders use Stryker vehicles equipped with the Iron Curtain APS to disrupt or destroy enemy military forces, to control land areas including populations and resources, and to conduct combat operations to protect U.S. national interests.

Major Contractors
- Rafael Advanced Defense Systems Ltd. – Haifa, Israel
- IMI Systems – Ramat HaSharon, Israel
- Artis, LLC – Reston, Virginia

Activity
- The Army divided APS testing into three phases:
  - Phase 1 (characterization phase) consists of limited characterization testing of threat interaction on the APS system. It is intended to determine fundamental performance and limitations of the system and to provide initial insight into the potential effects of installation of APS systems on the host platforms.
  - Phase 2 (UMR phase) should consist of testing the production-representative APS installed on operationally representative systems under realistic combat conditions to adequately assess the true capabilities and limitations of the systems, as intended to be used in combat, prior to fielding.
  - Phase 3 (program of record phase) should assess the effectiveness, suitability, and survivability of the system equipped with production-representative APS under realistic combat conditions against the spectrum of operationally relevant threats.
- The Army is currently executing Phase 1. Phase 2 is anticipated to begin in January 2018. The start of Phase 3 has not yet been determined.
- The Army conducted Phase 1 Trophy live fire testing at Redstone Arsenal, Alabama, from April through July 2017. Live fire testing included a total of 46 test events.
  - Twenty-nine performance characterization tests on Abrams to demonstrate basic, vendor-claimed APS capabilities. If the APS vendor did not project a successful engagement then the program manager either modified or eliminated the engagement. These tests included seven collateral damage collection events (in conjunction with live threat-countermunition interaction) to assess the potential injury to dismounted soldiers from fragmentation produced during an APS engagement.
  - Eight tests to demonstrate APS performance in operationally relevant and stressing conditions to include three simultaneous (dual) threat engagement tests, two defilade tests, one elevated foliage test, and two tests with metallic clutter on the ground to assess potential radar interference. The program manager deferred testing of one threat class, tests in urban environments and tests in rainy conditions, originally planned for Phase 1 to Phase 2.
  - Nine additional characterization tests on a Marine Corps M1A1 tank using inert rounds to determine APS system performance on a moving (vehicle and/or turret) platform.
- The Army conducted two Phase 1 Trophy user events at Yuma Test Center, Arizona, in June and September 2017.
- Phase 1 testing of the Iron Fist APS implementation on Bradley has been hampered by vehicle power requirements and some component software problems. Consequently, Phase 1 testing of Iron Fist APS on Bradley is 4 months behind schedule.
- Phase 1 testing of Iron Curtain APS on Stryker has been hampered by the replacement of some of the APS components to include the radar. Consequently, Phase 1 testing of Iron Curtain APS on Stryker is 6 months behind schedule.
- Phase 2 test planning is ongoing. The Army has not yet delivered a plan for DOT&E review.
- Contingent upon successful installation and characterization for all three platforms (Phase 1) and guidance from the Army Requirements Oversight Council (AROC), the Army is expected to complete the necessary design and tailored testing (Phase 2) to procure and rapidly field APS to one Armored Brigade Combat Team (Abrams and Bradley vehicles) of pre-positioned stocks, and to one Stryker battalion task force, under a UMR basis. Direction from the AROC may include additional sets to be fielded.

Assessment
- Phase 1 Trophy live fire testing demonstrated the capability of the Trophy APS system to counter two of the three class threats tested. However, the additional protection afforded to the crew and system by the APS and the tradeoff between APS performance and known performance of reactive armor tiles (which APS replaces on certain parts of the vehicle) should be further verified in Phase 2 testing. Phase 1 testing included several limitations that inhibit an assessment of the APS performance with confidence.

  - The Army conducted testing on assets that were not configured for combat, and often lacked critical components such as a functional engine. This inhibited the ability to assess any adverse effects of the APS on vehicle power generation capability.
  - Tests were severely limited in realism by unexpected system corrections, calibrations, and limitations imposed by the contractors. Some contractors also communicated several unexpected performance limitations of their APS systems, requiring extensive modification of planned test events. Because of these and other limitations, it is reasonable to assume that any performance reporting from Phase 1 is optimistic and needs to be confirmed in more operationally realistic conditions in Phase 2.
  - The test design did not incorporate suitable means for quantifying residual vehicle penetration because rolled homogeneous armor plates were used as witness material in lieu of the complex armors present on the Abrams.
- Phase 1 Trophy user testing in June identified a turret weight imbalance problem caused by the addition of Trophy. The September event demonstrated that mitigations can minimize the effect of the weight imbalance.
  - The June 2017 user assessment event identified a degradation in turret traverse performance resulting from an imbalance of the turret due to the additional weight of the Trophy system. The crew could not traverse the turret manually on slopes greater than 5 degrees and power traverse capability was degraded on slopes greater than 8 degrees. Technical analysis indicated a high likelihood of delays between pulling the trigger and the main gun round actually firing.
  - The subsequent user testing in September 2017 identified several mitigations that reduced the degradation in turret traverse performance enough for crews to conduct combat operations with the additional weight, and the potential trigger delay problems were not observed during the event. The Army has not made a final decision on the final configuration for mitigations.
- The UMR Phase 2 effort should inform the Army's decision to field any of the APS systems on these vehicles. This decision should be made not only on the basis of threat defeat criteria and comparison to vehicles that are not APS-enabled, but also with the risks associated with operating in all battlefield and operational conditions. Unit combat effectiveness and risks associated with collateral effects, maintenance, and user-based tactics, techniques, and procedures should also be kept firmly in mind.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendations. The Army should:
  1. Ensure that Phase 2 test assets are fully functional and configured for combat to determine the true performance of the APS in an operationally realistic configuration and environment.
  2. Focus Phase 2 testing more on the combat vehicle and crew/occupant instead of solely on threat/countermunition interaction from the APS engagement; this is the only way true unit-level survivability can be assessed to inform decisions regarding risks in an operational context.
  3. Minimize contractor involvement in Phase 2 testing to the extent possible.
  4. Design Phase 2 testing to enable an assessment of any residual damage effects even given a successful intercept of the threat.
  5. Include an adequate user assessment to ensure turret imbalance does not further degrade system performance.
  6. Include logistical considerations for installation, maintenance, countermunition resupply, and transportation in future test design.

AH-64E Apache

Executive Summary

- The Army conducted 30 mm gun accuracy testing to verify accuracy performance of a redesigned AH-64E Apache gun mount. The redesigned mount corrected a portion of the accuracy problem that had been reported by units with fielded AH-64E aircraft.
- The Army conducted developmental flight testing of upgraded subsystems to the Version 6 AH-64E aircraft in preparation for FOT&E II of the Version 6 aircraft in 2018.
- Targeting systems on the Apache aircraft generated large target location and target velocity errors that will reduce Joint Air-to-Ground Missile (JAGM) performance. These errors should be corrected to support integrated testing of JAGM and future use in combat.

System

- The AH-64E is a modernized version of the AH-64D Attack Helicopter. The Army intends to sustain the Apache fleet through the year 2040. The Army uses the AH-64E in Attack/Reconnaissance Battalions assigned to Combat Aviation Brigades. Each battalion has 24 aircraft.
- The AH-64E's advanced sensors, improved flight performance, and ability to integrate off-board sensor information provide increased standoff and situational awareness in support of the joint force.
- The Army fielded the AH-64E in two Versions (1 and 4). Version 1, after successful IOT&E in 2012, and Version 4, after successful FOT&E I in 2014, with operational testing of Version 6 planned in 2018.
- The major Version 1 AH-64E capability improvements included:
  - The ability of the aircrew to control the flight path and the payload of an Unmanned Aircraft System
  - Improved aircraft performance with 701D engines, composite main rotor blades, and an improved rotor drive system
  - Enhanced communication capability, which includes satellite communication and an integrated communication suite to meet global air traffic management requirements
- The Version 4 AH-64E retained Version 1 capabilities and added hardware and software for Link 16 network participation.
- The Army will conduct FOT&E II with Version 6 AH-64E in May 2018. Version 6 will add multiple enhancements to include:
  - Radar Frequency Interferometer (RFI) passive ranging
  - Fire Control Radar range extension and maritime targeting mode
  - Cognitive Decision Aiding System
  - Modernized Day Sensor Assembly with color and high-definition displays
  - Interoperability with Soldier Radio Waveform networks
- The Army acquisition objective is to procure 767 AH-64E aircraft. Conversion of fielded Version 1 AH-64E aircraft to Version 4 has begun. Once Version 6 begins fielding, all fielded AH-64E aircraft will be converted to Version 6.

Mission

The Joint Force Commander and Ground Maneuver Commander employ AH-64E-equipped units to shape the area of operations and defeat the enemy at a specified place and time. The Attack/Reconnaissance Battalions assigned to the Combat Aviation Brigade employ the AH-64E to conduct the following types of missions:

- Attack
- Movement to contact
- Reconnaissance
- Security

Major Contractors

- Aircraft: The Boeing Company Integrated Defense Systems – Mesa, Arizona
- Targeting Sensors and Unmanned Aircraft System datalink:
  - Longbow Limited Liability Company – Orlando, Florida, and Baltimore, Maryland
  - Lockheed Martin Corporation – Orlando, Florida, and Owego, New York
  - L3 Communications Systems – Salt Lake City, Utah

Activity

- Following reports of poor accuracy of the 30 mm gun from units with fielded AH-64E aircraft, the Program Office investigated the original AH-64E design and found the gun mount came loose after sustained firing and reported erroneous azimuth and elevation positions of the gun.
- The Army redesigned the mounting hardware and conducted 30 mm gun accuracy testing of AH-64E aircraft in flight.
- The Army conducted developmental flight testing of upgraded Version 6 AH-64E subsystems to include RFI passive ranging, the Fire Control Radar range extension and maritime targeting, the Cognitive Decision Aiding System, and the Modernized Day Sensor Assembly with color and high-definition displays.
- The Army completed all testing in accordance with a DOT&E-approved test plan.
- In FY16, the Army developed an Operational Test Agency Test Plan for LFT&E of Apache Version 6 system modifications. The plan includes test and evaluation of: 1) the Fire Detection and Expansion System (FDES) sensors, which are intended to mitigate fire-induced aircraft losses in the tail boom; 2) the Fire Detection and Suppression System (FDSS) upgrades, which are intended to mitigate engines fires; and 3) an evaluation of the Aircraft Survivability Product Improvement (ASPI) equipment for effects on aircraft system vulnerability. Testing of the FDES sensor began in September 2017.
- Apache aircraft supported 18 integrated test JAGM shots in FY17.
- The Army has selected AH-64E to be one of the five systems to complete an evaluation of cyber vulnerabilities to comply with the directive in section 1647 of the National Defense Authorization Act for FY16. The Army conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) in September 2017 and will conduct an Adversarial Assessment (AA) of the Version 6 AH-64E in May 2018 as part of FOT&E II.

Assessment

- In recent 30 mm gun accuracy testing, the Army did not observe any failures of the redesigned gun mount after more than 15,000 rounds of gun testing. The AH-64E 30 mm gun demonstrated improved accuracy with the redesigned gun mount. The Army identified contributing sources of gun accuracy errors and is continuing to investigate the other sources of error. The Army is retrofitting fielded AH-64E aircraft and will incorporate the redesigned mounting hardware into new AH-64E aircraft as they are fielded.
- The Apache Modernized Target Acquisition Designation Sight and Fire Control Radar on occasion generated erroneous target velocities that were passed to the JAGM without cueing the gunner. These errors should be corrected to support JAGM integration.
- Live fire planning and testing is ongoing in accordance with DOT&E guidance.

Recommendations

- Status of Previous Recommendations. The Army has begun to address recommendations from the FY14 annual report. Actions include:
  1. Improve infrared countermeasures performance, upgrade radar- and laser-warning systems, and improve integration of aircraft survivability equipment on the Version 4 AH-64E. The Army integrated the APR-39D(V)2 Radar Warning Receiver onto the Version 4 AH-64E and conducted operational testing against expected threats. See the AN/APR-39 Radar Warning Receiver Annual Report on page 147.
  2. Plan and conduct exploitation of any potential vulnerabilities discovered during CVPA and AA.
  3. Conduct adequate cybersecurity testing in conjunction with the Version 6 FOT&E II in 2018.
- FY17 Recommendations.
  1. The Army should continue to investigate sources of 30 mm gun error and implement fixes as appropriate.
  2. The Apache Program Office should work with the JAGM Program Office to identify the source of spurious sensor targeting data and eliminate or mitigate targeting errors.

Army Integration of the Department of the Navy (DON) Large Aircraft Infrared Countermeasure (LAIRCM) Advanced Threat Warner (ATW) on the AH-64E

Executive Summary

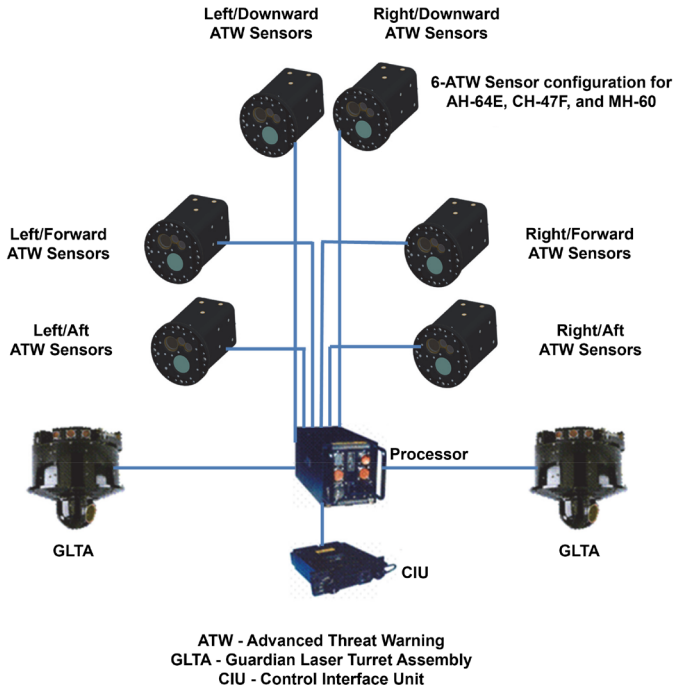
- The Army is integrating the Department of the Navy (DON) Large Aircraft Infrared Countermeasure (LAIRCM) with the Advanced Threat Warner (ATW) on the AH-64E, CH-47F, HH/UH-60M, and UH-60L in response to a U.S. Special Operations Command (USSOCOM) Joint Urgent Operational Need.
- DON LAIRCM is effective as integrated on the AH-64E and has a suitable pilot-vehicle interface.
- Multiple failures in DON LAIRCM ATW sensors have occurred in theater with Formal Release 2.5 software. Although Northrop Grumman identified the problem and the Army put a pilot procedural workaround in place, the potential still exists for aircrew to fly with a failed sensor since system indication of sensor failures is visual only.
- The Army halted integration on the HH/UH-60 variants and CH-47F platforms due to design flaws in the sensor placement and mount systems. A redesign is required.

System

- The DON LAIRCM system, a variant of the Air Force LAIRCM system, is a defensive system for aircraft, which is designed to defend against surface-to-air infrared missile threats.
- The system combines two-color infrared missile warning sensors with the Guardian Laser Transmitter Assembly (GLTA). The missile warning sensor detects an incoming missile threat and sends the information to the processor which then notifies the aircrew through the control interface unit and simultaneously directs the GLTA to slew to and jam the threat with laser energy.
- The ATW capability upgrades the processor and missile warning sensors to provide improved missile detection, and adds hostile fire and laser warning capability with visual/audio alerts to the pilots.

Mission

- Commanders employ Army rotorcraft equipped with DON LAIRCM ATW to conduct medium and heavy lift logistical support, medical evacuation, search-and-rescue, armed escort, and attack operations.
- During Army missions, DON LAIRCM ATW is intended to provide automatic protection for rotary-wing aircraft against shoulder-fired, vehicle-launched, and other infrared missiles.



Major Contractor

Northrop Grumman, Electronic Systems, Defensive Systems Division – Rolling Meadows, Illinois

Activity

AH-64E

- The Army tested DON LAIRCM ATW on the AH-64E from August 25 to October 13, 2016, at Eglin AFB, Florida; Houston, Texas; and Huntsville, Alabama.
- The Army conducted all flight testing in accordance with the DOT&E-approved test plan.

- DOT&E published a classified report on the AH-64E integration of DON LAIRCM ATW in January 2017.
- In March 2017, the Army fielded the system with Formal Release 1.0 software on the AH-64E.
- The Army subsequently fielded Formal Release 2.5 software on AH-64E aircraft in theater to enhance system performance.

UH-60L/M and CH-47F

- The Army began airworthiness and safety flights on the UH-60M with DON LAIRCM.
- CH-47F flight testing began in July 2017. This testing was halted because of poor system performance.

Assessment

AH-64E

- DON LAIRCM is effective as integrated on the AH-64E. The Army did not collect reliability data during AH-64E integration testing; however, pilot survey responses showed that the system was suitable for use.
- The Army incorporated an in-theater pilot procedural workaround for DON LAIRCM ATW sensor failures. This procedural workaround creates the possibility of flying with a failed sensor because system indication of sensor failures is visual only and insufficient.
- Multiple failures in DON LAIRCM ATW sensors have occurred in theater with Formal Release 2.5 software. Northrop Grumman determined the failures occurred due to a system communication problem.
  - Northrop Grumman intended to correct the problem with Formal Release 3.0 software. However, 3.0 software failed aircraft regression testing.
  - Northrop Grumman incorporated further software changes in Formal Release 3.1 to be delivered in October 2017

UH-60L/M and CH-47F

- DON LAIRCM ATW is not properly integrated on the CH-47F or the UH-60 platforms.
  - Structural failure of the UH-60 M/L mounts for the GLTAs requires a redesign.
  - Incorrect ATW sensor placement on the CH-47F aircraft caused poor system performance.
- The Army is in the process of redesigning integration of the DON LAIRCM ATW system on both the UH-60 the CH-47F.

Recommendations

- Status of previous recommendations. This is the first annual report for this program.
- FY17 Recommendations. The Army should:
  1. Redesign the sensor placement and mount systems on the H-60 platforms and CH-47F aircraft and then conduct integration testing before fielding.
  2. Upgrade fielded software to fix sensor reliability problems, and decrease aircraft vulnerability against a growing infrared missile threat.

Army Tactical Missile System - Service Life Extension Program (ATACMS- SLEP)

Executive Summary

- The Army is converting the M39/M39A1 Army Tactical Missile System (ATACMS) with anti-personnel and anti-materiel (APAM) bomblets to the M57 ATACMS Unitary using the same single warhead used in the Navy's Harpoon missile.
- The Army is integrating a proximity sensor into the ATACMS Unitary to add an airburst mode and regain some area effects capability.
- To date, five of five M57E1 ATACMS with proximity sensors have detonated within the required burst range. An operational test is planned for March 2018. DOT&E intends to publish a report in 3QFY18.

System

- The ATACMS Service Life Extension Program converts the M39/M39A1 ATACMS with APAM bomblets to the M57 ATACMS with a single 500-pound APAM warhead and then will add a proximity sensor to regain an area effects capability. The new missile will be designated M57E1 ATACMS Unitary.
- The Army will re-grain the M39/M39A1 motor, update obsolete navigation and guidance software and hardware, and replace the M39/M39A1 APAM bomblets with the WDU-18/B warhead that is used in the Navy's Harpoon missile. The Army intends the warhead change to meet the unexploded ordnance rate requirement defined in the 2008 DOD Policy on Cluster Munitions and Unintended Harm to Civilians.
- The M57E1 missile uses Inertial Measurement Unit and GPS guidance to engage point and area targets out to a range of 300 kilometers.
- The M57E1 missiles can be fired from the tracked M270A1 Multiple Launch Rocket System and the wheeled M142 High Mobility Artillery Rocket System.

Mission

Commanders intend to use M57E1 ATACMS missiles to engage long-range point or area-located targets including air defense, command posts, assembly areas, and high value targets without the hazard of unexploded sub munitions.

Major Contractor

Lockheed Martin Missiles and Fire Control – Grand Prairie, Texas; assembled in Camden, Arkansas

Activity

- In FY17, the Army conducted seven system qualification tests of the ATACMS Unitary with and without the proximity sensor at White Sands Missile Range, New Mexico. The Army conducted two ATACMS tests without the proximity sensor in order to qualify electronics and the re-grained solid rock motor; these tests did not have targets. Live fire testing consisted of two M57E1 ATACMS with the proximity sensor fired against witness panels and two M57E1s fired against an array of targets.
- The Army conducted a soldier-executed user demonstration on September 14, 2017, in accordance with a DOT&E-approved test plan. During this demonstration, a soldier crew fired one M57E1 against a larger array of targets.
- As part of the M57 Stockpile Reliability Program, a missile was fired against the same array of targets as the M57E1 live fire tests. This will allow a comparison of effects between ATACMS with and without the airburst capability.
- The Army has planned for operational testing of the M57E1 in March 2018, which will support the Army decision to produce the M57E1 ATACMS with proximity sensor.

Assessment

- ATACMS continues to perform reliably. Five of five ATACMS with proximity sensors reliably detonated.
- The proximity sensor consistently detonated within the required height of burst range and within the accuracy requirement.
- Lethality results are being assessed.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendations. None.

Bradley Family of Vehicles (BFoV) Engineering Change Proposal (ECP)

Executive Summary
- In September 2016, DOT&E approved an updated Test and Evaluation Master Plan (TEMP) to support the Engineering Change Proposal (ECP) production contract award scheduled for June 2017.
- In 2017, the Army continued efforts to test and improve the Bradley's reliability prior to the FOT&E in 4QFY19.
- The program is using developmental testing to identify and correct current M2A4 and legacy M2A3 failure modes. While ECP2 is not meeting its reliability requirement in ongoing developmental testing, reliability for ECP2 is improving.
- The Army has created an integrated planning team to assess and recommend corrective action for current and legacy faults.

System
- The Bradley Family of Vehicles (BFoV) ECP program intends to integrate new technologies so that existing system performance is not further degraded. The ECPs are not intended to exceed the operational capability outlined in current system requirements documents.
- The initial phase, known as ECP1, was a suspension and track upgrade, which began in FY11 to restore ground clearance and suspension reliability because of increases in Bradley armor and weight. ECP2 will upgrade the electrical system and power train to restore lost mobility and integrate new technologies to improve situational awareness and vehicle survivability.
- Installation of ECP1 and ECP2 kits will result in the conversion of existing M2A3 version Bradley Fighting Vehicles into the M2A4 version and the M7A3 Bradley Fire Support Team vehicle into the M7A4 version.
- The current plan is that all Bradley A3s will become A4s. The A3 baseline configuration includes the additional Bradley Urban Survivability Kits, Bradley Reactive Armor Tiles, and Add-on Armor Kit that the Army developed and fielded in response to Operational Needs Statements during Operation Iraqi Freedom.

Mission
Combatant Commanders employ Armor Brigade Combat Teams equipped with Bradley Fighting Vehicles to provide protected transport of soldiers, provide direct fires to support dismounted infantry, to disrupt or destroy enemy military forces, and to control land areas.

Major Contractor
BAE Systems Land and Armaments – Sterling Heights, Michigan

Activity
- In September 2016, DOT&E approved an updated TEMP to support the production contract award for ECP2 originally scheduled for June 2017. Government changes in desired quantity, a late delivery of the proposal by the contractor, and increased cost per vehicle estimates by the contractor have resulted in a slip in the production contract award to February 2018 (estimated).
- The Army continued efforts in 2017 to test and improve ECP2 reliability prior to the FOT&E in 4QFY19. The program created an integrated planning team to assess and recommend corrective action for current and legacy reliability failure modes.
- Due to unexpected reliability problems, developmental testing was increased to verify design changes for corrective actions, software updates, and reliability improvements, which have resulted in potential trade-offs in approved developmental and operational test scope. An updated TEMP is being developed for review and approval.

Assessment
- The program focused early developmental testing on identifying and correcting current M2A4 and legacy M2A3 failure modes. As a result, ECP2 is not meeting its reliability

requirement in ongoing developmental testing. ECP2 averaged 281 mean miles between combat mission failures in August 2017. The requirement is 400. Reliability is improving.
- Seventy-six percent of combat mission failures are hardware to include failures of power pack components. The largest single cause of combat mission failures in early testing were transmission oil cooler (TOC) failures. The program designed and implemented a fix for TOC failures. The fix was verified in developmental testing. The program continues to design and implement fixes for remaining failure modes.
- ECP2 software version R1 is not mature and not reliable. Software version R1.1 is expected to correct nuisance faults and is scheduled for formal release in February 2018. The Army will address remaining software reliability problems with an additional R2 Software drop in February 2019 prior to the FOT&E in 4QFY19.
- The Army is working with the contractor to reduce ECP cost increases and is expected to have a production contract award in 2QFY18 or 3QFY18.

Recommendations
- Status of Previous Recommendations. The Army addressed the previous recommendation to conduct technical testing of survivability improvement kits and modifications.
- FY17 Recommendations. None.

Heavy Equipment Transporter (HET) Urban Survivability Kit (HUSK)

Executive Summary
- The Heavy Equipment Transporter (HET) Urban Survivability Kit (HUSK) is designed to protect the crew against small arms, IEDs, artillery rounds, and blast mines at the Mine Resistant Armor Protected (MRAP) Capability Production Document 1.1 levels.
- In FY16, the Army completed LFT&E of the HUSK demonstrating that the armored cab:
  - Provides protection against Key Performance Parameter threats at threshold levels and some objective levels
  - Includes impediments to egress due to post-attack fuel fires outside the cab that could be mitigated with additional design changes
- The Army plans to award a production contract for 60 HUSKs to be built to production-level technical data package specifications. The program intends to make a decision in FY18 to build HUSK either at a government depot or contract with industry.

System
- The HET A1 is a combat support battlefield operating system assigned to combat heavy equipment transport companies.
- In May 2013, an Acquisition Decision Memorandum authorized the Army to develop and acquire armored replaceable cabs for HET A1, leading to the HUSK. HUSK is designed to protect the crew against small arms, IEDs, artillery rounds, and blast mines at the MRAP Capability Production Document 1.1 levels.
- The HUSK interior survivability features include energy attenuating seats, a floating floor, blast-mitigating floor mats, and an automatic fire extinguishing system. The exterior is constructed of 5059 aluminum and it is attached to the frame rails of the vehicle chassis. The cab can accommodate six soldiers: the driver, the assistant driver, and four crew of the transported vehicle.

Mission
Army commanders will employ military units equipped with HUSK to support operational and tactical moves by evacuating and transporting heavy tracked and wheeled equipment – primarily the combat-loaded M1 Abrams main battle tank – while providing crew protection against operational threats.

Major Contractor
None yet. The U.S. Army Tank Automotive Research, Development and Engineering Center designed and built the test articles using a production-level technical data package.

Activity
- The Army conducted the LFT&E program at Aberdeen Proving Ground, Maryland, in accordance with DOT&E-approved test plans, which included:
  - Armor coupon testing from April to May 2016 to assess the protection capabilities of the armor against operationally anticipated threats
  - Armor exploitation testing in May 2016 intended to identify vulnerabilities in the HUSK integrated armor
  - Six full-up system-level live fire tests from June to September 2016 to evaluate crew survivability and vehicle performance against a subset of mines and IEDs
  - Automatic Fire Extinguishing System test in July 2016 to assess its effectiveness
- DOT&E provided a classified report to Congress in June 2017, evaluating the HUSK protection afforded to the crew given by the armor replaceable cab.

Assessment
- HUSK provides increased protection over the legacy HET A1 system.
- HUSK demonstrated the ability to protect the crew against small arms, IEDs, artillery rounds, and blast mines. More specifically, HUSK provides protection against all non-overmatching threshold threats at levels indicated in the MRAP Capability Production Document 1.1.

- Armor exploitation testing revealed HUSK door vulnerabilities. The Army mitigated the vulnerability by correcting the design deficiency, and demonstrated, through additional tests, the effectiveness of the system design changes.
- HUSK crew egress could be challenged during post-combat engagement. The roof hatch was accessible as a secondary means to exit the vehicle after each test event.
- HUSK did not introduce any changes that would adversely affect the effectiveness of the Automatic Fire Extinguisher System. The system provided the required fire suppressant concentrations in the crew compartment.
- HUSK protected the crew from fuel fires that Army testers observed outside the cab during full-up system-level live fire tests.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendations. The Army should:
  1. Conduct exploitation testing on the production HUSK, after contract award, to assess any manufacturing-induced differences not identified in the level III technical data package specifications.
  2. Consider incorporating cab design changes to: (1) improve crew protection against underbody blast mines beyond threshold levels, (2) improve crew egress ability post attack by mitigating the risk to combat-induced fires outside the cab.

Javelin Close Combat Missile System - Medium

Executive Summary

- In FY17, the Army completed testing of the Spiral 2 missile and continued development of the Spiral 3 missile and a new Light Weight Command Launch Unit (CLU). The Army intends these efforts to improve lethality against non-armored targets and to reduce unit cost and weight.
- The Program Office investigated and addressed Spiral 2 precursor warhead (PCWH) failures experienced in FY16. The Army resumed testing in FY17. The final production-representative configuration of the Spiral 2 missile performed reliably in 14 of 14 flight tests.
- Test results and lethality modeling of the Spiral 2 missile, which includes a new Multi-Purpose Warhead (MPWH), indicate the Spiral 2 missile has improved warhead fragmentation while maintaining required primary target armor penetration.
- Through 22 flight tests, the Spiral 2 missiles demonstrated proper target lock-on and missile launch resulting in 18 successful hits against vehicles, 2 successful hits against structure targets, and 1 near miss and 1 complete miss against an IED team in the open.
- DOT&E and the Army continue planning the testing required for the Spiral 3 missile and Light Weight CLU developments.

System

- The Javelin Close Combat Missile System – Medium is a man-portable, fire-and-forget, anti-tank guided missile used to defeat threat armored combat vehicles out to 2,500 meters.
- The Javelin system consists of a missile in a disposable launch tube assembly and a reusable CLU. The CLU mechanically engages the launch tube assembly for shoulder firing, has day and night sights for surveillance and target acquisition, and electronically interfaces with the missile for target lock-on and missile launch. An operationally-ready Javelin system weighs 49.5 pounds.
- The Javelin missile employs a tandem shaped charged warhead to defeat vehicle armor and can be fired in direct-fire or lofted trajectory top-attack modes.
- The Army plans four Javelin system improvements to reduce unit cost and weight and improve lethality against non-armored targets. These improvements are referred to as missile Spiral 1, 2, 3, and Light Weight CLU.
  - The Spiral 1 effort replaced electronic components in the control actuator section of the missile for cost and weight savings. Production missiles are designated FGM-148E.

  - The Spiral 2 effort developed a new PCWH, and an MPWH that uses enhanced fragmentation to improve lethality against non-armored targets and personnel in the open while maintaining lethality against armored threats. Production missiles will be designated FGM-148F.
  - The Spiral 3 effort will develop a new launch tube assembly and battery unit, and will replace the current gas-cooled seeker with an uncooled seeker in the guidance section of the missile. Production missiles will be designated FGM-148G.
  - The Light Weight CLU effort will develop a new CLU that is smaller and lighter while maintaining or improving system performance.

Mission

- Commanders use Army and Marine Corps ground maneuver units equipped with the Javelin to destroy, capture, or repel enemy assault through maneuver and firepower.
- Service members use the Javelin to destroy threat armor targets and light-skinned vehicles, and to incapacitate or kill threat personnel within fortified positions. In recent conflicts, Javelin was used against enemy bunkers, caves, urban structures, mortar positions, snipers, and personnel emplacing IEDs.

Major Contractors

- Raytheon – Tucson, Arizona
- Lockheed Martin – Orlando, Florida

Activity

- In FY17, the Army Aviation and Missile Research, Development and Engineering Center completed testing of the Spiral 2 missile improvements in accordance with the DOT&E-approved live fire strategy.

- From FY16 through FY17, the Army conducted a total of 16 static warhead tests and 22 missile flight tests at the Redstone Test Center, Alabama.
  - In FY16, testing was halted after nine static warhead tests and seven missile flight tests due to a reoccurring failure of the new PCWH. Following an analysis of the failures, the Army decided to replace the new PCWH with the proven legacy PCWH.
  - In FY17, the Army conducted the remaining 7 static warhead tests and 15 flight tests.
- Three FGM-148D (Block 0) and three FGM-148E (Spiral 1) missiles were fired to demonstrate backward compatibility with current CLUs and new missile software.
- DOT&E and the Army continued to plan testing required for the Spiral 3 missile and Light Weight CLU, and the Javelin Program Office began an update to the Test and Evaluation Master Plan (TEMP).

Assessment

- During FY16 testing, the new PCWH failed to detonate in two static tests and in two flight tests. The failure was caused by age-related degradation in the explosive material of the PCWH. The program determined the best course of action was to use the legacy PCWH in the Spiral 2 missiles. The remaining test missiles were rebuilt with the legacy PCWH and the Army resumed testing in FY17. No additional failures occurred during the remaining 7 static tests and 14 tactical missile flight tests.
- Missile flight and static test results indicate improved fragmentation enabling the intended, improved lethality against light-skinned vehicles and targeted personnel in the open, while maintaining effectiveness against armored targets.
- Through 22 flight tests, the Spiral 2 missiles demonstrated proper target lock-on and missile launch resulting in 18 successful hits against vehicles, 2 successful hits against structure targets, and 1 near miss and 1 complete miss against an IED team in the open. Personnel in the open are a secondary target for the Javelin.
- The failure of the new PCWH was the sole failure mode to occur during Spiral 2 missile testing. Following the PCWH change, the production-representative missile performed reliably in 14 of 14 flight tests.
- DOT&E assesses that Javelin Spiral 2 would meet its reliability requirement.

Recommendations

- Status of Previous Recommendations. The Army and DOT&E are planning testing required for the Spiral 3 missile and Light Weight CLU. The Army agrees that an operational test should be conducted prior to fielding to confirm that effectiveness/lethality and suitability have not been compromised, and to ensure compatibility with applicable fielded variants of the missile. The Javelin Program Office is updating the TEMP.
- FY17 Recommendation.
  1. The Javelin Program Office should perform additional testing and modeling to establish the capability of the Spiral 2 missile to hit targeted personnel in the open (such as the three-man IED team). Information gained should inform the Spiral 3 missile design.

Joint Air-to-Ground Missile (JAGM)

Executive Summary

- As of September 28, 2017, the Army has completed 2 successful ground launches and 20 successful Integrated Test and Evaluation shots launched from an Apache aircraft, 4 of which included live warheads. The program intends to fire 48 Engineering Manufacturing and Development (EMD) missiles in support of Milestone C in FY19. Ten of the missile shots will occur during the planned Limited User Test in January 2018.
- Eighteen of 20 EMD missiles hit their intended targets. One warhead did not function. Failure analysis is underway to determine the root cause.
- Testing has revealed that targeting systems on the Apache aircraft generate large target location and target velocity errors that will affect the Joint Air-to-Ground Missile (JAGM) performance.
- The system completed the first of two planned cybersecurity assessments. The contractor identified a Category I vulnerability during test preparation: a trained and knowledgeable cyber analyst could gain access to the missile guidance software.

System

- The JAGM combines the capabilities of the HELLFIRE II and Longbow HELLFIRE missiles into a single missile. The major contractor combined two sensor technologies – semi-active laser (SAL) and millimeter wave (MMW) radar – into a single seeker and guidance system and mated it to the HELLFIRE Romeo warhead, motor, and flight control systems.
- The dual seeker, in addition to providing independent SAL and MMW targeting, offers two combined modes using both the laser and MMW seekers to maintain desired performance in degraded environments and against threat countermeasures.

- The HELLFIRE Romeo warhead Integrated Blast and Fragmentation Sleeve (IBFS) detonates with a programmable delay fuse and a Height-of-Burst (HOB) feature. This updated warhead blast provides a capability to engage armored vehicles while the IBFS and HOB feature engage personnel in the open. The programmable delay allows time for the warhead to penetrate deep into a building, bunker, or lightly armored vehicle before detonating to incapacitate the personnel and destroy the equipment inside.

Mission

Army and Marine Corps commanders intend to employ JAGM from rotary-wing and unmanned aircraft to engage enemy combatants in stationary and moving armored and unarmored vehicles, within complex building and bunker structures, in small boats, and in the open.

Major Contractor

Lockheed Martin Corporation, Missiles and Fire Control Division – Grand Prairie, Texas

Activity

- The Army conducted two ground-launched risk reduction shots in October 2016. Both hit their target. The second shot repeated an earlier risk reduction shot that missed the target following extended exposure to cold temperatures.
- The Army conducted two successful aircraft-launched risk reduction shots in December 2016 and January 2017. One missile was launched by an AH-64D over water against a small boat target and the other was launched by an AH-64E against a T-72 tank.
- The Army conducted a cybersecurity Cooperative Vulnerability and Penetration Assessment of the JAGM guidance section in April 2017.
- The Army conducted 2 ground-launched safety-of-flight shots in April 2017 and 20 Integrated Test and Evaluation shots from Apache through September 28, 2017, using EMD phase production missiles.
- Safety-of-flight and integrated test shots included four live fire shots against a brick-over-block wall with a high temperature thermally soaked warhead, a 2S1 self-propelled howitzer, a T-72 with explosive reactive armor, and an armored personnel carrier.
- Live fire testing in FY17 has also included component tests, behind armor debris, arena, and rolled homogenous armor testing to characterize warhead lethality and to compare its

performance to the legacy AGM-114-R HELLFIRE missiles. Fuse and dynamic penetration testing is planned for February to April 2018.
- The program intends to fire 48 EMD missiles in support of Milestone C in FY19. Ten of the missile shots will occur during the planned Limited User Test in January 2018.
- The Army conducted all testing in accordance with the DOT&E-approved test plan.

Assessment
- The program is proceeding according to schedule toward Milestone C. As of September 28, 2017, the Army has completed 20 successful missile launches from an AH-64E Apache aircraft at Yuma Proving Ground, Arizona. Eighteen of these missiles hit their intended targets under carefully controlled developmental flight test conditions. Missile geometries and modes were selected from among those in the most favorable part of the performance envelope. EMD and risk reduction testing has demonstrated that the Apache's Modernized Target Acquisition Designation Sight and Fire Control Radar occasionally generate erroneous target velocities that are passed to the missile without cueing the gunner of the errors.
- One EMD missile missed the intended target, hitting the ground well outside the burst radius of the warhead. A second EMD missile hit near the bottom of the vehicle track and road wheels. Post-test investigation will adjudicate whether this missile hit or missed the intended target.
- Eighteen missile launches from an AH-64E hit the intended target, one of the four launches that included a live warhead failed to detonate. Failure analysis is currently underway to determine the root cause.
- Preliminary results of component and other warhead characterization tests indicate JAGM warhead lethality is equivalent to the legacy HELLFIRE system.
- The initial cybersecurity testing of the JAGM guidance section in April 2017 revealed a Category I vulnerability: a trained and knowledgeable cyber analyst could gain access to the missile guidance software.
- Development of Apache software to recognize the JAGM missile and enable all its operational modes is under way with an early version to be available just before Milestone C. Until that software is available, Apache aircrews must launch the JAGM missile using non-standard procedures and an engineering test page in the cockpit.

Recommendations
- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendation.
  1. The Apache Program Office should work with the JAGM Program Office to identify the source of spurious sensor targeting data and eliminate or mitigate targeting errors.

Joint Light Tactical Vehicle (JLTV) Family of Vehicles (FoV)

General Purpose

Heavy Guns Carrier

Utility/Shelter Carrier

Close Combat Weapons Carrier

Executive Summary

- DOT&E approved the Annex to the Joint Light Tactical Vehicle (JLTV) Milestone C Test and Evaluation Master Plan (TEMP) in October 2017.
- The Army Test and Evaluation Command (ATEC) and Marine Corps Operational Test and Evaluation Agency (MCOTEA) plan to complete the LFT&E in accordance with the DOT&E-approved test plan by January 2018.
- In November 2017, the Army designated the Army test unit for the February 2018 Multi-Service Operational Test and Evaluation (MOT&E). This late decision affects ATEC's ability to work with the Army unit to develop operationally relevant missions and ensure that the unit is trained, equipped, and manned to execute these missions.
- The approved JLTV Milestone C (MS C) TEMP requires an amphibious ship during the MOT&E to support the assessment of the JLTV employment in amphibious operations. The Navy has not committed to providing an amphibious ship for the MOT&E affecting MCOTEA's ability to conduct the end-to-end amphibious operations during the MOT&E.
- In February 2018, ATEC and MCOTEA plan to conduct the JLTV MOT&E at Twenty-nine (29) Palms and Camp Pendleton in California. The results of the MOT&E will support a Full-Rate Production decision in 1QFY19.

System

- The JLTV Family of Vehicles (FoV) is the partial replacement for the High Mobility Multi-purpose Wheeled Vehicle (HMMWV) fleet for the Marine Corps and Army. The Services intend JLTV to provide increased crew protection against IEDs and underbody attacks, improved mobility, and higher reliability than the HMMWV.
- The JLTV FoV consists of two vehicle categories: the JLTV Combat Tactical Vehicle, designed to seat four passengers, and the JLTV Combat Support Vehicle, designed to seat two passengers.
- The JLTV Combat Tactical Vehicle has a 3,500-pound payload and three mission package configurations:
  - Close Combat Weapons Carrier (CCWC) Vehicle
  - General Purpose Vehicle
  - Heavy Guns Carrier Vehicle
- The JLTV Combat Support Vehicle has a 5,100-pound payload and one mission package configuration:
  - Utility Prime Mover that can accept a shelter
- As a result of General Motor's decision to discontinue the JLTV engine used during Engineering Manufacturing Development, the JLTV program plans to field two vehicle

versions: the JLTV A0 and A1. The JLTV A1 has a new Duramax engine that replaces the A0 engine.
  - The Army plans to field approximately 47,099 JLTV A1 and 2,000 JLTV A0 vehicles.
  - The Marine Corps plans to field approximately 9,091 JLTV A1 vehicles.
- JLTVs are equipped with two armor levels: the A-kit, or base vehicle, which the Services intend to employ in low threat environments, and the B-kit, an add-on armor kit, for additional force protection against enhanced small arms, fragmentation, and underbody threats.

Mission
- Commanders employ military units equipped with JLTV as a light, tactical-wheeled vehicle to support all types of military operations. Airborne, air assault, amphibious, light, Stryker, and heavy forces use JLTVs as reconnaissance, maneuver, and maneuver sustainment platforms.
- Small ground combat units will employ JLTV in combat patrols, raids, long-range reconnaissance, and convoy escort.

Major Contractor
Oshkosh Corporation – Oshkosh, Wisconsin

Activity
- ATEC began Production Qualification Test (PQT) and Reliability Qualification Test (RQT) in January 2017 on the JLTV A0. The purpose of PQT was to ensure that the JLTV performance, reliability, weapon integration, and transportability met the requirements outlined in the JLTV Capability Production Document. ATEC completed the majority of JLTV A0 PQT and RQT events by December 2017.
  - PQT and RQT at the Cold Regions Test Center conducted in Fort Greeley, Alaska, assessed the JLTV A0 performance and reliability in extreme cold-weather environments.
  - RQT at Aberdeen Proving Ground (APG), Maryland, and Yuma Proving Ground (YPG), Arizona, accumulated over 96,000 combined miles to assess the A0 vehicle reliability.
  - Transportability testing consisted of helicopter sling load, internal air transport, and rail transport for transportability certification.
- DOT&E approved the Annex to the JLTV Milestone C TEMP in October 2017.
- Tube-launched, Optically tracked, Wire-guided (TOW) integration testing of the JLTV CCWC is ongoing at Redstone Test Center, Alabama.
- Low Velocity Air Drop testing began at Fort Bragg, North Carolina in November 2017.
- ATEC and MCOTEA plan to complete the LFT&E at APG in accordance with the DOT&E-approved test plan by January 2018.
  - Full-up system-level live fire testing evaluated crew survivability and vehicle performance against mine and IED threats, overhead artillery, rocket-propelled grenades, and homemade explosives.
  - Ballistic cab testing characterized the explosively formed penetrator armor kit.
  - Exploitation testing on the JLTV Combat Support Vehicle evaluated the survivability of the JLTV against small arms and fragments.
- The program conducted performance, reliability, and cybersecurity testing on the JLTV A1 from September through December 2017 at APG, YPG, and the Electronic Proving Ground (EPG) at Fort Huachuca, Arizona.
  - Reliability testing at APG and YPG accumulated over 24,000 miles to assess the Mean Miles Between Operational Mission Failures (MMBOMF) requirement.
  - Automotive performance testing at APG assessed critical automotive and mobility requirements.
  - A Cooperative Vulnerability and Penetration Assessment at EPG supported the development of a mitigation plan to reduce vulnerabilities and improve cybersecurity.
- In December 2017, the program conducted the JLTV Maritime Prepositioned Force Shipboard Evaluation at Charleston, South Carolina. The assessment provided the program with information regarding the capability to embark, maneuver, stow, and disembark from decks on Military Sealift Command vessels.
- ATEC and MCOTEA plan to conduct the JLTV MOT&E at 29 Palms and Camp Pendleton in February 2018. The results of the MOT&E will support a Full-Rate Production decision in 1QFY19. In November 2017, the Army designated the test unit that will participate in the MOT&E.
- The approved JLTV MS C TEMP requires an amphibious ship at MOT&E to support the end-to-end test of the JLTV employment in amphibious operations. The Navy has not committed an amphibious ship to support the Marines conducting amphibious operations during MOT&E.

Assessment
- The Army's late selection of an Army test unit for the February 2018 MOT&E affects ATEC's ability to develop operationally relevant missions and ensure that the unit is trained, equipped, and manned to execute these missions.
- Results from PQT of the JLTV A0 and A1 variants indicate the vehicle is meeting automotive performance requirements.
- During extreme cold weather testing, the Army crew equipped with the JLTV experienced improved mobility and ride quality relative to the HMMWV over snow-covered terrain. The vehicle heating system warmed the cab quickly. Soldiers installed tire chains and changed tires with no problems.
- Initial analysis of ongoing reliability testing indicates that the JLTV A1 and A0 variants are meeting the reliability requirement of 2,400 MMBOMF.

- Based on Weapons Integration Testing, the JLTV CCWC has restricted firing zones to avoid vehicle damage and ensure crew safety after TOW mission firings. DOT&E will assess the operational impact of the CCWC firing restriction during the MOT&E.
- The combat payload is expected to exceed 3,500 for the HGC and CCWC mission packages, which will result in the rear axle of the JLTV to be overloaded.
- Analysis is ongoing to assess the impact of cybersecurity deficiencies with respect to operationally relevant threats and their effect on JLTV survivability.
- Preliminary analysis of full-up system-level live fire testing did not reveal any unexpected vulnerabilities.
- DOT&E plans to complete detailed survivability analysis in FY18, to include results of modeling and simulation on the performance of the JLTV against the threshold force protection requirements and other operationally relevant threats. This analysis will support DOT&E's classified JLTV LFT&E report.

Recommendations

- Status of Previous Recommendations. The Army has made progress addressing the previous FY15 recommendations.
- FY17 Recommendations. None.

M109 Family of Vehicles (FoV) Paladin Integrated Management (PIM)

Executive Summary

- The Army began the M109 Family of Vehicles (FoV) Paladin Integrated Management (PIM) IOT&E 1 in October 2016 at Fort Hood, Texas. IOT&E 1 was suspended after the first record test vignette because 28 soldiers were affected by toxic fumes released into the M109A7 Self-Propelled Howitzer (SPH) cab.
- Feedback from the root cause analysis indicates that the toxic fumes are related to breech reliability, training on the M109A7, and technical manuals.
- IOT&E 1 was adequate to conclude the M109A7 SPH is not operationally effective and not operationally suitable.
- Cannon artillery units equipped with PIM SPH cannot execute delivery of cannon field artillery munitions using the M232A1 Modular Artillery Charge System (MACS 5H) charge increment, which is needed to reach beyond 18 kilometers of range.
- The M109A7 SPH did not meet reliability, availability, and maintainability requirements.
- The primary M109A7 SPH failure modes are associated with the breech and its sub-components. Demand for repair parts associated with the breech exceeded the supply inventory of operational units. The breech has not changed as part of the M109A7 PIM program.
- In January 2017, DOT&E submitted an Operationl Assessment to Congress for the suspended IOT&E. A second IOT&E is scheduled for March 2018 following the Army's implementation of corrective actions from the IOT&E 1.
- The Army continued multiple phases of the M109A7 FoV PIM weapons firing and automotive performance, and reliability developmental testing at Yuma Proving Ground, Arizona.

System

- The M109 FoV PIM consists of two vehicles: the SPH and Carrier Ammunition Tracked (CAT) resupply vehicle.
  - The M109A7 SPH is a tracked, self-propelled 155 mm howitzer designed to improve sustainability over the legacy M109A6 howitzer. The production howitzers have a modified M109A6 turret with a high-voltage electrical system and a modified Bradley Fighting Vehicle chassis, power train, and suspension. The Army is updating the breech based on results from testing in IOT&E 1. A crew of four soldiers operates the SPH and use it to engage targets at ranges of 22 km using standard projectiles and 30 km using rocket-assisted projectiles.
  - The M992A3 CAT supplies the SPH with ammunition. The ammunition carriers have a chassis similar to the SPH. The ammunition carriers are designed to carry 12,000 pounds or 98 rounds of ammunition in various configurations. A crew of four soldiers operates the CAT.

- The Army will equip the SPH and CAT with two armor configurations to meet two threshold requirements for force protection and survivability – Threshold 1 (T1) and Threshold 2 (T2).
  - The base T1 armor configuration is integral to the SPH and CAT. The Army intends the T2 configuration to meet protection requirements beyond the T1 threshold with add-on armor kits.
  - The Army plans to employ PIM vehicles in the T1 configuration during normal operations and will equip the SPH and CAT with T2 add-on armor kits during combat operations.
- The Army designed an underbody kit to determine the potential protection an SPH and CAT could provide against IEDs similar to those encountered in Iraq and Afghanistan. The Army purchased five underbelly kits for test purposes. The Army does not intend to equip the SPH or CAT with the underbody kit at this time.
- The Army intends to employ the M109 FoV as part of a Fires Battalion in the Armored Brigade Combat Team and Artillery Fires Brigades.
- The Army plans to field up to 574 sets of the M109 FoV with full-rate production planned for FY18.

Mission

Commanders employ field artillery units equipped with the M109 FoV to destroy, defeat, or disrupt the enemy by providing integrated, massed, and precision indirect fire effects in support of maneuver units conducting unified land operations.

Major Contractor
BAE Systems – York, Pennsylvania

Activity
- The Army began the M109 FoV PIM IOT&E 1 in October 2016 at Fort Hood, Texas. IOT&E 1 was suspended after the first record test vignette because 28 soldiers were affected by toxic fumes released into the M109A7 SPH cab.
- DOT&E submitted an Operationl Assessment to Congress for the suspended IOT&E in January 2017.
- A second IOT&E is scheduled for March 2018 at Fort Riley, Kansas.
- The Army continues to conduct Production Qualification Testing (PQT) at Yuma Proving Ground, Arizona.
- The Army is developing concepts for design and production of an extended range cannon and breech assembly.
- In FY18, the Army plans to conduct additional exploitation testing on the SPH to complete validation of modifications to the T1 and T2 armor systems. These modifications are to address vulnerable areas identified in earlier testing.

Assessment
- Although the Army suspended the IOT&E 1, the test was adequate to conclude the M109A7 SPH is not operationally effective and not operationally suitable.
  - In the suspended IOT&E, both the CAT and the SPH showed significant improvement over the speed and maneuverability demonstrated by the legacy ammunition carrier and howitzer.
  - In the suspended IOT&E, breech failures were the most common failure. Eleven of the 16 failures were related to the breech components requiring parts replacement (firing mechanism, plunger pins, firing pin retainers, split rings, obturator pads, etc.) and or field-level repair. The breech is a legacy component from the fielded M109A6 SPH and was not changed as part of the M109A7 PIM program in order to fire propellant charges necessary to attain extended range in combat. Cannon artillery units equipped with the M109A7 SPH cannot execute delivery of cannon field artillery munitions using the M232A1 MACS 5H charge increment, which is needed to reach beyond 18 km of range.
  - During IOT&E 1, a field artillery unit equipped with M109A7 SPH was not able to provide the volume of fire needed to support an Armor Brigade Combat Team due to breech failures.
  - During the test, cannon artillery units equipped with the M1097A7 SPH generated a high demand for repair parts associated with the breech in order to correct the frequent failures.
- Since IOT&E 1, the Army developed a phased approach to its breech reliability failures that addresses subcomponents of the legacy breech in phase one, with more comprehensive design changes in phase two. Neither phase will change the basic breech design. The phase one changes may reflect a modest increase in reliability over what was seen in IOT&E 1. Although phase one could reflect an increase in reliability, phase two will not be executed until FY19, after IOT&E 2 in FY18.
- In addition to the phase one breech subcomponent improvements, the Army updated technical manuals to address methods to mitigate toxic fumes, maintenance requirements, and breech subcomponent related failures.
- The M109A7 SPH did not meet reliability, availability, and maintainability requirements. The CAT did very well in the suspended IOT&E and shows promise to meet its requirements in IOT&E 2.
- Non-breech reliability problems found on both the CAT and the SPH have been addressed in a comprehensive test-fix-test cycle throughout PQT. Engine component failures in both the CAT and the SPH have been initially traced to transmission oil cooler design discrepancies. An interim design change has mitigated further failures.
- During IOT&E 1, the M1068/A3 Fire Direction Center tracked vehicle could not execute a mix of missions a self-propelled field artillery would be expected to complete. The M1068/A3 Fire Direction Center tracked vehicle cannot keep pace with the PIM FoV, and lacks necessary mobility and reliability.
- The Program Office has taken considerable action to correct deficiencies identified in early testing and to validate associated fixes over the course of the Developmental Performance, Automotive, and LFT&E program.
  - During armor exploitation testing, most of the modified armored areas demonstrated that they provide protection against Key Performance Parameter threats.
  - Changes to the CAT's crew compartment Automatic Fire Extinguisher System (AFES) mitigate the deficiency identified in early testing and reduce its vulnerability to fires.
- The crew compartment AFES in the SPH was designed to protect a small, localized area in the crew compartment. Live fire testing demonstrated that the system is deficient in providing adequate fire survivability. The Program Office is redesigning this system to improve SPH survivability to fires. While not yet optimized, the M109A7 provides improved crew fire safety compared to the currently fielded M109A6 because:
  - The M109A7 has crew compartment AFES capability while the M109A6 has none.
  - The M109A7 has reduced fire hazards compared to the M109A6 because of the replacement of hydraulic systems, found on the M109A6, with electric drives.

Recommendations

- Status of Previous Recommendations. The Army addressed seven of the previous recommendations. The following recommendations remain valid:
  1. Continue developmental breech component upgrades and verify corrections for the breech deficiencies.
  2. Consider replacing the M1068/A3 Fire Direction Center tracked vehicle with an alternative vehicle until the Armored Multi-Purpose Protection Vehicle is fielded.
  3. Examine suspension component wear associated with road wheels and track pads, and determine whether there is an inconsistency with Bradley in comparable weight configuration.
  4. Correct the deficiencies in the SPH crew compartment AFES and validate those fixes in test.
- FY17 Recommendations. The Army should:
  1. Leverage lessons learned from the suspended IOT&E and develop, implement, and test requisite hardware, software, training, and maintenance actions in comprehensive, operationally realistic IOT&E.
  2. Continue pursuit of final design, development, and testing of new cannon and breech assembly to address legacy breech and cannon reliability and to mitigate range and rate of fire shortcomings of the M109A7 as contrasted with allied and threat cannon artillery systems.

M88A2 Heavy Equipment Recovery Combat Utility Lift and Evacuation System (HERCULES)

Executive Summary
- The Army is planning to execute an Engineering Change Proposal (ECP) to the M88A2 Heavy Equipment Recovery Combat Utility Lift and Evacuation System (HERCULES) to enable single vehicle recovery (SVR) of the heaviest tracked combat vehicles in the fleet. The SVR capability has been lost due to incremental weight increases of the Abrams tank.
- The Army conducted four underbody blast events and an exploitation event in FY17 against the M88A2 HERCULES to establish the baseline survivability performance of the platform and inform required design improvements in the ECP program.
- The program funding is projected to start in FY18 and follow-on M88A2 ECP testing is planned for FY20.

System
- The M88A2 HERCULES included upgrades to the hoist, boom, main recovery winch, and engine of the M88A1. The Army intends the M88A2 ECP to regain SVR of the heaviest tracked combat vehicles in the fleet (currently the Abrams tank) by improving the powertrain, suspension, and track.
- The M88A2 HERCULES is currently unable to safely perform single vehicle recovery of the Abrams tank due to incremental weight increases of the Abrams over the years. The Abrams System Enhancement Package version 2 (SEPv2) has a combat weight of approximately 74 tons while the Abrams SEPv3 will increase the combat weight even further by 5 tons.
- The Army is exploring additional upgrades to be included in the M88A2 ECP program, expected to result in increased speed (both with and without load), better braking and slope performance, more hoisting and winching capacity, increased survivability, and increased reliability.

Mission
- Commanders will employ the upgraded M88A2 HERCULES to provide single vehicle towing, winching, and hoisting operations to support battlefield recovery operations and evacuation of heavy tanks and other tracked combat vehicles.
- The M88A2 HERCULES-equipped unit will recover tanks mired to different depths, remove M1 Abrams turrets and power packs, and upright overturned heavy combat vehicles.

Major Contractor
BAE Systems – York, Pennsylvania

Activity
- The Army conducted four underbody blast events from December 2016 to April 2017 to demonstrate the M88A2 baseline performance and inform the potential improvements to underbody survivability of the M88A2 HERCULES ECP program.
- The Army continued the assessment of M88A2 HERCULES performance in the FY15 to FY17 timeframe. The activities included towing, recovery and survivability technical assessments, auxiliary power unit performance testing, and follow-on production qualification.
- The prototyping will start as soon as the Army approves and funds the M88A2 ECP strategy. The next phase of testing is projected to begin in FY20.

Assessment

- The results of underbody mine testing in FY17 demonstrated the baseline survivability performance of the M88A2 HERCULES platform, and provided data to inform potential design improvements in an M88A2 ECP program, which could include improved seating and a reinforced floor structure.
- Limited space in the crew cabin, especially when the crew of the disabled vehicle is being transported in the M88A2 HERCULES, presents challenges both for survivability and ergonomics.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendations. None.

Patriot Advanced Capability-3 (PAC-3)

Executive Summary

- The Army conducted the Patriot Post Deployment Build-8 (PDB-8) IOT&E throughout FY/CY17, concluding in November 2017. Data from the IOT&E will support the PDB-8 fielding and Patriot Advanced Capability-3 (PAC-3) Missile Segment Enhancement (MSE) Full-Rate Production decisions in 2018.
- The Army conducted five Patriot flight test engagements using Patriot interceptors in FY/CY17, achieving intercepts of all targets: three short-range ballistic missile (SRBM) targets, one medium-range ballistic missile (MRBM) target, and one cruise missile target.
- As part of the IOT&E, the Army conducted Sustained Operations, Mobile Flight Mission Simulator, Interoperability, and Regression Phases, as well as a Cooperative Vulnerability and Penetration Assessment (CVPA) and a partial Adversarial Assessment (AA).

System

- Patriot is a mobile air and missile defense system that counters missile and aircraft threats. The newest version of Patriot hardware and software under development is PDB-8, which consists of improvements required to:
  - Counter the evolving threat
  - Improve combat identification and the Air Defense Interrogator Mode 5 Identification, Friend or Foe capability
  - Mitigate false tracks
  - Improve electronic protection
  - Integrate further the MSE interceptor/ground system capabilities
- The system includes the following:
  - C-band, multi-function, phased-array radars for detecting, tracking, classifying, identifying, and discriminating targets and supporting the guidance functions
  - Battalion and battery battle management elements
  - Communications Relay Groups and Antenna Mast Groups for communicating between battery and battalion assets
  - A mix of PAC-3 hit-to-kill interceptors and PAC-2 blast fragmentation warhead interceptors for negating missile and aircraft threats
- The newest version of the PAC-3 interceptor, the MSE, is in the production and fielding phase. The PAC-3 MSE provides increased battlespace defense capabilities and improved lethality over prior configuration Patriot interceptors.
- Earlier versions of Patriot interceptors include the Patriot Standard interceptor, the PAC-2 Anti-Tactical Missile, the Guidance Enhanced Missile (GEM) family (includes the GEM-T and GEM-C interceptor variants intended to counter tactical ballistic missiles (TBMs) and cruise missiles), the PAC-3 (baseline), and the PAC-3 Cost Reduction Initiative (CRI) variant.

Mission

Combatant Commanders use the Patriot system to defend deployed forces and critical assets from missile and aircraft attack and to defeat enemy surveillance air assets in all weather conditions and in natural and induced environments.

Major Contractors

- Prime: Raytheon Company, Integrated Defense Systems – Tewksbury, Massachusetts (ground system and PAC-2 and prior generation interceptors)
- PAC-3, PAC-3 CRI, and PAC-3 MSE Missiles: Lockheed Martin Corporation, Missile and Fire Control – Grand Prairie, Texas

Activity

- The Army conducted most testing in accordance with the DOT&E-approved Test and Evaluation Master Plan and test plans. The Army postponed one of the Missile Flight Test-A (MFT-A) intercepts against a fixed-wing aircraft target employing countermeasures until PDB-8.1 flight testing in 2021. The Army did not conduct the Patriot AA according to the DOT&E-approved test plan, resulting in some gaps in understanding PDB-8 cybersecurity. To address these gaps, the Army plans to conduct a second Patriot AA in October 2018.

- The Army conducted the PDB-8 IOT&E throughout FY/CY17 to support the PDB-8 fielding and PAC-3 MSE Full-Rate Production decisions. The IOT&E included the following events:
  - Sustained Operations phase in October 2016
  - CVPA in January 2017
  - Mobile Flight Mission Simulator missions in February to April 2017
  - A partial AA in May 2017
  - Interoperability testing in June 2017
  - MFT-A1 in June 2017 at White Sands Missile Range (WSMR), New Mexico. During this test, Patriot engaged a TBM target with a PAC-3 MSE interceptor and a GEM-T interceptor, and then engaged a cruise missile target with a PAC-3 MSE interceptor.
  - MFT-B in September 2017 at the Reagan Test Site, Kwajalein Atoll, Marshall Islands. During this test, Patriot engaged an MRBM target using a ripple method of fire (discharge of missiles in quick succession) and three PAC-3 MSE interceptors.
  - Regression Testing in July to August 2017 and in October to November 2017.
  - MFT-A2 in November 2017 at WSMR. During this test, Patriot simultaneously engaged and intercepted two TBM targets using two mixed ripples of interceptors (PAC-3 MSE/PAC-3 CRI and PAC-3 CRI/PAC-2 GEM-T).

Assessment

- Patriot successfully engaged all five targets during the PDB-8 IOT&E. Patriot also demonstrated some problems, including the following:
  - Patriot training remained inadequate to prepare operators for complex Patriot engagements. This was true during the PDB-7, PDB 6.5, and PDB-6 Limited User Tests (LUTs) as well.
  - Patriot had some classified effectiveness shortfalls.
  - Preliminary data suggest that Patriot ground system reliability did not meet the threshold requirement.
  - Patriot had some classified survivability and cybersecurity shortfalls.
- During the MFT-A1 flight test, Patriot demonstrated the capability to detect, track, engage, and intercept a TBM target with a mixed ripple engagement using PAC-3 MSE and PAC-2 GEM-T interceptors, and the capability to detect, track, engage, and intercept a cruise missile target with a PAC-3 MSE interceptor. During the MFT-A2 flight test, Patriot demonstrated the capability to detect, track, engage, and intercept two TBM targets using two ripples of interceptors (PAC-3 MSE/PAC-3 CRI and PAC-3 CRI/PAC-2 GEM-T). The PAC-3 MSE intercepted the Sabre target in its extended battlespace.
- During the MFT-B flight test, Patriot demonstrated the capability to detect, track, engage, and intercept an MRBM target in the PAC-3 MSE extended battlespace.
- Patriot has not had a flight test against a TBM target with a threat-representative payload since 2000, which limits the ability to assess Patriot lethality against TBMs.
- The Patriot CVPA revealed some cybersecurity shortfalls. The partial AA was not adequate to support a full assessment of cybersecurity.

Recommendations

- Status of Previous Recommendations. The Army satisfactorily addressed 15 of the previous 25 recommendations. The Army should continue to address the following recommendations:
  1. Conduct Patriot air and missile defense testing during joint and coalition exercises that include large numbers of different aircraft types, sensors, battle management elements, and weapons systems. Additionally, the Army should conduct Red Team AAs during joint exercises to test Patriot cybersecurity.
  2. Conduct a Patriot flight test against an anti-radiation missile target to validate models and simulations.
  3. Improve Patriot training to ensure that Patriot operators are prepared to use the system in combat.
  4. Have Patriot participate with live interceptors in Terminal High-Altitude Area Defense (THAAD) flight testing to determine Patriot-to-THAAD interoperability and the capability for Patriot to intercept tactical ballistic missile targets that THAAD does not intercept. (The FY16 National Defense Authorization Act requires at least one intercept or flight test each year that demonstrates interoperability and integration among Patriot, THAAD, and/or Aegis BMD.)
  5. Collect operational reliability data on Patriot systems in the field in order to calculate the Mean Time Between Critical Mission Failures.
  6. Use test units for future Patriot operational tests that have operationally representative distributions in soldier proficiency.
  7. Conduct future operational flight tests with unannounced target launches within extended launch windows.
  8. Improve Patriot radar reliability.
  9. Conduct a simultaneous engagement of a cruise missile target with a PAC-2 GEM-T interceptor and a maneuvering full-scale, fixed-wing aircraft target employing electronic countermeasures with a PAC-3 MSE interceptor.
  10. Have Patriot participate with live interceptors in Aegis BMD flight testing to determine Patriot-to-Aegis BMD interoperability and the capability for Patriot to intercept ballistic missile targets that Aegis BMD does not intercept.
- FY17 Recommendations. The Army should:
  1. Fix the cybersecurity vulnerabilities identified during the CVPA and limited AA and verify these fixes through subsequent cybersecurity testing.
  2. Conduct future TBM flight tests with targets having threat-representative payloads to adequately assess Patriot lethality against TBMs.
  3. Conduct an adequate AA that assesses insider, nearsider, and outsider attack vectors using representative trained soldier-operators in all manned stations.

Soldier Protection System (SPS)

Executive Summary

- The Soldier Protection System (SPS) is a suite of personal protection subsystems intended to provide equal or increased levels of protection against small-arms and fragmenting threats compared to existing personal protection equipment and at reduced weights.
- The SPS consists of the soft armor Torso and Extremity Protection (TEP) subsystem; the hard armor Vital Torso Protection (VTP) subsystem; the Integrated Head Protection System (IHPS) subsystem; and the Transition Combat Eye Protection (TCEP) subsystem. Each SPS subsystem is compatible with existing personal protective equipment. The Army plans to issue SPS to deploying units rather than issue SPS to individual soldiers at each Army installation.
- Each of the four SPS subsystems (TEP, VTP, IHPS, and TCEP) is a separate Program of Record with its own schedule. The Army made a Full-Rate Production decision for the TEP in September 2016, and plans to make Full-Rate Production decisions for VTP and IHPS in 3QFY18.
- The Army resumed first article testing of the Enhanced Small Arms Protective Insert (ESAPI) and the X Threat Small Arms Protective Insert (XSAPI) VTP hard armor plates. The Army began testing the IHPS in August 2017, and is scheduled to complete testing of both the VTP and IHPS in early FY18.

System

- The SPS is a suite of personal protection subsystems intended to provide equal or increased levels of protection against small-arms and fragmenting threats compared to existing personal protection equipment and at reduced weights. The SPS subsystems are designed to protect a soldier's head, eyes, and neck region; the vital torso and upper torso areas, as well as the extremities; and the pelvic region. Soldiers can configure the various components to provide different tiers of protection depending on the threat and the mission.
- The SPS consists of four subsystems:
  - VTP consists of front and rear hard armor torso plates (either the ESAPI or the XSAPI), along with the corresponding hard armor side plates (Enhanced Side Ballistic Insert (ESBI) or the X Threat Side Ballistic Insert (XSBI)).
  - TEP consists of the soft armor Modular Scalable Vest (MSV) with provision for adding the Ballistic Combat Shirt (BCS) for extremity protection, the Blast Pelvic Protector (BPP) for pelvic and femoral artery protection, and a Load Distribution System (LDS) that is integrated within the TEP and provides the capability to redistribute the weight burden from the shoulders to the hips. In response to soldier feedback and an updated requirement, the Army intends to procure a Battle Belt as a stand-alone weight distribution system (WDS) instead of the LDS.

  - IHPS consists of a helmet with provision for adding a mandible and/or visor, as well as for mounting an applique to the outside of the helmet for additional ballistic protection.
  - TCEP consists of either ballistic spectacles or goggles to protect the soldier's eyes as well as provide the capability to transition from light to dark and dark to light in 1 second or less to enhance the soldier's vision in varying combat conditions.
- The Army initially plans to issue SPS via a Rapid Fielding Initiative (RFI) to deploying units rather than issue SPS to individual soldiers at each Army installation.

Mission

Units with soldiers wearing the SPS will accomplish assigned missions while concurrently protecting themselves against injury from a variety of ballistic (small-arms and fragmenting) threats.

Major Contractors

- TEP Full-Rate Production Vendors/Designs (Multiple vendors to stimulate competition and achieve best price through Fair Opportunity awards):
  - KDH Defense Systems Inc. – Eden, North Carolina (MSV, BPP)
  - Bethel Industries Inc. – Jersey City, New Jersey (MSV, BPP)
  - Hawk Protection – Pembroke Pines, Florida (MSV, BPP)

- Short Bark Industries – Venor, Tennessee (BCS)
- Carter Enterprises Industries Inc. – Brooklyn, New York (BCS, LDS)
- Eagle Industries Unlimited – Virginia Beach, Virginia (BCS)
- TBD mid-CY18 (Battle Belt)

- IHPS Vendor:
  - 3M/Ceradyne – Costa Mesa, California
- VTP LRIP Vendors:
  - BAE Systems – Phoenix, Arizona (XSAPI, ESBI, XSBI)
  - 3M/Ceradyne – Costa Mesa, California (ESAPI)

Activity

- The SPS consists of four subsystems (TEP, VTP, IHPS, and TCEP); the development, testing, and production/fielding of the four subsystems are on different timelines. The Army made a Full-Rate Production decision for the TEP in September 2016, and plans to make Full-Rate Production decisions for both VTP and IHPS in April 2018. Each SPS subsystem is compatible with existing (legacy) personal protective equipment (for example, soldiers can use existing hard armor plates in the new MSV). The Army is testing SPS ballistic performance in accordance with DOT&E-approved test plans.
- An LDS was originally a component of the TEP subsystem that addressed a TEP requirement for an integrated WDS. In response to soldier feedback and concerns about the LDS, the Army revised the WDS requirement to that of a stand-alone WDS. The Army intends to use a Battle Belt to meet this requirement and plans Battle Belt contract award in mid-CY18.
- The Army began VTP testing in December 2015 with first article testing of the ESAPI hard armor plates. Shortly thereafter, the Army halted further ESAPI testing because test personnel found deficiencies in the plates while conducting physical characterization of the plates prior to starting ballistic testing. Following a period of corrective action, the vendor resubmitted the ESAPI plates for first article testing, which occurred July through August 2016. Although the ESAPI met ballistic requirements, there were non-ballistic deficiencies for the vendor to correct. While the vendor was addressing these non-ballistic deficiencies, the vendor offered a newer, lighter weight design to the Army. The Army accepted this new design, and began testing it in June 2017. The Army conducted first article testing of the ESBI, XSBI, and XSAPI hard armor plates in May 2016. The XSAPI plate did not meet either the ballistic or the non-ballistic requirements. The vendor completed corrective actions and resubmitted the XSAPI for another first article test, which began in August 2017. The Army will continue VTP testing in FY18.
- The Army began testing of IHPS in August 2017. IHPS testing included:
  - A Limited User Test of the IHPS and TCEP in August 2017 at Joint Base Lewis-McChord, Washington, to assess the effect of the IHPS/TCEP on soldier mobility and subsequent mission effectiveness. DOT&E is analyzing the data from this test.
  - A series of first article and sub-system-level live fire testing of the IHPS began in August 2017 and will continue into FY18. Sub-system-level testing will include testing of the IHPS against various foreign threats. Future testing includes a series of events to characterize the performance of the IHPS when subjected to blast threats, as well as flash heat and fire threat testing to evaluate the IHPS's ability to protect an individual from burns resulting from a flash fire.
- The Army conducted first article testing of the TCEP in July 2017. The TCEP did not meet requirements, so the vendor has initiated corrective action to correct the deficiencies and resubmit the TCEP for first article testing.

Assessment

- DOT&E documented the performance of the TEP subsystem in the report to Congress in September 2016 to support the TEP Full-Rate Production decision.
- The assessment of the VTP and IHPS data is ongoing. DOT&E will report on VTP and IHPS performance upon test completion in FY18.

Recommendations

- Status of Previous Recommendations. The Army addressed the previous recommendation to improve the design of both the LDS and the BCS. The Army still needs to:
  1. Continue to improve its body armor blast testing and analysis procedure.
  2. Use a broader range of fragment simulators to more fully represent the expected threat environment and to then more fully characterize TEP performance.
  3. Quantify the uncertainty associated with its modeling estimates and assess the impact of that uncertainty on the evaluation of TEP performance.
  4. Ensure that all modeling of TEP is accompanied by at least one actual test against a modeled threat to compare modeled TEP performance with actual test results.
- FY17 Recommendations. None.

Spider Increment 1A M7E1 Network Command Munition

Executive Summary
- The Program Executive Officer approved Spider Increment 1A's entry into low-rate initial production in June 2017.
- Spider Increment 1A is not meeting the reliability requirement for the Remote Control Station (RCS) to operate a Spider munition field for a 72-hour mission with a 96 percent chance of not having an Essential Function Failure (EFF).
- Software version 1.8.3 is not mature. The program has no plans to change or update software version 1.8.3 prior to the IOT&E planned for 4QFY18.
- During the August 2017 Cooperative Vulnerability and Penetration Assessment (CVPA), the Army demonstrated that it had mitigated most of the cyber vulnerabilities reported in DOT&E's January 2017 Operational Assessment. Some vulnerabilities still exist. Analysis of the data continues.

System
- The Army uses Spider as a landmine alternative to satisfy the requirements outlined in the 2004 National Landmine Policy that directed the DOD to:
  - End use of persistent landmines after 2010
  - Incorporate self-destructing and self-deactivating technologies in alternatives to current persistent landmines
- A Spider munition field includes:
  - Up to 63 Munition Control Units (MCUs), each housing up to 6 miniature grenade launchers or munition adapter modules (the modules provide remote electrical firing capabilities)
  - An RCS consists of a Remote Control Unit (RCU) and RCU Transceiver (RCUT). An operator uses the RCS to maintain "man-in-the-loop" control of all munitions in a field. The RCU is the component upgraded in Spider Increment 1A.
  - A repeater or communications relay device for use in difficult terrain or at extended ranges
- Spider incorporates self-destructing and self-deactivating technologies to reduce residual risks to non-combatants and has the capability to use non-lethal munitions such as the Modular Crowd Control Munition that fires rubber sting balls.
- The Army fielded Spider Increment 1 systems in FY09 under an Urgent Materiel Release. The system reached Initial Operational Capability in FY11 and obtained its Full Materiel Release in FY13.

Mission
Brigade Combat Team commanders employ engineer units equipped with Spider to provide force protection and counter-mobility obstacles using lethal and non-lethal munitions. Spider functions as a stand-alone system or in combination with other obstacles to accomplish the following:
- Provide early warning
- Protect the force
- Delay and attrit enemy forces
- Shape the battlefield

Major Contractor
Command and Control hardware and software: Northrop Grumman Information Systems Sector, Defense Systems Division – Redondo Beach, California

Activity
- DOT&E published an Operational Assessment report in January 2017 based on results from the 2016 Spider Increment 1A Limited User Test (LUT).
- The Army approved a change in the Spider Increment 1A Capabilities Production Document in January 2017. The document establishes the requirement to send digital obstacle reports from Spider Increment 1A to the classified mission command system. The Army downgraded this Key Performance Parameter from a threshold to an objective requirement.
- The Army continued its contract with Northrop Grumman to refine Spider Increment 1A software during FY17. Northrop Grumman conducted a number of reliability tests to assess

software changes designed to address reliability problems found in the 2016 LUT.
- The Army conducted a Formal Qualification Test in April 2017 and a Record Reliability Test in May 2017.
- DOT&E approved the Spider Increment 1A Milestone C Test and Evaluation Master Plan (TEMP) in June 2017. The Army conducted all 2017 testing in accordance with an approved TEMP.
- The Army conducted the System Verification Test in June 2017 to demonstrate Spider Increment 1A reliability. Portions of the test included soldiers per DOT&E request.
- The Program Executive Officer approved Spider Increment IA to enter low-rate initial production in June 2017 and awarded the contract in October 2017.
- The Army conducted the CVPA to assess cyber vulnerabilities in August 2017.

Assessment
- The DOT&E operational assessment of the 2016 LUT found that a unit could use Spider Increment 1A as a component of protection and counter-mobility missions. Poor reliability slowed emplacement times and forced commanders to extend planning times during mission preparations. Spider Increment 1A did not meet its reliability requirement during the LUT using software release 1.3. DOT&E found that Spider was not survivable in cyber and electronic warfare contested environments.
- Spider Increment 1A is not meeting the reliability requirement for the RCS to operate a Spider munition field for a 72-hour mission with a 96 percent chance of not having an EFF.
  - An EFF causes the system to lose control of the munition field for more than 20 minutes.
  - Thirteen of 18 missions (72 percent) in the Formal Qualification Test, Record Reliability Test, and System Verification Test did not have an EFF.
  - Most test missions were less than 72 hours.
  - These tests used experienced civilian operators.
- Software version 1.8.3 is not mature. DOT&E attributed 37 of the 101 failures during testing to the RCU with version 1.8.3 software. At this time, the Army has no plans to change or update the Spider software version 1.8.3 prior to the IOT&E planned for 4QFY18.
- The CVPA found the updated software addressed many of the vulnerabilities identified in the DOT&E FY17 Operational Assessment. Some vulnerabilities still exist. Analysis of the results is ongoing.
- Spider Increment 1A is no longer required to send digital obstacle reports to the classified mission command system. At this time, there is no approved cross-domain solution allowing the unclassified Spider to pass digital information to the classified mission command system. This makes it more difficult for units to update the mission command system, which adversely affects the ability of units to know in real time where Spider fields are located on the battlefield.

Recommendations
- Status of Previous Recommendations. The Army addressed previous recommendations with the exception of the following:
  1. The Army has not resolved the problem between Spider Increment 1A and the mission command system preventing Spider Increment 1A from sending digital obstacle reports to the classified mission command systems. The Army has downgraded this Key Performance Parameter to an objective requirement.
  2. The Army developed a reliability growth program, but reliability problems to the RCU and RCUT caused critical failures during reliability testing. Additionally, MCU reliability problems seen at the 2016 LUT continue to occur. The Army does not plan to address reliability problems found during recent reliability testing until after the IOT&E.
- FY17 Recommendation.
  1. The Army should update the current Increment 1A software to address known reliability problems and demonstrate improved MCU reliability prior to the 4QFY18 IOT&E.

Stryker 30mm Infantry Carrier Vehicle – Dragoon (ICVD)

Executive Summary
- The Army initiated the Stryker 30 mm Infantry Carrier Vehicle – Dragoon (ICVD) program in July 2015 in response to an Operational Needs Statement (ONS) from U.S. Army Europe for improved or upgraded lethality of organic direct fire weapons to support dismounted infantry when engaging like units, or those supported by light armored vehicles.
- The ICVD integrates an unmanned turret with a 30 mm autocannon onto a flat-bottom Stryker Infantry Carrier Vehicle chassis with upgraded suspension and larger tires.
- In FY17, the Army conducted full-up system-level (FUSL) live fire testing of the ICVD to assess platform survivability against a spectrum of operationally realistic threats. Preliminary assessments demonstrate that stowed 30 mm ammunition on the ICVD represents a unique platform vulnerability that is not present on other vehicles in the Stryker fleet. Underbody protection afforded by the ICVD is limited due to the flat-bottom Stryker hull.
- In FY17, the Army conducted a user excursion using soldiers from the 2nd Cavalry Regiment (2CR) to validate development of gunnery training tables to support the operational test in February 2018 in Germany.
- Lethality testing to assess the 30 mm ammunition is ongoing.

System
- The Stryker 30 mm ICVD program integrates an unmanned turret with a 30 mm autocannon onto a flat-bottom Stryker Infantry Carrier Vehicle. Initiated via a limited ONS, the ICVD is not a program of record.
- The 30 mm autocannon is intended to employ High Explosive Incendiary – Tracer and Armor Piercing Fin Stabilized Discarding Sabot – Tracer rounds. The crew is intended to be able to reload these munitions under armor.
- The ICVD features a coaxial machine gun and smoke grenades on the turret.

- A Directed Requirement memorandum from the Assistant Secretary of the Army (Acquisition, Logistics and Technology) approves 81 Stryker ICVD vehicles for fielding to 2CR.

Mission
- Units equipped with the Stryker ICVD will provide Combatant Commanders a medium-weight force capable of rapid strategic and operational mobility to disrupt or destroy enemy military forces, to control land areas including populations and resources, and to conduct combat operations to protect U.S. national interests.
- The direct fire weapon system upgrade is intended to provide effective mounted and dismounted combined arms and freedom of maneuver during combat operations.

Major Contractors
- General Dynamics Land Systems – Sterling Heights, Michigan
- Kongsberg Gruppen – Kongsberg, Norway
- Orbital ATK – Mesa, Arizona

Activity
- DOT&E approved the Operational Test Agency Test Plan and Detailed Test Plan for the Stryker ICVD FUSL live fire survivability testing on June 14, 2017. The testing consists of 12 events encompassing theater-relevant threats to include underbody mines, airburst artillery, and rocket-propelled grenades. FUSL live fire testing is scheduled to be complete in December 2017.
- The Army conducted an ICVD user excursion in 4QFY17 using soldiers from 2CR to validate gunnery tables, collect early user feedback on the usability of the 30 mm weapon system, and refine training material taught to crews during New Equipment Training.
- Planning for lethality testing is ongoing and will include characterization of 30 mm ammunition and engagements against operationally realistic targets.

Assessment
- Stowage of 30 mm ammunition in the ICVD represents a unique vulnerability not present for other Stryker vehicles. Live fire testing has revealed that threat engagement consequences for the ICVD may differ significantly from the rest of the Stryker family of vehicles due to stowed ammunition.

- The current ICVD live fire test plan addresses threats specific only to the European theater. The scope of this test plan will need to increase to support worldwide fielding of the ICVD if this becomes a program of record.
- Soldier and crew feedback collected during the user excursion was used to validate development of gunnery training tables to support the operational test in February 2018.
- Previous 30 mm ammunition test data along with preliminary coupon testing indicate that the 30 mm ammunition is expected to produce the desired effects against threat armored vehicles in the target suite; the ongoing lethality testing will verify this assertion. Effects against urban barriers are inferred from previous 30 mm ammunition test data. Although the 30 mm ammunition fired against urban barriers in previous tests was not fired from an ICVD platform, terminal effects are expected to be similar.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendation.
  1. If the Stryker 30 mm ICVD becomes a program of record, additional testing will be required to fully characterize the platform against the worldwide threat spectrum and against urban barriers.

Stryker Double V-Hull A1 (DVH A1) Engineering Change Proposal (ECP)

Executive Summary

- The Army Test and Evaluation Command (ATEC) conducted a side-by-side test of Infantry Carrier Vehicles from the legacy Stryker Double V-Hull (DVH) fleet and the future Stryker DVH A1 Engineering Change Proposal (ECP) fleet at Aberdeen Test Center (ATC), Maryland, in March 2016. The purpose of the event was to collect early feedback on the differences between the Infantry Carrier Double V-Hull (ICVV) and the ECP-modified ICVV (ICVV-A1).
- The ICVV-A1's automotive performance and engine power is superior to that of the ICVV based on collected soldier feedback and instrumentation data. Soldiers noted the ICVV-A1 improved drivetrain easily negotiated steep grades with decreased engine load, which should result in greater mobility in combat.
- ATC completed full-up system-level (FUSL) live fire testing for the Stryker ICVV-A1 in 1QFY17 in accordance with DOT&E-approved test plans. ATC also completed Automatic Fire Extinguishing System (AFES) testing for the Stryker DVH A1 ECP in 1QFY17. Testing revealed that ECP modifications did not result in any new, critical vulnerabilities for the Stryker DVH A1 ECP.

System

- The Stryker DVH A1 ECP Family of Vehicles (FoV) consists of seven variants on a common vehicle platform, each of which replaces a legacy Flat-Bottom Hull (FBH) Stryker:
  - Anti-Tank Guided Missile (ATVV-A1)
  - Commander's Vehicle (CVV-A1)
  - Engineer Squad Vehicle (ESVV-A1)
  - Fire Support Vehicle (FSVV-A1)
  - Infantry Carrier Vehicle (ICVV-A1)
  - Mortar Carrier Vehicle (MCVV-A1)
  - Medical Evacuation Vehicle (MEVV-A1)
- The ICVV-A1 can be equipped with a scout Mission Equipment Package (MEP) modification. The ICVV-A1 with the scout MEP replaces an eighth legacy FBH variant, the Reconnaissance Vehicle (RV), providing Stryker infantry and cavalry scouts with RV functionality on a unique DVH A1 ECP-based platform.
- The Army intends to implement the following Stryker DVH A1 ECP configuration upgrades:

Mechanical Power Upgrade

- Replaces a 350 horsepower Caterpillar C7 engine with a 450 horsepower Caterpillar C9 engine
- Integrates improved power pack thermal management and additional environmental conditioning

Electrical Power Upgrade

- Replaces a 570 amp alternator with a 910 amp alternator capable of supporting electrical power required for future network upgrades and 20 percent growth
- Replaces the Power Distribution Panel (PDP) and Power Distribution Panel 2 (PDP2) with the Enhanced Power Distribution Unit (EPDU)

Chassis Upgrade

- Increases chassis payload capacity from 55,000 pounds Gross Vehicle Weight Rating (GVWR) to 63,000 pounds GVWR
- Optimizes the driveline to match the new mechanical power upgrade

Implementation of an In-Vehicle Network Architecture

- Establishes the framework for future embedded, VICTORY compliant, Army Network integrations, and provides for sharing of platform data among the Stryker's common crew stations
- Provides gigabit Ethernet capability

Mission

Units equipped with the Stryker DVH A1 ECP FoV will provide Combatant Commanders a medium-weight force capable of rapid strategic and operational mobility to disrupt or destroy enemy military forces, to control land areas including populations and resources, and to conduct combat operations to protect U.S. national interests.

Major Contractors
General Dynamics Land Systems – Joint Base Lewis-McChord, Washington; Sterling Heights, Michigan; Anniston, Alabama

---

Activity
- ATEC conducted a side-by-side test of Infantry Carrier Vehicles from the legacy Stryker Double V-Hull fleet and the future Stryker Double V-Hull A1 ECP fleet at ATC in March 2016. The Army published its final report in December 2016. ATEC used soldier surveys and vehicle instrumentation to compare automotive performance and collect Human Systems Integration feedback on the differences between the ICVV and ICVV-A1.
- The Program Executive Office used data from the side-by-side developmental test to authorize the conversion of up to 253 DVH variants to DVH ECP A1 variants. The Army plans to use soldier feedback and instrumented data from the operational test scheduled for 4QFY18 to inform its decision to authorize the conversion of three additional brigades from DVH variants to DVH A1 ECP variants.
- The Army has not announced which Stryker Brigade Combat Team will be the first to field the Stryker DVH ECP A1 variants.
- ATC completed FUSL live fire testing for the Stryker ICVV-A1 in 1QFY17 in accordance with DOT&E-approved test plans. FUSL testing consisted of 14 events encompassing a spectrum of operationally realistic threats to include underbody and underwheel mines, ground-emplaced IEDs, airburst artillery, rocket-propelled grenades, and explosively formed penetrators. ATC also completed AFES and controlled damage testing for the Stryker DVH A1 ECP in 1QFY17.
- The Army is writing a Test and Evaluation Master Plan (TEMP) to test all Stryker DVH A1 ECP variants in an operationally realistic environment against an opposing force. The Army intends for the TEMP to include Cooperative Vulnerability and Penetration Assessment and Adversarial Assessment cybersecurity testing.

Assessment
- Soldier feedback and instrumentation identified:
  - ICVV-A1 automotive performance and engine power is superior to that of the ICVV. Soldiers noted the ICVV-A1 improved drivetrain easily negotiated steep grades with decreased engine load, which should result in greater tactical mobility in combat.
  - The ICVV-A1 was initially slower than the ICVV when starting from a stationary position but the ICVV-A1 has greater acceleration beyond 50 meters once the turbocharger is engaged.
- The soldiers noted:
  - The Driver's Situational Awareness Display and Commander's Situational Awareness Display in the ICVV-A1 enhanced shared understanding among crew members regarding automotive data and performance.
  - The ride quality of the ICVV-A1 is superior to the DVH when traveling off-road or traversing rough terrain.
  - The external noise level of the ICVV-A1 is higher than the ICVV. There is no change to the interior noise level
- Side-by-side developmental soft soil mobility testing was not conclusive. Follow-on analysis using the NATO Reference Mobility Model and comparative testing during a controlled damage experiment show the ICVV-A1 has greater soft soil mobility than the ICVV.
- FUSL live fire testing and AFES testing demonstrated that ECP modifications did not result in any new, critical vulnerabilities for the Stryker DVH A1 ECP.

Recommendations
- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendations. None.

Warfighter Information Network – Tactical (WIN-T)

Executive Summary

- In July 2017, the Army conducted a Warfighter Information Network – Tactical (WIN-T) Increment 2 Tactical Communications Node – Lite (TCN-L) and Network Operations Security Center – Lite (NOSC-L) FOT&E to support a fielding decision to light forces. The FOT&E was conducted in accordance with a DOT&E-approved test plan and was adequate to assess operational effectiveness, operational suitability, and survivability.
- Results from the TCN-L and NOSC-L FOT&E are:
  - The TCN-L and NOSC-L are operationally effective. The TCN-L and NOSC-L supported light infantry brigade missions under operationally realistic conditions.
  - The TCN-L and NOSC-L are operationally suitable. Both systems met their reliability requirements, and exceeded their availability and maintainability requirements.
  - WIN-T Increment 2 is survivable. WIN-T Increment 2 demonstrated a robust cyber network defense to protect against an operationally realistic cyber threat opposing force. The virtual firewall and improved software tools were effective. The program provided one expert field service representative to implement improved cybersecurity by configuring the virtual firewall and assisting soldiers with operation and maintenance of the virtual firewall. To sustain this level of improved cybersecurity, the Army must either resource field service representatives or train Signal Soldiers to accomplish these complex tasks.
- The FY16 National Defense Authorization Act directed the DOD to conduct a comprehensive assessment of the current and future capabilities and requirements of the Army's air-land, mobile tactical communications and data networks. As a result of this assessment, the Army requested to halt procurement of WIN-T Increment 2 at the end of FY18. The Army intends to field TCN-L and NOSC-L to Infantry Brigade Combat Teams and complete fielding of WIN-T Increment 2 to Stryker Brigade Combat teams. The Army no longer plans to field WIN-T Increment 2 to Armored Brigade Combat Teams.

CH-47 Transporting TCN-L

Network Operations Security Center - Lite (NOSC-L)

Tactical Communications Node - Lite (TCN-L)

System

- The Army designed WIN-T as a three-tiered communications architecture (space, terrestrial, and airborne) to serve as its high-speed and high-capacity tactical communications network.
- The Army intends WIN-T to provide reliable, secure, and seamless communications for units operating at theater level and below.
- The WIN-T program consists of three funded increments. In May 2014, the Defense Acquisition Executive approved the Army's request to stop development of the Increment 3 aerial tier of networked, airborne communications relays and limit Increment 3 to network management and satellite waveform improvements.
  - Increment 1: "Networking At-the-Halt" enables the exchange of voice, video, data, and imagery throughout the tactical battlefield using a Ku-band and Ka-band satellite-based network. The Army has fielded WIN-T Increment 1 to its operational forces.
  - Increment 2: "Initial Networking On-the-Move" provides command and control on-the-move down to the company level for maneuver brigades and implements an improved network security architecture.
    - WIN-T Increment 2 supports on-the-move communications for commanders with the addition of the Point of Presence and the Soldier Network Extension, and provides a mobile network infrastructure with the Tactical Communications Node. It employs a terrestrial Highband Networking Waveform and a satellite Network Centric Waveform to support its network mobility goals.
    - WIN-T Increment 2 provides a downsized, air-transportable variant of the High Mobility Multi-purpose Wheeled Vehicle (HMMWV)-mounted configuration to support the Army's Global Response Force and other light brigades. The downsized WIN-T variants include the TCN-L and the NOSC-L.
  - Increment 3: "Full Networking On-the-Move" was to provide full mobility mission command for all Army field commanders, from theater to company level using networked airborne communication relays. With program

reductions, WIN-T Increment 3 now provides enhanced network operations and an improved satellite waveform to WIN-T Increments 1 and 2.

Mission

Commanders at theater level and below will use WIN-T to:

- Integrate satellite-based communications capabilities into an everything-over-Internet Protocol network to provide connectivity, while stationary, across an extended, non-linear battlefield, and at remote locations (Increment 1).
- Provide division and below maneuver commanders with mobile communications capabilities to support initial command and control on-the-move (Increment 2).

Major Contractor

General Dynamics, C4 Systems – Taunton, Massachusetts

Activity

- In September 2016, the Army conducted the WIN-T Increment 2 Developmental Test Phase One at Fort Bliss, Texas. The developmental test validated TCN-L technical Key Performance Parameters and readiness for entrance into operational test.
- In December 2016, the Army conducted the WIN-T Increment 2 Developmental Test Phase Two at Fort Campbell, Kentucky. The developmental test validated the readiness of the NOSC-L for entrance into operational testing and served to validate instrumentation and data reduction for operational test.
- The Army conducted a WIN-T Increment 2 TCN-L and NOSC-L FOT&E during the July 2017 Network Integration Evaluation 17.2. The 2nd Infantry Brigade Combat Team, 101st Airborne Division conducted operationally realistic missions at Fort Bliss, Texas. The FOT&E focused on the integration of TCN-L and NOSC-L capabilities into HMMWV platforms and the ability of a unit equipped with the downsized configuration items to support its mission. The Army conducted the test in accordance with a DOT&E-approved test plan.
- DOT&E finalized the emerging results for the WIN-T Increment 2 TCN-L NOSC-L FOT&E in October 2017 and intends to complete an assessment of the FOT&E to support an Army TCN-L NOSC-L fielding decision in 1QFY18.
- The FY16 National Defense Authorization Act directed the DOD to conduct a comprehensive assessment of the current and future capabilities and requirements of the Army's air-land, mobile tactical communications and data networks. As a result of this assessment, the Army requested to halt procurement of WIN-T Increment 2 at the end of FY18. The Army intends to field TCN-L and NOSC-L to Infantry Brigade Combat Teams and complete fielding of WIN-T Increment 2 to Stryker Brigade Combat teams. The Army no longer plans to field WIN-T Increment 2 to Armored Brigade Combat Teams.

Assessment

- The Army's execution of the WIN-T Increment 2 TCN-L and NOSC-L FOT&E was adequate to support the assessment of operational effectiveness, operational suitability, and survivability.
- Results from the WIN-T Increment 2 TCN-L NOSC-L FOT&E are:
  - The TCN-L and NOSC-L are operationally effective. The downsized TCN-L and NOSC-L demonstrated success in supporting the unit's mission. Brigade soldiers were able to plan, install, operate, and maintain a WIN-T network under operationally realistic conditions.
  - NOSC-L tools were effective and useful with the exception of the network operations summary board, which portrayed delayed network information and did not support network monitoring.
  - The brigade was able to transport the TCN-L and NOSC-L by CH-47F helicopters in a realistic tactical environment.
  - The NOSC-L is operationally suitable and met its reliability requirement. NOSC-L training provided by the Army should be improved. Soldiers requested more in-depth training to include advanced theory of operations, system operations, troubleshooting, and software use.
  - The TCN-L is operationally suitable and met its reliability requirement, but not with confidence (80 percent lower confidence bound). TCN-L training provided by the Army is not adequate for soldiers to be able to install, operate, and maintain the system.
  - The TCN-L and NOSC-L exceeded their availability and maintainability requirements.
  - WIN-T Increment 2 is survivable. WIN-T Increment 2 demonstrated a robust cyber network defense to protect against an operationally realistic cyber threat opposing force. The virtual firewall and improved software tools were effective. The program provided one expert field service representative to implement improved cybersecurity by configuring the virtual firewall and assisting soldiers with operation and maintenance of the virtual firewall. To sustain this level of improved cybersecurity, the Army must either resource field service representatives or train Signal Soldiers to accomplish these complex tasks.

Recommendations

- Status of Previous Recommendations. The program addressed four of five previous recommendations. The Army has not demonstrated an improved integration of WIN-T into Stryker combat vehicles.
- FY17 Recommendations. The Army should:

1. Fix the implementation of WIN-T cybersecurity. The Army should either resource field service representatives or train Signal Soldiers to accomplish these complex tasks.
2. Improve training provided to TCN-L and NOSC-L soldiers.
3. Improve the NOSC-L network operations summary board to provide timely and accurate information to support WIN-T network monitoring.
4. Demonstrate WIN-T improvements in future operational test.

XM17/XM18 Modular Handgun System (MHS)

Executive Summary

- The Army selected SIG SAUER's full-size (XM-17) and compact (XM-18) variant pistols for the Army Modular Handgun System (MHS), and awarded a production contract to SIG SAUER on January 19, 2017.
- The Army conducted operational and live fire testing for both variants in FY17. Analysis is ongoing for operational effectiveness, operational suitability, and lethality. DOT&E intends to submit a combined IOT&E/LFT&E report to Congress in 2QFY18.
- During drop testing in which an empty primed cartridge was inserted, the striker struck the primer causing a discharge. SIG SAUER implemented an Engineering Change Proposal (ECP) to correct this deficiency by implementing lightweight components in the trigger group mechanism. This fix may have contributed to the splintering of two triggers during the IOT&E.
- Both the XM17 and XM18 pistols experienced double-ejections where an unspent ball round was ejected along with a spent round. Due to the increased frequency of occurrence during Product Verification Test (PVT), the Army stood up a root cause analysis team to identify the cause of the double ejections in parallel with continued PVT. As of this report, this analysis is still ongoing.
- During the PVT testing, the MHS with ball ammunition demonstrated significantly more stoppages than with the special purpose munition.
- During IOT&E, the MHS with special purpose munition met its Mean Rounds Between Failure (MRBF) reliability requirement. It did not meet its Mean Rounds Between Stoppage (MRBS) reliability requirement. For the MHS, a stoppage is defined as any deficiency that prevents the pistol from operating as intended, but is corrected through immediate action. A failure is defined as a hardware deficiency that requires replacement or repair. Slide stoppages accounted for 50 percent of XM17 stoppages, and 75 percent of the XM18 stoppages observed during IOT&E. In these stoppages, the slide failed to lock after users fired the last round in the magazine.

1 - XM17, Full Size, with 21-round magazine
2 - XM18, Compact, with 17-round magazine
3 - XM1152 Ball round
4 - XM1153 Special Purpose (SP) round
5 - XM1156 Dummy round
6 - XM1157 Blank round
7 - Slide Catch Lever

System

- The MHS program is comprised of the XM17 full-size variant and XM18 compact variant 9 mm pistols. The majority of Army MHS users will use the XM17 variant. Individuals and units requiring a concealed weapon will use the XM18 variant.
- Both variants include modular features to allow for the future addition of different targeting enablers (e.g., infrared and visible laser pointers), pistol grips, and alternate magazine options.
  - Targeting enablers can be mounted on the weapon using a standard platform known as Picatinny rails.
  - Small, medium, and large polymer grip modules accommodate different hand sizes.
- The XM17 and XM18 pistols are mechanically locked, short-recoil operated weapons. Common features include an automatic striker pin safety lock reversible magazine catch to accommodate left- or right-handed shooters, ambidextrous manual safety, and external slide catch lever. Loading is automatic with each shot fired, until the magazine is empty. The slide is locked to the rear after the last shot is fired.
- The MHS incorporates a non-reflective, neutral color for detection avoidance. The Army intends for the MHS to be operable with a future suppressor.
- The Army required the weapon to use ball ammunition and special purpose ammunition. The XM1152 Ball cartridge uses a 115 grain truncated nose full metal jacket projectile and the

XM1153 Special Purpose cartridge uses a 147 grain jacketed hollow point projectile.
- The contractor provides two 21-round magazines and one 17-round magazine with each pistol as part of the MHS.
- The MHS is an Army program with joint interest. The Army, including Army Special Operations Command, intends to purchase 238,000 pistols (approximately 231,000 XM17 and 7,000 XM18). The Navy, Marine Corps, and Air Force may purchase 224,000 pistols under the same contract.

Mission
- Military personnel conducting core mission combat operations use the MHS for personal self-defense and as their secondary weapon system. Core missions include anti-terrorism, direct action, force protection, anti-hijacking, evasion, special investigations, special operations, reconnaissance, protective service, law enforcement, resource protection, base security and terminal air control, and combat search and rescue. Civil affairs and peacekeeping operations are core missions in some Services.
- Military personnel conducting collateral activities use the MHS as their primary weapon system. Collateral activities include foreign and U.S. humanitarian assistance, counter-terrorism, and counter-narcotics, all of which may involve military operations in urban terrain/operations, close quarters battle, and other operations on the battlefield.

Major Contractors
- Pistol: SIG SAUER Inc. – Newington, New Hampshire
- Ammunition: Olin-Winchester – East Alton, Illinois

Activity
- The Army's Program Executive Office Soldier released the final solicitation for the MHS to industry on August 28, 2015.
- The Army conducted bid sample testing from February 16 through June 22, 2016. This testing included initial ballistic characterization of candidate ammunition.
  - The program's acquisition strategy, as reflected in its request for proposal (RFP), allowed the Army to select up to three vendors based on bid sample testing to continue into PVT.
  - Vendors submitted nine proposal submissions. The Army selected the 9 mm MHS submission from SIG SAUER, which is a variant of their P320, and awarded a production contract to SIG SAUER on January 19, 2017.
- Glock filed a protest with the Government Accountability Office (GAO) on February 24, 2017.
  - Glock challenged the Army's interpretation of the solicitation regarding the minimum number of contract awards required by the RFP.
  - The GAO denied the challenge, finding that the RFP allowed the Army to make one award in June 2017.
- The Army entered into PVT in April 2017 for both the XM17 full-size variant and XM18 compact variant MHS pistols. This testing consisted of developmental testing, LFT&E, a fixed stand accuracy assessment, and a shooter-in-the-loop accuracy assessment.
- During drop testing in which an empty primed cartridge was inserted, the striker struck the primer causing a discharge. The Army directed SIG SAUER to develop an ECP to correct this deficiency. SIG SAUER modified the trigger mechanism to eliminate this deficiency. Subsequent testing validated that this ECP corrected the deficiency and the pistol no longer fired when dropped. The MHS with this ECP modification was submitted as the production-representative pistol for PVT, LFT&E, and IOT&E.
- During PVT testing with the ball ammunition, both MHS variant pistols would occasionally experience double ejections in which it would eject unspent ammunition along with the spent ammunition. The frequency of this occurrence increased as more rounds were fired through the pistol. The program manager created a team to determine the root cause of this failure.
- Several reliability stoppages were observed with both the XM17 and XM18 when shooting ball ammunition. The ball ammunition was not included in the IOT&E because of the demonstrated reliability problems during PVT and the ongoing root cause analysis.
- The Army conducted IOT&E for the XM17 and XM18 with shooters for all Services firing special purpose munition from August 14 through September 22, 2017, at Fort Bragg, North Carolina, in accordance with the DOT&E-approved test plan.
- The Army received a Conditional Materiel Release for the XM17 and XM18 with both the special purpose munition and the ball ammunition in November 2017. The 101st Airborne Division is the first unit scheduled to receive the pistol.
- The Army completed live fire testing that consisted of firing the ball and special purpose rounds into ballistic gelatin and through realistic battlefield barriers of interest for ball cartridges. The Army will combine the results of this testing with the results of "shooter-in-the-loop" accuracy testing to model MHS lethality.
- The Army intends to have a Full-Rate Production decision in September 2018. DOT&E intends to submit a combined IOT&E and LFT&E report in 2QFY18.

Assessment
- The MHS met its accuracy requirement that 10 shots at 35 meters can be covered by a 4-inch disk, with the center of the grouping being no more than 4 inches from the point of aim, 90 percent of the time. This was an entrance criterion for the IOT&E.
- During PVT, the XM17 and XM18 were tested for MRBF and MRBS with special purpose munition and with ball ammunition with testing out to the required service life of 25,000 rounds per pistol. The MRBF reliability requirement

is 5,000 MRBF for a 98 percent probability of completing a 96-hour mission without a failure. The MRBS reliability requirement is 2,000 MRBS for a 95 percent probability of completing a 96-hour mission without a stoppage.
- During PVT, the XM17 and XM18, with special purpose munition, met its requirement for both MRBF and MRBS:
  - The XM17 demonstrated 8,929 MRBF (99 percent probability)
  - The XM18 demonstrated 8,333 MRBF (99 percent probability)
  - The XM17 demonstrated 1,923 MRBS (95 percent probability)
  - The XM18 demonstrated 2,155 MRBS (96 percent probability)
- During PVT, the XM17 with ball ammunition met its requirement for MRBF but not its requirement for MRBS. The XM18 with ball ammunition did not meet its MRBF or MRBS requirement.
  - The XM17 demonstrated 6,944 MRBF (99 percent probability)
  - The XM18 demonstrated 3,906 MRBF (98 percent probability)
  - The XM17 demonstrated 343 MRBS (75 percent probability)
  - The XM18 demonstrated 197 MRBS (61 percent probability)
- The IOT&E was conducted only with the special purpose munition. The ball ammunition was not included due to the PVT reliability problems and the initiation of an engineering team to determine root cause analysis.
- During IOT&E, the Army observed 120 stoppages for XM17 and 85 stoppages for XM18. Operators were able to rapidly recover by performing immediate action drills without any additional maintenance or support. The stoppages had minimal operational impact on the operators' ability to fire and continue the mission. The assessment of operational suitability is ongoing.
- Preliminary data from the IOT&E indicate that the XM17 and XM18 met the MRBF reliability requirement of 5,000 MRBF and a 95 percent probability of completing a 96-hour mission without a failure. Neither weapon met the MRBS reliability requirement of 2,000 MRBS and a 95 percent probability of completing a 96-hour mission without a stoppage.
  - The XM17 demonstrated 38,247 MRBF (99 percent probability).
  - The XM18 demonstrated 9,501 MRBF (99 percent probability).
  - The XM17 demonstrated 336 MRBS (74 percent probability).
  - The XM18 demonstrated 229 MRBS (65 percent probability).
- The predominant cause of stoppages was the failure of the slide to lock (FSLR) after the firing of the last round in the magazine (60 of 120 stoppages for the XM17 and 63 of 85 stoppages for the XM18). The purpose of the slide locking to the rear is to inform the operator that the last round has been expended, and that the operator needs to reload a magazine into the weapon. Operators who are trained in pistol qualification, as taught by the Army marksmanship unit, utilize what is known as a high pistol grip. This grip places the non-dominant hand along the pistol slide on top of the slide catch lever. Many operators stated that the placement of the slide catch lever caused them to engage it while firing the pistol, which resulted in the slide not locking to the rear when the last round was expended in a magazine. Sixty percent of all FSLR stoppages (75 of 123) were experienced by 8 shooters out of the 132 who participated in the IOT&E. The Army marksmanship unit experts stated that this is an insignificant problem that can be mitigated with training and experience with the weapon. The MRBS demonstrated during IOT&E is significantly increased if this stoppage is eliminated:
  - The XM17 demonstrated 708 MRBS (87 percent probability).
  - The XM18 demonstrated 950 MRBS (90 percent probability).
- There were two trigger splintering hardware deficiencies observed during the IOT&E. Preliminary analysis indicates that this may be correlated with the ECP developed by SIG SAUER to correct the deficiency of the pistol firing when dropped with the safety not engaged.
- The assessment of LFT&E results is ongoing.

Recommendations
- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendations. The Army should:
  1. Upon identification of the root cause of the double ejections and ball ammunition relability problems, confirm fixes to both the XM17 and XM18 in future testing.
  2. Work with the vendor to identify and eliminate cause of variability in the manufacture of the trigger group mechanism.
  3. Consider redesign of the slide catch lever or operator training changes to prevent engagement by operators while shooting the pistol.

Navy Programs

Navy Programs

Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI) for AN/BQQ-10(V) Sonar

Executive Summary

- The Navy conducted FOT&E on the Advanced Processing Build 2013 (APB-13) variant of the AN/BQQ-10 Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI) sonar system in FY17. Testing included in-lab comparison testing between the APB-11 and APB-13 variants and at-sea testing of anti-submarine warfare (ASW) search capability of APB-13 against a U.S. submarine acting as a high-end threat nuclear submarine. Analysis is in progress; however, preliminary analysis shows an improvement from APB-11 in operator detection and classification times of presented submarine acoustic data.
- The Navy scheduled the remaining FOT&E event, evaluation of APB-13 capability to support situational awareness in an environment with a large number of contacts. Poor weather and submarine availability prevented the test event three times in FY17. This test is deferred to FY18 and will be conducted as part of APB-15 testing.
- DOT&E will submit a classified FOT&E report in FY18.

System

- The AN/BQQ-10 A-RCI sonar system is the undersea sensing system utilized by U.S. submarines. It uses active and passive sonar to conduct ASW and submerged operations in the execution of all assigned submarine missions. Acoustic energy is processed and displayed to enable operators to detect, classify, localize, and track threat submarines and other waterborne objects (surface ships, mines, bottom features, etc.).
- The AN/BQQ-10 A-RCI sonar system is an open-architecture system that includes biennial software upgrades (APBs) and complementary biennial hardware upgrades (Technical Insertions (TIs)). These upgrades are intended to maintain an advantage in acoustic detection of threat submarines.
- TIs normally support a preceding and subsequent APB (e.g., TI-12 would normally support both APB-11 and APB-13 software builds). Due to FY13 sequestration funding limitations, no TI-12/APB-13 systems were released. APB-13 was limited to platforms that completed an upgrade to TI-14. Furthermore, almost all TI-14 platforms will upgrade to APB-15 upon its release in FY18.

- The AN/BQQ-10 A-RCI sonar system consists of:
  - Interface to submarine acoustic sensors to include the spherical array or large aperture bow array, hull array, wide aperture array, conformal array, high-frequency array, and two towed arrays (i.e., the fat-line array consisting of the TB-16 or TB-34, and the thin-line array consisting of the TB-23, TB-29A, or TB-29A Reduced Length)
  - Processing capability that utilizes environmental data (e.g., water depth, bottom contour, sound velocity profiles, etc.) and received acoustic energy on all acoustic sensors and displays the processed data in a way that supports operator search, detection, classification, and localization/track of contacts of concern or contacts of interest

Mission

The Operational Commander will employ submarines equipped with the AN/BQQ-10 A-RCI sonar system to:

- Search for, detect, and track submarine and surface vessels in open-ocean and littoral sea environments
- Search for, detect, and avoid mines and other submerged objects
- Covertly conduct intelligence, surveillance, and reconnaissance
- Covertly conduct Naval Special Warfare missions
- Perform under-ice operations

Major Contractor

Lockheed Martin Maritime Systems and Sensors – Manassas, Virginia

Activity

- In July 2016, the Navy completed two phases of cybersecurity test and evaluation of the APB-13 variant of the AN/BQQ-10 A-RCI sonar system in accordance with a DOT&E-approved test plan. Specifically, the Navy completed a Cooperative Vulnerability and Penetration Assessment (CVPA) and an Adversarial Assessment (AA).
- In December 2016, DOT&E approved a Test and Evaluation Master Plan (TEMP) covering the APB-13 variant of the

AN/BQQ-10 A-RCI sonar system. The Navy has since completed the following operational testing of the system in accordance with the DOT&E-approved TEMP and DOT&E-approved test plans.
  - In December 2016, the Navy completed in-lab comparison testing between variants APB-11 and APB-13 using 60 real-world sonar recordings of non-U.S. submarines. Sonar recordings were played on each variant using 20 fleet operators to assess operator detection and classification metrics. The Navy conducted this test event as combined developmental and operational testing.
  - In January 2017, the Navy completed four days of open-ocean ASW search in the Southern California Operating Areas against a U.S. submarine acting as a high-end threat nuclear submarine. Data were collected to assess the capability of APB-13 to support detection through engagement of a high-end threat nuclear submarine.
- In January, July, and September 2017, the Navy scheduled a 2-day evaluation of APB-13 capability to support situational awareness in an environment with a large number of contacts, but all events were canceled due to poor weather, test submarine unplanned maintenance, or test submarine assignment to a higher fleet priority. The Navy was unsuccessful in rescheduling this test in FY17. This test is deferred to FY18 and will be conducted as part of APB-15 testing.
- In September 2017, the Navy completed its test strategy and test design development for operational test of APB-15 of the AN/BQQ-10 A-RCI sonar system. The Navy expects to submit the APB-15 TEMP for approval in early FY18. APB-15 operational testing includes at-sea evaluations focusing on ASW and situational awareness in high-density contact management situations, in-lab comparison testing between APB-13 and APB-15, and in-port evaluation of cybersecurity.
- Navy efforts to obtain high-end, diesel electric submarine target services to test APB-13 capabilities were unsuccessful in FY17. The Navy is pursuing the Rim of the Pacific Exercise (RIMPAC 2018) and Diesel Electric Submarine Initiative (DESI) exercises as opportunities to obtain high-end, diesel electric submarine target services to test APB-15 capability in FY18.

Assessment

- Cybersecurity testing identified system vulnerabilities that could negatively affect the system's operational effectiveness. DOT&E will identify specific vulnerabilities in a classified FOT&E report in FY18. The Navy is updating the system to correct the identified vulnerabilities starting with TI-14/APB-15 system updates and continuing into future TI and APB developments.
- In-lab comparison testing between APB-11 and APB-13 showed improvement in operator detection and classification times for presented non-U.S. submarine acoustic data. The operational impact of these improvements cannot be quantified because the scenarios utilized recorded data and therefore did not allow in-situ tactical response (i.e. test and target platforms maneuvers could not be modified) during the playback periods.
- The at-sea ASW search event showed no degradation in performance from APB-11. Due to the significantly different environments in which the APB-11 and APB-13 variants were tested, DOT&E cannot make a confident determination of improvement between variants. DOT&E will provide details of observed performance and test limitations in a classified FOT&E report in FY18.
- The Navy generates and approves the requirements documents and TEMPs in parallel with APB development and installation due to the biennial software and quadrennial hardware development cycle. As a result, the fleet assumes additional risk, since most operational testing is not completed before the system is initially deployed.

Recommendations

- Status of Previous Recommendations. The Navy made progress in addressing four of five recommendations outlined in DOT&E's classified FOT&E report on APB-11, dated November 12, 2015. Six significant recommendations remain outstanding from previous DOT&E reports. The significant unclassified recommendations are:
  1. Re-evaluate the use of the current time difference between system and operator detection times as the ASW Key Performance Parameter for a more mission-oriented metric to accurately characterize system effectiveness.
  2. Evaluate the covertness of the high-frequency sonar during a future submarine-on-submarine test.
  3. Determine the performance of the AN/BQQ-10 A-RCI sonar system in detecting near-surface mines.
  4. Perform an ASW event against a high-end, diesel-electric, hunter-killer submarine at a periodicity of at least every other APB variant (i.e., APB-11 and again in APB-15) of the AN/BQQ-10 A-RCI sonar system and upon introduction of new wet end sensor or software capabilities improving ASW mission capability.
- FY17 Recommendations. None.

Aegis Modernization Program

Executive Summary

- The Navy is modernizing the Aegis Weapon System (AWS) on Aegis guided missile cruisers and destroyers via Advanced Capability Build (ACB)-12 and ACB-16 baseline upgrades.
  - ACB-12 Baseline 9.A0 upgrades Baseline 3 *Ticonderoga* (CG 47)-class cruisers.
  - ACB-12 Baseline 9.C1 upgrades Flight I *Arleigh Burke* (DDG 51)-class destroyers.
  - ACB-12 Baseline 9.C1 will also be equipped on new construction Flight IIA DDG 51 destroyers, beginning with USS *John Finn* (DDG 113).
  - ACB-16 Baseline 9.C2 upgrades will be installed on Flight IIA DDG 51 destroyers and Baseline 8 and Service Life Extension Program CG 47 cruisers.
- The Navy conducted a subset of planned Baseline 9.A0 operational testing in FY15 and FY16; the remaining test events have not been scheduled. The Navy began Baseline 9.C1 operational testing in FY16 and continued testing through FY17.
- To date, the live area air defense flight test events on Baselines 9.A0 and 9.C1 suggest that area air defense performance against single subsonic and supersonic high-diving targets remains consistent with historical performance against comparable threats. DOT&E intends to issue a final report on Baselines 9.A0 and 9.C1 in FY18.
- To adequately assess the Probability of Raid Annihilation requirement for the self-defense mission for Flight III DDG 51 destroyers/ACB-20, the Navy must provide an accredited modeling and simulation (M&S) suite of the Aegis Combat System (ACS) and an Aegis-equipped Self-Defense Test Ship (SDTS) where the ship's full self-defense kill chain can be tested.
- The SECDEF directed in FY16 and reiterated in FY17 that the Navy fund long-lead items for an Aegis SDTS to be used for testing Aegis ACB-20, DDG 51 Flight III, the Air and Missile Defense Radar (AMDR, a.k.a. AN/SPY-6), and Evolved Seasparrow Missile (ESSM) Block II; the Navy initially complied with the direction but subsequently removed all funding for the Aegis SDTS and the required aerial targets.
- Navy Integrated Fire Control – Counter Air (NIFC-CA) From-the-Sea (FTS) Increment I became a fielded capability in 2015 and was fully integrated as a tactical option in fleet air defense. Future testing of ACB-16, ACB-20, and Standard Missile-6 (SM-6) will evaluate the NIFC-CA FTS Increment II capability.
- The Navy's Aegis Baseline 9.A0 and Aegis Ashore installation (Baseline 9.B) cybersecurity testing identified deficiencies, which are classified. The nature of these deficiencies is such that they could pose significant operational risk in a cyber-contested environment. The implementation of fixes to previous problems is not anticipated until ACB-16; therefore, the Navy and DOT&E canceled cybersecurity testing of Baseline 9.C1, which will instead take place during ACB-16 operational testing.

System

- The Navy's Aegis Modernization program provides updated technology and systems for CG 47-class Aegis guided missile cruisers and DDG 51-class Aegis guided missile destroyers. This planned, phased program provides similar technology and systems for new construction destroyers.
- The AWS integrates the following components:
  - AWS AN/SPY-1 three-dimensional (range, altitude, and azimuth) multi-function radar
  - AN/SQQ-89 undersea warfare suite that includes the AN/SQS-53 sonar, SQR-19 passive towed sonar array (DDGs 51 through 78, CGs 52 through 73), and the SH-60B or MH-60R helicopter (Flight IIA DDGs 79 and newer have a hangar to allow the ship to carry and maintain its own helicopter)
  - Close-In Weapon System
  - A 5-inch diameter gun
  - Harpoon anti-ship cruise missiles (DDGs 51 through 78, CGs 52 through 73)
  - Vertical Launch System that can launch Tomahawk land attack missiles, Standard Missile 2 and 6 surface-to-air missile variants, ESSMs, and Vertical Launch Anti-Submarine Rocket missiles
- The AWS is upgraded through quadrennial ACBs. The Navy is upgrading the AWS to Baseline 9.A0 on CG 47 cruisers and to Baseline 9.C1 on Flight I and new construction DDG 51 destroyers. Baseline 9 will provide the following new capabilities:

  - Full SM-6 integration
  - Integrated Air and Missile Defense (IAMD), to include simultaneous air defense and ballistic missile defense missions on Aegis destroyers equipped with the new Multi-Mission Signal Processor
  - NIFC-CA FTS capability
- Starting with USS *John Finn* (DDG 113), new construction Aegis-guided missile destroyers will have Baseline 9 variants of AWS.

Mission

The Joint Force Commander/Strike Group Commander employs AWS-equipped DDG 51 guided missile destroyers and CG 47 guided missile cruisers to conduct:

- Area and self-defense anti-air warfare in defense of the Strike Group
- Anti-surface warfare and anti-submarine warfare
- Strike warfare, when armed with Tomahawk missiles
- IAMD, to include simultaneous offensive and defensive warfare operations
- Operations independently or in concert with Carrier or Expeditionary Strike Groups and with other joint or coalition partners

Major Contractors

- General Dynamics Marine Systems Bath Iron Works – Bath, Maine
- Huntington Ingalls Industries (formerly Northrop Grumman Shipbuilding) – Pascagoula, Mississippi
- Lockheed Martin Maritime Systems and Sensors – Moorestown, New Jersey

---

Activity

- The Navy conducted Baseline 9.A0 operational testing in FY15 and FY16, but weather and schedule constraints prevented execution of a majority of the planned events. Uncompleted events include a combined surface warfare and air defense firing scenario and a combined supersonic sea-skimming and subsonic sea-skimming anti-ship cruise missile (ASCM) raid. These events are scheduled for FY19. The Navy's Operational Test and Evaluation Force issued a report on Baseline 9.A0 in June 2017 with performance against supersonic sea-skimming ASCM unresolved. DOT&E will report on Baseline 9 operational testing in FY18.
- The Navy continued at-sea operational testing of Baseline 9.C1 on USS *Milius* in May 2017. Additional integrated testing for Baseline 9.C1 on a new construction DDG 51 destroyer was scheduled on USS *John Finn* in September 2017, but it was not successfully executed due to target failure and test ship system casualty.
- Operational testing on DDG 51 destroyers in FY17 included a demonstration of capability against a supersonic sea-skimming stream raid, manned aircraft tracking exercises, a demonstration of fixes implemented to address problems observed in a March 2016 test, and a maintenance demonstration.
- The Navy conducted all operational testing in accordance with DOT&E-approved test plans.
- Cybersecurity testing of Aegis Baseline 9.C1 has been canceled until ACB-16 Baseline 9.C2 operational testing.
- The Navy is developing an M&S suite that can supplement live testing and facilitate a more complete evaluation of air defense performance for DDG 51 Flight III ships in FY23. As part of the overall M&S development strategy, the Navy plans to make limited use of the M&S suite for operational testing of the ACB-16 (Baseline 9.C2) in FY18-22.
- The Navy is developing Test and Evaluation Master Plans (TEMPs) for Aegis ACB-16 (Baselines 9.A2 and 9.C2) and for DDG 51 Flight III/ACB-20 (Baseline 10). The Navy plans to conduct ACB-16 operational testing in FY18 with additional phases through FY22.

Assessment

- The Navy will not fully assess Aegis IAMD until an AWS M&S test bed is developed and validated. The test bed is under development and is planned to be available by FY20; however, there is no agreed upon strategy to validate the model to support assessment of the close-in self-defense battlespace. A limited Baseline 9.C1 IAMD operational assessment suggests that DDGs can simultaneously support limited air defense and ballistic missile defense missions within overall radar resource constraints. This assessment is supported by a single successful live firing event, managed by the Missile Defense Agency, which included simultaneous live firing of SM-2 and SM-3 missiles against threat-representative targets in an IAMD engagement.
- Early testing of Aegis Baselines 9.A0 and 9.C2 indicate that air defense performance against relatively benign presentations of ASCMs is consistent with historical performance. Operationally realistic presentations during recent operational testing demonstrated multiple challenges associated with defending against more stressing raids.
  - A 2017 test to verify correction of deficiency of problems observed in May 2016 found that the Navy successfully implemented corrective action, but the corrective action did not fully address operational performance concerns.
  - Aegis Baseline 9.C1 has incorporated software changes to address performance against certain stressing air defense threat presentations; however, these changes proved ineffective during developmental testing.
- Developmental testing of Baseline 9 against surface threats indicates that AWS does not fully meet the Navy's desired surface warfare performance levels.
- As appropriate, and until the full capability may be operationally tested, DOT&E will provide periodic operational

assessments to inform Navy and OSD leadership, as well as Congress, on the progress of T&E of the IAMD mission area.
- Until an Aegis-equipped SDTS is available for testing, it is not possible to characterize the self-defense capabilities of the Aegis cruisers and destroyers, and it is not possible to accredit an M&S suite to determine if the AWS satisfies its Probability of Raid Annihilation requirements.
- In February 2016, the SECDEF directed the Navy to acquire long-lead items needed for an Aegis and AMDR SDTS required for conducting adequate self-defense operational testing for DDG 51 Flight III, Aegis ACB-20, AMDR (also known as AN/SPY-6), and ESSM Block II. The Navy complied with this direction by budgeting for a single face of the AMDR to be procured. However, the Navy has not budgeted for the needed ACS or the test resources to support the self-defense operational testing for DDG 51 Flight III. Additionally, the SECDEF directed the Navy to update the Aegis/Flight III, AMDR, and ESSM TEMPs to include the Aegis SDTS and self-defense test events; the Navy has not complied with this direction. Subsequently, in FY17, the Navy removed all funding for the SDTS.
- The Navy's Aegis Baseline 9.A cybersecurity testing identified deficiencies, which are classified. The nature of these deficiencies is such that they could pose operational risk in a cyber-contested environment. Details can be found in DOT&E's Early Fielding Report dated July 2015. Subsequent to this report, follow-on cybersecurity testing of Aegis Ashore installation (Baseline 9.B) revealed similar problems. Therefore, the Navy and DOT&E canceled cybersecurity testing of Baseline 9.C1 and will evaluate implementation of fixes to previous problems as part of ACB-16 operational testing.
- During both integrated and operational testing events, the instability of the Aegis operator consoles adversely affected the conduct of test events. The Navy is addressing these problems and DOT&E intends to assess the Navy's efficacy in the final Baseline 9 report in FY18.

Recommendations
- Status of Previous Recommendations. The Navy has not addressed the following previous recommendations to:
  1. Continue to improve Aegis ships capability to counter high-speed surface threats in littoral waters.
  2. Synchronize future baseline operational testing and reporting with intended ship-deployment schedules to ensure that testing and reporting are completed prior to deployment.
  3. Provide the necessary funding to support the procurement of an advanced AMDR- and Aegis-equipped SDTS that is needed to support Aegis Modernization, advanced AMDR DDG 51 Flight III, and ESSM Block 2 operational testing.
  4. As soon as possible, produce an integrated test strategy for the DDG 51 Flight III, AMDR, Aegis Modernization, and ESSM Block 2 programs and capture that strategy in the TEMPs to be approved by DOT&E.
  5. Develop and deploy necessary cybersecurity corrective actions and verify correction with a follow-on operational cybersecurity test during ACB-16 operational testing.
  6. Complete the planned FOT&E events as detailed in the approved test plan as soon as is practical.
  7. Include planning for NIFC-CA FTS Increment II and NIFC-Collateral testing in future updates to the Aegis Modernization ACB-16 and ACB-20 and SM-6 TEMPs.
- FY17 Recommendations. The previous recommendations remain valid for FY17.

AGM-88E Advanced Anti-Radiation Guided Missile (AARGM) Program

Executive Summary

- The Navy completed testing, including some testing with the operational test agency, of the AGM-88E Advanced Anti-Radiation Guided Missile (AARGM) Block 1 in March 2017 and fielded the system in July 2017.
- AARGM Block 1 is a software-only upgrade addressing deferred capabilities and deficiencies discovered in FY12 during IOT&E.
- AARGM Block 1 software demonstrated some improved capabilities over the previous Block 0 software, but still demonstrated shortfalls in key areas of reliability and accuracy.
- Navy test squadrons VX-31 and VX-9 conducted Block 1 integrated testing beginning in 4QFY14 and ending after DOT&E rescinded test approval in 3QFY16. VX-31 and VX-9 continued limited testing of Block 1 as a developmental test assist in order to characterize the system.
- In FY17, VX-31 completed the final three of eight live fire test events. Of the eight live fire events, six were successful engagements and two were unsuccessful because the missiles did not impact anything of tactical significance. The analysis of the two unsuccessful events revealed classified deficiencies.
- AARGM Block 1 is not operationally suitable, having failed to satisfy two Capability Production Document (CPD)-defined reliability requirements in addition to demonstrating a decline in reliability compared to Block 0.
- Testing during the period was not adequate to provide an evaluation of operational effectiveness or survivability.
- Cybersecurity testing was conducted in accordance with the approved test plan but the test strategy proved ineffective for assessing AARGM's survivability against cyber-attacks. The Navy released Block 1 software in July 2017 without completing operational testing and without adequately addressing the performance and software stability problems discovered during Block 1 testing.
- The AARGM Extended Range (ER) variant is currently based on Block 1 software capabilities, which will require additional work to correct the accuracy, reliability, and software deficiencies to be effective against advanced threats.

System

- The Navy designed AARGM to improve the effectiveness of the legacy AGM-88B/C High-Speed Anti Radiation Missile (HARM) against fixed and relocatable radar and communication sites, particularly those that shut down in order to counter anti-radiation missiles.
- The seeker is optimized to passively detect and guide on radio frequency emissions from a radar site then transition to an active Millimeter Wave terminal radar to detect and track air defense unit elements.

- AARGM incorporates digital Anti-Radiation Homing, a GPS, Millimeter Wave guidance, and a Weapon Impact Assessment transmitter.
  - Anti-Radiation Homing improvements include an increased field of view and increased detection range compared to HARM.
  - The GPS allows position accuracy in location and time.
  - The Weapons Impact Assessment capability allows transmission of a real-time hit assessment via a national broadcast data system.
  - The Millimeter Wave radar technology allows target discrimination and guidance during the terminal flight phase.
  - The weapon uses an internal GPS and Inertial Navigation System with mission planning data to establish Missile Impact Zones and Missile Avoidance Zones in an effort to reduce fratricide.
- The Navy employs AARGM on all variants of the F/A-18 aircraft.
- The Navy intended for AARGM Block 1 to deliver Full Operational Capability, including Block 0 capability improvements and software changes to provide deferred capabilities and address deficiencies identified during IOT&E.

Mission

Commanders are intended to use AARGM-equipped aircraft to conduct pre-planned, on-call, and time-sensitive reactive anti-radiation targeting in order to suppress, degrade, and destroy radio frequency-enabled surface-to-air missile defense systems regardless of whether the systems continue radiating or shut down.

Major Contractor

Orbital/Alliant Techsystems – Northridge, California

Activity

- In June 2015, DOT&E approved the AARGM FOT&E test plan developed by the Program Office and the Navy's Operational Test and Evaluation Force (OPTEVFOR). The test plan was adequate to address the testing of deferred capabilities and deficiencies discovered during developmental test and IOT&E.
- In January 2016, DOT&E issued a memorandum describing problems with AARGM's performance (in particular, Guidance/Navigation Computer anomalies), poor reliability, and multiple software stability problems during integrated testing. In June 2016, DOT&E rescinded approval of the AARGM FOT&E Test Plan because the Navy had taken no significant actions to address these concerns and because integrated testing revealed additional problems.
- At a Gate 6 review, conducted August 2, 2016, the Navy decided to continue test and evaluation as a developmental test assist in order to field Block 1 software. OPTEVFOR and DOT&E attended all remaining test events to observe system performance.
- Navy test squadrons VX-31 and VX-9 completed test items from the Integrated Evaluation Framework as a developmental test assist from 3QFY16 to 2QFY17 at Naval Air Weapons Station China Lake, California, and Naval Base Ventura County, Point Mugu, California.
- The program developed and delivered software versions R2.1, R2.2, R2.2.1, R2.2.2, and R2.2.3 to address some of the deficiencies discovered during testing. R2.2.3 is the current version of Block 1 software but was only evaluated for 24.00 hours of the 234.09 hour test.
- In total, the AARGM Block 1 FOT&E and developmental test assist periods consisted of 32 sorties and 234.09 flight hours consisting of 222 captive carry runs and 8 live fire events.
- In FY17, VX-31 completed the final three of eight live fire test events. Of the eight live fire events, six were successful engagements and two were unsuccessful because the missiles did not impact anything of tactical significance. The analysis of the two unsuccessful events revealed classified deficiencies.
- The test team and OPTEVFOR observed 12 system of systems operational mission failures (OMFs) during 234.09 flight hours, resulting in a system of systems reliability of 19.50 hours Mean Time Between Operational Mission Failures (MTBOMF). This did not satisfy the CPD-defined requirement of greater than or equal to 28.00 hours.
- The test team and OPTEVFOR observed 7 OMFs during 234.09 flight hours, resulting in a system under test reliability of 33.40 hours MTBOMF. This did not satisfy the CPD-defined requirement of greater than or equal to 72.00 hours.
- OPTEVFOR did not conduct vulnerability scanning or penetration testing. The cybersecurity data consist of subject matter opinion and exploration of possibilities, with very little actual operational testing. The remaining cybersecurity test points were limited to interviews with AARGM operators and maintainers.
- In June 2017, OPTEVOR released a letter of observation providing operationally relevant observations of AARGM Block 1 performance during the FOT&E and developmental test assist periods. In July 2017, the Navy fielded Block 1 software and began retrofitting Block 1 software into all Block 0 AARGM.
- The Navy is negotiating a contract with Orbital/Alliant Techsystems to address the overall system reliability shortfalls.
- The Navy's FY16 budget included funding for an AARGM-ER variant that utilizes the existing guidance system and warhead of the AGM-88E with a solid integrated rocket motor to increase range. Development funding will last until 2020.
- In FY17, the Navy contracted with Orbital/Alliant Techsystems to identify near-term risks associated with the thermal protection properties of the current nose cone and seeker design if the rocket motor were redesigned to extend missile range. Results are expected in early FY18.

Assessment

- The operational testing of AARGM Block 1 was adequate to support an evaluation of operational suitability but was not adequate to support an evaluation of operational effectiveness or survivability.
- The Navy evaluated the current version of Block 1 software for only 24.0 hours of the 234.09 hour test. This led to a lack of operationally relevant data to make conclusions on effectiveness and survivability with an acceptable level of statistical confidence.
- AARGM Block 1 software demonstrated improved capabilities over the previous Block 0 software version but also demonstrated effectiveness shortfalls in key capabilities of reliability and accuracy. The details of the improvements and deficiencies are discussed in the classified "AGM-88E Advanced Anti-Radiation Guided Missile FOT&E Report," released in September 2017.
- Detailed analysis of the two live fire failures is classified, but the failures do affect weapon accuracy and performance. The Program Office made adjustments to correct the problems but did not verify the effectiveness of the corrections with additional live fire events before fielding Block 1. Based on known guidance logic, AARGM will likely be ineffective against advanced surface-to-air missile threat systems, particularly in an Anti-Access and Area Denial (A2AD) environment.
- AARGM Block 1 is not operationally suitable. AARGM Block 1 did not satisfy two CPD-defined reliability requirements. AARGM Block 1 demonstrated a slight decline in reliability compared to Block 0, which failed to satisfy reliability requirements during IOT&E but was suitable with a Verification of Correction of Deficiencies period in FY12. The operational effects of poor reliability are decreased availability of training missiles for fleet users and increased maintenance man-hours troubleshooting the missile and associated aircraft systems.

- The Navy attempted to streamline the AARGM Block 1 FOT&E test design by conducting developmental and operational testing simultaneously in a prolonged integrated test phase. There was no dedicated developmental testing designed into the original test plan. In retrospect and for future AARGM-ER testing, a dedicated developmental test phase is recommended for a weapon system software upgrade of this magnitude. This allows for a dedicated period of problem discovery and correction to take place prior to beginning operational testing with an operationally representative configuration.
- Cybersecurity testing was inadequate to assess AARGM survivability against cyber-attacks.
- The Navy released Block 1 software in July 2017 without completing operational testing and without adequately addressing performance and software stability problems discovered during Block 1 testing.
- Block 1 performance provides limited employment capability against advanced threat surface-to-air radar systems. AARGM-ER will use Block 1 software, which will require additional work to correct the accuracy, reliability, and software deficiencies to be effective against advanced threats.

Recommendations

- Status of Previous Recommendations. The Navy still needs to address the following previous recommendations:
  1. Submit an updated operational test plan for DOT&E approval to correct the accuracy, reliability, and software deficiencies discovered during previous Block 1 testing prior to fleet release.
  2. Assess current and future Navy and Marine Corps doctrine to counter advanced threat surface-to-air missile systems, particularly in an A2AD environment, taking into account the classified problems discovered during previous testing.
  3. Improve seeker performance against advanced threat surface-to-air radar systems prior to investing time, money, and resources in extending the current system's range in an AGM-88E AARGM ER concept.
- FY17 Recommendations. The Navy should:
  1. Conduct dedicated developmental testing prior to further operational testing to ensure the operational test asset performance is stable and is production representative.
  2. Conduct a cybersecurity Adversarial Assessment of AARGM and supporting systems, including AARGM employment from weapons storage and loading, mission planning, and aircraft employment.

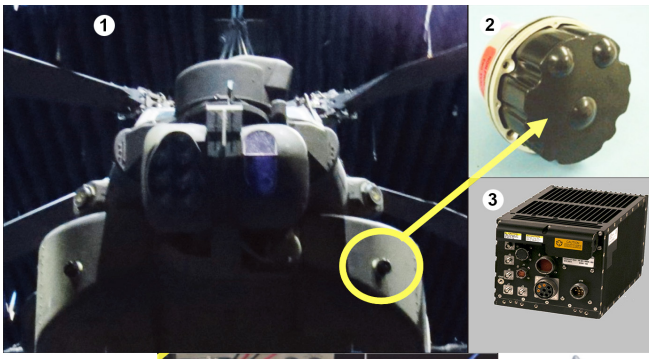
AN/APR-39D(V)2 Radar Signal Detection Set (RSDS)

Executive Summary

- The Army's operational assessment (OA) and FOT&E test results indicate that the Army has resolved the deficiencies from the legacy AN/APR-39 family (A(V)1, A(V)4, and C(V)1) of Radar Warning Receivers (RWRs) on the AH-64 by using the AN/APR-39D(V)2 Radar Signal Detection Set (RSDS).
- Test results show the AN/APR-39D(V)2 as installed on the Army's AH 64D/E platform has an initial Mean Time Between Operational Mission Failures (MTBOMF) of 22.2 hours during the OA and 18.4 hours during the FOT&E. Both are well below the mission-based requirement of 81 hours.

System

- The AN/APR-39D(V)2 is a digital upgrade to the AN/APR-39 family of analog RWRs used by nearly all DOD rotorcraft.
- The AN/APR-39D(V)2 RSDS consists of the following:
  - Four new dual-polarized E- through M-band (high band) antennas, and a C- though D-band (low band) direction of arrival antenna.
  - New quadrant receivers (two to four per aircraft). Each receiver has two channels that can accept signals from two E- through M-band antennas.
  - A new radar data processor with two wideband digital receivers.
  - A crystal video receiver processor and a Quad Core i7-based processor.
- The system uses either a separate display unit or integrates with the onboard aircraft displays to visually and aurally alert the pilots to active threat radars.
- For Navy aircraft, the system also acts as the electronic warfare bus controller.



1 - AH-64 Antenna Installation
2 - High Band Quadrant Antenna
3 - DV2 Processor
4 - Quadrant Receiver
5 - Low Band Directional Antenna

- The lead Army aircraft is the AH-64 D/E and the lead Navy aircraft is the MV-22B.

Mission

Commanders employ units equipped with the AN/APR-39D(V)2 RSDS to improve the mission survivability of Navy and Army aircraft by identifying radio frequency signals from threat surface-to-air missiles, airborne interceptors, and anti-aircraft artillery through cockpit alerts.

Major Contractor

Northrop Grumman – Rolling Meadows, Illinois

Activity

- The Army completed a developmental test period (DT-2) at the Electronic Combat Range (ECR), China Lake, California, in October 2016.
- The Army completed an OA at the ECR in November 2016.
- The Navy completed three Risk Reduction Data Collection flights on the KC-130T at the ECR in November 2016.
- DOT&E approved the Navy's Test and Evaluation Master Plan (TEMP), which included Army test activities and resources, in February 2017.
- The Navy completed a developmental test of cybersecurity from March 14-16, 2017, at the Electronic Combat Simulation and Evaluation Laboratory (ECSEL) at Point Mugu, California.
- The Army completed FOT&E at the ECR in July 2017. However, cybersecurity testing and the maintenance demonstration were not attempted and will not begin until 2QFY18.
- All testing was completed in accordance with a DOT&E-approved test plan.
- An FOT&E report will be released after completion of the maintenance demonstration and cybersecurity testing.
- The Army has planned a fielding decision in 4QFY18.

Assessment

- The Army demonstrated in laboratory and open-air testing that the AN/APR-39D(V)2, as installed on the AH-64 (D/E) aircraft, resolved all the Army's legacy APR-39 deficiencies.
- By combining the Army's DT-2 and OA suitability data, the Army demonstrated an MTBOMF of 22.2 hours for the AH-64D/E. Preliminary results show the MTBOMF

during the FOT&E was 18.4 hours. Both are well below the mission-based derived requirement of 81 hours for the AH 64E.

Recommendations

- Status of Previous Recommendations. The Army and Navy satisfactorily addressed three of the four FY16 recommendations. They still need to plan and fly additional KC-130T and AH-64 flights to accumulate more operational flight hours to better determine system reliability.
- FY17 Recommendation.
  1. The Army and Navy should plan and fly additional KC-130T and AH-64 flights to accumulate more operational flight hours to better determine system reliability.

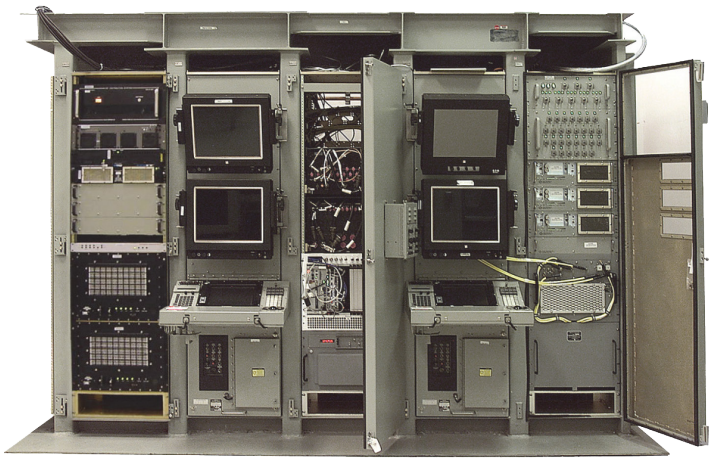
AN/BLQ-10 Submarine Electronic Warfare Support System

Executive Summary

- In August 2017, DOT&E issued a classified report on FOT&E completed in FY16 and concluded that the AN/BLQ-10 system with the Technical Insertion 10 (TI-10) upgrade improves the system's intercept capability against communications signals. The test was adequate to determine the system's operational effectiveness but not its operational suitability. DOT&E's assessment is discussed in the classified report.
- DOT&E removed the AN/BLQ-10 program from oversight in FY17.

System

- The AN/BLQ-10 system is an electronic warfare support system for U.S. submarines. It is intended to provide automatic intercept capability (detection, classification, localization, and identification) for both radar and communications signals.
- The AN/BLQ-10 uses multiple subsystems to process signals collected with the submarine's masts. Radar signals are collected by the imaging mast, which is either a photonics mast (on the *Virginia* class) or a periscope (on all other classes). Communications signals are collected from both the imaging mast and a dedicated communications intercept mast, which is either an AN/BRD-7 (on the *Los Angeles* and *Seawolf* classes), an AN/BSD-2 (on the *Virginia* class), or a Multifunction Modular Mast (MMM) (recently fielded on some *Los Angeles*- and *Virginia*-class ships). These masts provide largely the same functionality but with different frequency coverage and localization accuracy.
- The AN/BLQ-10 provides support for specialized, carry-on electronic warfare equipment and personnel.
- The program has adopted an open architecture, incremental development process. Hardware and software updates, referred to as TIs, are fielded every 2 years.
  - TI-08 was the first such upgrade, which added a subsystem to intercept some Low Probability of Intercept (LPI) radar signals.
  - TI-10 has been fielded. It consists of updates to commercial off-the-shelf (COTS) processors and displays, as well as upgrades of the Radar Narrowband to improve reliability and maintainability, improvement of the collection process, and an upgrade for the Improved Communications Acquisition and Direction Finding (ICADF) system.



  - TI-12 has been fielded on 688I SSN *Los Angeles*-class submarines. It brings new and more powerful servers; adds some TI-10 capabilities to this class of submarines; and connects directly to the submarine's combat system enclave guard, thus standardizing the cybersecurity process.
  - The first TI-14 modernization installations will be completed late FY17 into early FY18, with the first deployment in FY18. TI-14 will be installed on 688I SSNs and new construction *Virginia*-class submarines. It consists of updates to COTS processors and displays, and Electronic Warfare Server First Generation, which provides the Electronic Support System operator and platform decision-makers with improved tactical situational awareness.

Mission

Submarine Commanders use the AN/BLQ-10 electronic warfare support system to provide threat warning information to avoid counter-detection and collision, and to conduct intelligence, surveillance, and reconnaissance in support of fleet or battlegroup objectives.

Major Contractor

Lockheed Martin Mission Systems and Training – Syracuse, New York

Activity

- The Navy completed FOT&E in FY16. The FOT&E was conducted in accordance with a DOT&E-approved test plan.
- In June 2017, the Navy's Operational Test and Evaluation Force published a classified FOT&E report on the AN/BLQ-10 system with the TI-10 upgrade and the MMM.
- In August 2017, DOT&E published a classified FOT&E report on the AN/BLQ-10 system.
- DOT&E removed the AN/BLQ-10 program from oversight in FY17.
- The Navy is conducting ongoing land-based tests with TI-14 and other improvements at the Naval Undersea Warfare Center (NUWC) in Newport, Rhode Island, and at Lockheed Martin's facility in Syracuse, New York. The Navy intends to conduct an at-sea test in December 2017.

Assessment

- The FOT&E of the AN/BLQ-10 with TI-10 was adequate to determine the system's operational effectiveness but not its operational suitability.
- The TI-10 upgrade improves the previous version of the system (TI-08) by increasing the system's ability to intercept communication signals.
- The complete operational effectiveness assessment is discussed in DOT&E's classified FOT&E report.
- DOT&E could not fully assess the operational suitability of AN/BLQ-10 with TI-10. The FOT&E was insufficient to evaluate the Navy's training program and AN/BLQ-10 hardware reliability. Nonetheless, operational testing revealed AN/BLQ-10 training and software reliability problems that should be corrected.

Recommendations

- Status of Previous Recommendations. The Navy has addressed all previous recommendations.
- FY17 Recommendations. The Navy should:
  1. Improve software reliability.
  2. Conduct follow-on operational testing to assess AN/BLQ-10 hardware reliability and the Navy's training program. The complete list of recommendations is addressed in DOT&E's classified FOT&E report.

AN/SQQ-89A(V)15 Integrated Undersea Warfare (USW) Combat System Suite

Executive Summary

- In December 2014, DOT&E submitted a classified Early Fielding Report on the Advanced Capability Build 2011 (ACB-11) variant of the AN/SQQ-89A(V)15 Integrated Undersea Warfare (USW) Combat System Suite due to the installation of the ACB-11 variant on ships that deployed prior to IOT&E. From the data collected, DOT&E concluded the system demonstrated some capability to detect submarines and incoming U.S. torpedoes in deep water.
- Operational testing of the ACB-11 variant is expected to conclude in FY18. The final test event, a cybersecurity evaluation, was scheduled three times in FY17, but the tests were deferred because the test platforms were not available due to operational commitments or unplanned maintenance requirements. DOT&E will submit a classified FOT&E report in FY18 upon completion of the system's cybersecurity evaluation.

System

- The AN/SQQ-89A(V)15 is an integrated USW combat system that is deployed on *Ticonderoga*-class cruisers and *Arleigh Burke*-class destroyers. It is composed of the sensors, processors, displays, and weapons controls to detect, classify, localize, and engage threat submarines and alert on threat torpedoes. It is an open-architecture system that includes staggered biennial software upgrades (ACBs) and biennial hardware upgrades (Technical Insertions).
  - Acoustic sensors include a hull-mounted array, Multi-Function Towed Array (MFTA) TB-37 (including a towed acoustic intercept component), calibrated reference hydrophones, helicopter, and/or ship-deployed sonobuoys.
  - Functional segments process and display active, passive, and environmental data.
- The AN/SQQ-89A(V)15 interfaces with the Aegis Combat System to prosecute threat submarines using MK 46 and MK 54 torpedoes from surface vessel torpedo tubes, Vertical Launch Anti-Submarine Rockets, or MH 60R helicopters.

- The Navy intends to improve sensor display integration and automation, reduce false alerts, and improve onboard training capability to better support operations within littoral regions against multiple sub-surface threats.

Mission

- Theater and Unit Commanders use surface combatants equipped with the AN/SQQ-89A(V)15 to locate, monitor, and engage threat submarines.
- Maritime Component Commanders employ surface combatants equipped with the AN/SQQ-89A(V)15 as escorts to high-value units to protect against threat submarines during transit. Commanders also use the system to conduct area clearance and defense, barrier operations, and anti-submarine warfare (ASW) support during amphibious assault.

Major Contractor

Lockheed Martin Mission Systems and Training – Manassas, Virginia

Activity

- In December 2014, DOT&E submitted a classified Early Fielding Report for the ACB-11 variant of the AN/SQQ-89A(V)15 Integrated USW Combat System Suite. The report was submitted due to the installation of the ACB-11 variant on ships that deployed prior to IOT&E.
- In September 2015, the Navy completed a formal study that identified capability gaps in currently available torpedo surrogates and presented an analysis of alternatives that highlighted specific investments necessary to improve threat emulation capabilities. The Navy has since taken the following actions to address the identified capability gaps:
  - The Navy received funding through an FY16 Resource Enhancement Project (REP) proposal and is currently developing a threat-representative, high-speed quiet propulsion system.

  - The Navy submitted an FY17 REP proposal to develop a General Threat Torpedo (GTT) to further develop the aforementioned propulsion system by accurately representing threat torpedoes in both acoustic performance and tactical logic. The GTT project was recently funded and incorporates the remaining development and test of the threat-representative, high-speed quiet propulsion system project.
- The Navy's Operational Test and Evaluation Force (OPTEVFOR) continued IOT&E on the ACB-11 variant in March 2016. Testing was conducted in accordance with a DOT&E-approved test plan and included ASW transit search and area search operations using AN/SQQ-89A(V)15 onboard an *Arleigh Burke*-class destroyer. OPTEVFOR conducted testing in conjunction with an Aegis Baseline 9C operational test event at the Pacific Missile Range Facility, Barking Sands, Hawaii. The testing focused on ACB-11's capability to support submarine search in shallow water.
- The remaining ACB-11 operational testing involves an evaluation of the system's cybersecurity effectiveness. The Navy scheduled the cybersecurity evaluation three times in FY17, but all events were deferred due to test platform operational commitments or maintenance requirements. Testing is expected to occur in FY18.
- In December 2017, DOT&E approved the ACB-13 Test and Evaluation Master Plan (TEMP).

Assessment

- The final assessment of AN/SQQ-89A(V)15 variant ACB-11 is not complete, as testing will continue into FY18. DOT&E will provide a classified IOT&E final report in FY18, following the cybersecurity test event. The report will include an assessment of all test limitations. Preliminary results from the DOT&E classified Early Fielding Report and additional analysis conducted in FY17 showed the following:
  - The ACB-11 variant demonstrated the capability to detect and localize submarines in deep water, but demonstrated limited capability to translate a submarine detection to a prosecution.
  - The ACB-11 variant does not meet the Navy's performance metrics for torpedo detection as assessed against U.S. exercise torpedoes. The Navy is incorporating system modifications in ACB-15 that are intended to improve torpedo detection capability. ACB-13 was determined to be too far in its development process to incorporate these modifications.
  - The ACB-11 variant is currently not suitable due to low operational availability. The system's software reliability is sufficient, but significant delays repairing the MFTA and MFTA handling gear resulted in extended periods of limited system capability. The MFTA system requires continued supervision to ensure that the Navy's availability improvement plan remains on track. MFTA is the dominant sensor for submarine detection and torpedo alertment.
  - No assessment can be made against operationally relevant midget and coastal diesel submarine threats because the Navy does not have any test surrogates that accurately represent these platforms.
  - Preliminary analysis of in-water data collected subsequent to the DOT&E Early Fielding Report of FY16 indicates that ACB-11 has the capability to detect and classify a U.S. submarine in shallow water and supports *Arleigh Burke*-class destroyers' capability to translate this detection into an ASW prosecution using its organic assets.
- A representative threat torpedo surrogate is needed to adequately assess future AN/SQQ-89A(V)15 variants. GTT development will address many DOT&E concerns, but the GTT capability to support operational testing depends on future Navy decisions to procure a sufficient quantity of GTTs. Additionally, the GTT depends upon the successful development of the high-speed quiet propulsion system that has been significantly delayed due to performance problems and cost overruns.

Recommendations

- Status of Previous Recommendations. The Navy has made some progress on prior recommendations. However, the Navy should still:
  1. Develop and integrate high-fidelity trainers and realistic in-water test articles to improve training and proficiency of operators in ASW search and track of threat submarines, including midget and coastal diesel submarines.
  2. Revisit system requirements to ensure that funded improvement in subsequent ACBs supports Navy objectives for ASW against current and future threat submarines.
  3. Schedule and complete dedicated IOT&E to assess cybersecurity vulnerabilities.
  4. Complete development of the threat-representative, high-speed quiet propulsion system and acquire sufficient GTTs to support evaluation of the next ACB that has modifications affecting torpedo recognition capability (detection and/or classification).
  5. Address two additional classified recommendations listed in the December 2014 Early Fielding Report.
- FY17 Recommendations. None.

Assault Amphibious Vehicle Survivability Upgrade (AAV-SU)

Executive Summary

- The Assault Amphibious Vehicle Survivability Upgrade (AAV-SU) program conducted LFT&E from April 2016 to June 2017 and an operational assessment (OA) from April to June 2017.
- The Engineering and Manufacturing Development (EMD) Phase LFT&E focused on a limited number of specification compliance shots and demonstrated that AAV-SU meets its force protection requirements.
- The AAV-SU-equipped test unit successfully completed seven of eight mission profiles during the OA, demonstrating adequate capability in both desert and littoral environments to include entering and exiting the USS *San Diego* (LPD 22), an amphibious transport dock ship. In some cases, vehicle failures and transmission problems reduced combat power and caused delays during mission execution. In the unsuccessful mission profile, a sufficient number of vehicles could not be repaired in time to start the mission.
- Data from the OA indicate that reliability remains a problem for the AAV-SU. The AAV-SU's Mean Time Between Operational Mission Failures (MTBOMF) was 10.7 hours during the OA, as compared to the 14.2 hours demonstrated in developmental testing and the 25-hour user requirement.

System

- The AAV family of vehicles is the U.S. Marine Corps' principal amphibious lift system and armored personnel carrier. It is designed to provide combat support, armor protected firepower, and mobility for a reinforced rifle squad and associated combat equipment for operations on land or at sea.
- After-action reports from Operation Iraqi Freedom highlighted AAV shortfalls in survivability against explosive threats such as landmines and IEDs. These shortfalls limited the employment of AAVs in Iraq after 2007 and precluded employment in Afghanistan.
- The marines intend for the AAV-SU program to improve force protection against ballistic and underbelly explosive threats and maintain land and water mobility performance.
  - The survivability upgrades include new external armor, an added spall liner, underbelly protection, lower sidewall protection, integrated blast-mitigating seats, and improved fuel tanks.
  - The performance upgrades account for the added weight due to survivability upgrades and include improvements to the powertrain and suspension in order to maintain or increase the vehicle's land and water mobility performance compared to the current vehicle, the AAV Reliability, Availability, Maintainability/Rebuild to Standard (AAV RAM/RS).
- Initial Operational Capability for the AAV-SU is planned for FY19. The Marine Corps intends the AAV-SU to reach Full Operational Capability in FY23 and it must be sustained until at least 2035. The Marine Corps will field AAV-SU vehicles to each of its two active-component Assault Amphibian Battalions, the Combat Assault Battalion, 3rd Marine Division, and the Combat Assault Company, 3rd Marine Regiment. Additional vehicles will be utilized for training, testing, and supporting the maintenance cycle.

Mission

- Commanders employ Assault Amphibian Battalions to provide task-organized forces to transport assault elements, equipment, and supplies ashore; execute ship-to-shore, shore-to-shore, and riverine operations; support breaching of barriers and obstacles; and provide embarked infantry with armor protected firepower, communication assets, and mobility.
- AAV-SU-equipped units support surface power projection and forcible entry against a defended littoral region.

Major Contractor

SAIC – McLean, Virginia

Activity

- The U.S. Army Aberdeen Test Center conducted EMD Phase LFT&E for the AAV-SU from April 2016 to June 2017 at Aberdeen Proving Ground, Maryland, in accordance with DOT&E-approved test plans. LFT&E was adequate to support an evaluation of the AAV-SU force protection requirements:
  - System-level live fire testing characterized the AAV-SU force protection against two underbody mines, one undertrack mine, and one side IED event.
  - Ballistic exploitation testing of the AAV-SU characterized the abilities of unique features on the AAV-SU (e.g., gaps, seams, and unique geometries) to provide protection against ballistic threats.
- The Marine Corps Operational Test and Evaluation Activity (MCOTEA) conducted a pre-Milestone C OA from April 12 through June 14, 2017, and a Cooperative Vulnerability and Penetration Assessment (CVPA) at the Marine Corps Air Ground Combat Center, Twentynine Palms, California, and Marine Corps Base Camp Pendleton, California, in accordance with the DOT&E-approved test plan. The OA was adequate to support an evaluation of the AAV-SU.

Assessment

- The AAV-SU-equipped test unit successfully completed seven of eight mission profiles during the OA and was able to shoot, move, and communicate in order to close with and destroy the enemy in both desert and littoral environments.
  - The test unit demonstrated sufficient cross-country mobility and was able to operate with an M1A1 tank section during a desert mission profile.
  - During littoral operations, the AAV-SU-equipped test unit was able to enter and exit LPD 22 (an amphibious transport dock ship), operate in the ocean, and cross the surf zone.
  - Data from the OA indicate that reliability remains a problem for the AAV-SU. The AAV-SU entered the OA with less-than-required reliability observed during developmental testing. AAV-SU's MTBOMF was 10.7 hours in the OA, as compared to the 14.2 hours demonstrated in developmental testing, the 25-hour growth curve prediction, and the 25-hour user requirement. The revised reliability growth strategy is optimistic and does not reach the required MTBOMF by the IOT&E scheduled for 2QFY19.
  - The vehicle transmission was the source of three move-related problems:
    - When the AAV-SU's tracks are used for water propulsion, the crew can operate in this mode for just a short time before the transmission overheats – a problem that manifested itself when the water jets malfunctioned.
    - When coming ashore, AAV crews engage tracks prior to entering the surf zone providing both water jets and tracks for propulsion. The AAV-SU transmission requires the driver to slow the engine speed to idle before shifting, causing a pause during a critical sea-to-shore transition and creating a period of vulnerability during a contested beach landing.
    - The transmission has a hydraulic braking system that is used to slow or stop the vehicle. This transmission braking system has a safety feature that automatically brakes the vehicle in the event of certain automotive problems. If the driver manually applies the brakes after the system brakes itself automatically, all hydraulic pressure will be lost, and the brakes will lock. This results in a time-consuming and difficult process to unlock the brakes and requires one of the crew to be exposed outside the hull of the vehicle to gain access to a lever that is pumped in order to restore pressure to the system.
  - The AAV-SU accommodated 17 marines in cramped conditions despite some omitted equipment and supplies. The effects were:
    - The embarked troop commander could not egress through the AAV-SU troop compartment, as is done with the AAV RAM/RS, because of reduced clearance between his position and the troop compartment. Instead, he had to exit through the top-side hatch and climb down from the top of the vehicle on an exposed, narrow ladder, which caused him to lose contact with his personnel at a critical point.
    - Egress time, or the amount of time needed for the embarked infantry to exit the vehicle tactically, is prescribed by the user to be 18 seconds for the reinforced rifle squad loads. The AAV-SU combined (day and night) median egress time was 29 seconds, which exceeded the user requirement and was 11 seconds slower than the median value demonstrated for the AAV RAM/RS during the OA.
  - The CVPA investigated the ability to disrupt communications and exploit the controller area network (CAN) bus and the vendor's maintenance laptop. The CVPA verified that the CAN bus was isolated from the network, thereby preventing an outsider from exploiting this vehicle component network. The cyber test team found no outsider vulnerabilities. Details of cybersecurity vulnerabilities are discussed in the classified appendix to DOT&E's October 2017 OA report.
- LFT&E characterized vulnerabilities to operationally realistic direct and indirect fire threats that the AAV-SU is expected to encounter in combat . This included a number of specification compliance shots that demonstrated that AAV-SU meets its force protection requirements.
- The AAV-SU meets its force protection requirements for underbody threats.
  - A vulnerability in the initial AAV-SU design was discovered during the first underbody mine event. The contractor implemented fixes to correct this vulnerability. The test of the design modifications demonstrated adequate protection.
- A vulnerability was discovered during the side IED event. The program addressed this vulnerability, and the AAV-SU will be

retested against this threat during Full-Up System-Level live fire testing in the Production and Deployment (PD) phase.
- The bow armor will require additional testing in the PD phase to characterize its level of protection.

Recommendations
- Status of Previous Recommendations. The Marine Corps is working to ensure that enough test assets (e.g., armor coupons) are allocated for the appropriate phases of test for both the AAV-SU and Amphibious Combat Vehicle 1.1 programs.
- FY17 Recommendations. The following is a summary of key recommendations. A complete list of recommendations is contained in DOT&E's OA report dated October 2017.
  1. Reduce the troop capacity threshold and modify the vehicle troop compartment to allow a combat-configured marine to egress through the vehicle's troop compartment; allow more space for embarked marines; store required crew-served weapons, supplies, ammunition, and equipment; and improve egress times.
  2. Revise the reliability growth strategy to reflect the lower than projected reliability during EMD phase developmental and operational testing.
  3. Modify the vehicle or develop operational procedures to allow the crew to transition from water jets to track operations when coming ashore without a delay; prevent automatic locking of brakes when the driver inadvertently presses the brake pedal after the vehicle automatically brakes itself; allow the crew to restore brake/transmission pressure from within the vehicle; and support water track operations without the transmission overheating.

CH-53K - Heavy Lift Replacement Program

Executive Summary

- The Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted its operational assessment (OA) of the CH-53K at Sikorsky's West Palm Beach, Florida, facility and completed it on October 19, 2016.
- DOT&E published its "CH-53K Heavy Lift Replacement Program" OA and LFT&E report in February 2017 to support the Defense Acquisition Board CH-53K Milestone C decision.
- The OA indicated that the CH-53K has the capability to support the Amphibious Pre-Assault/Raid Operations mission, the aircraft's most stressing mission profile.
- The CH-53K demonstrated 84.8 percent mission reliability during testing up through the OA, which is greater than the required value of approximately 83 percent at that point in its projected reliability growth.
- The Defense Acquisition Executive approved the CH-53K program's Milestone C and entry into low-rate initial production (LRIP) on February 28, 2017.
- Flight testing continues, using the four Engineering Development Model (EDM) aircraft and the Ground Test Vehicle (GTV). The four EDM aircraft have flown 552.6 flight hours as of September 30, 2017. Delivery of the first of six system development test article (SDTA) aircraft is imminent. SDTA aircraft will join the test program leading to IOT&E, which will use the SDTAs.
- After completion of the fourth SDTA in West Palm Beach, final assembly of the last two SDTAs and LRIP aircraft will relocate to the Sikorsky facility in Stratford, Connecticut. All future CH-53Ks, including full-rate production aircraft, will be completed at that facility.
- The CH-53K design is not finalized. Sikorsky is working on but has not yet resolved multiple problems discovered during testing. These include airspeed indication anomalies, main rotor gearbox low reliability, hot gas impingement on aircraft structures, tail boom and tail rotor structural problems, main rotor dampers overheating, fuel system anomalies, high temperatures in the #2 engine bay, and hot gas ingestion by the #2 engine reducing available power.
- Live fire testing against the threshold threats is not complete. The Navy's analysis of data available to date indicates that the CH-53K may not meet the Survivability Key Performance Parameter (KPP) without mitigations, which the Navy is investigating. Navy analysis indicates that the CH-53K is more survivable than the legacy CH-53E aircraft.

System

- The CH-53K is a new-build, fly-by-wire, dual-piloted, three-engine, heavy lift helicopter slated to replace the aging CH-53E. The CH-53K is designed to carry 27,000 pounds of useful payload (three times the CH-53E payload) over a distance of up to 110 nautical miles, climbing from sea level at 103 degrees Fahrenheit to 3,000 feet above mean sea level at 91.5 degrees Fahrenheit.
- The greater lift capability is facilitated by increased engine power (7,500 shaft horsepower versus 4,380 horsepower per engine in the CH-53E) and a composite airframe. The composite airframe is lighter than the CH-53E metal airframe.
- The CH-53K design incorporates the following survivability enhancements:
  - Large Aircraft Infrared Countermeasures with the advanced threat warning sensors (combines infrared, laser, and hostile fire functions into a single system), an AN/APR-39D(V)2 radar warning receiver, and an AN/ALE-47 countermeasure dispensing system
  - Pilot armored seats, cabin armor for the floor and sidewalls, fuel tank inerting, self-sealing fuel bladders, and 30-minute run-dry capable gear boxes
- The Navy intends the CH-53K to maintain a shipboard logistics footprint equivalent to that of the CH-53E.

Mission

Commanders employ the Marine Air-Ground Task Force equipped with the CH-53K for:

- Heavy lift missions, including assault transport of weapons, equipment, supplies, and troops
- Supporting forward arming and refueling points and rapid ground refueling
- Assault support in evacuation and maritime special operations
- Casualty evacuation
- Recovery of downed aircraft, equipment, and personnel
- Airborne control for assault support

Major Contractor

Sikorsky Aircraft, a Lockheed Martin Company – Stratford, Connecticut (subsidiary company since 2015)

Activity

- The first OA using Marine Corps pilots and ground personnel completed all ground and flight events in accordance with a DOT&E-approved test plan at the Sikorsky facility in West Palm Beach, Florida, concluding on October 19, 2016.
- In February 2017, DOT&E published its "CH-53K Heavy Lift Replacement Program" OA and LFT&E report to support the Defense Acquisition Board CH-53K Milestone C decision.
- The Defense Acquisition Executive approved the CH-53K program's Milestone C and entry into LRIP on February 28, 2017.
- The program has four EDM aircraft which continue to support integrated developmental and operational flight testing. All four EDM aircraft have been flying in the integrated test program since EDM-4 achieved first flight on August 31, 2016. The four EDM aircraft have flown 552.6 flight hours as of September 30, 2017.
- The Navy is using a Ground Test Vehicle (GTV) to qualify key dynamic components; assess aircraft stresses, vibrations, and rotor performance; and support long-term reliability testing and verification of aircraft systems performance. The GTV is a complete CH-53K that is fully representative of the EDM aircraft. The Navy is using the GTV to investigate fixes for aircraft technical problems and to provide a platform for aircrew training.
- The Navy will use the GTV for transportability demonstrations on a C-17 airlifter and as the test article for full-up system-level LFT&E projected for FY19.
- Sikorsky is manufacturing the first four of six SDTA aircraft at its facility in West Palm Beach, Florida, with delivery of the first SDTA projected for early FY18. SDTA aircraft will join the integrated test program and the SDTA aircraft will be used for IOT&E. The Program Office has incorporated retrofit periods into the master schedule to ensure these SDTA aircraft will be as production-representative as possible. Upon completion of the fourth SDTA aircraft, Sikorsky will transition final assembly of CH-53K aircraft to its Stratford, Connecticut, facility for the fifth and sixth SDTAs and LRIP aircraft. Full-rate production is planned for the Stratford plant.
- The Navy completed ballistic testing of four flight critical main and tail rotor system components in FY15 against a range of operationally relevant small arms threats under static loads representative of flight conditions. In FY17, the Navy completed post-ballistic endurance testing to assess residual flight capability for these components. The objective of this endurance testing is to evaluate the ability of these components to continue to function and thereby enable the aircraft to land before catastrophic component failure due to a ballistic event. Vendor reports on these endurance tests will be completed and sent to Sikorsky and Naval Air Systems Command (NAVAIR) for review. NAVAIR will then incorporate the post-endurance test results into a comprehensive live fire test report to be submitted to DOT&E in 2020.
- In 2QFY16, the failure of a test fixture at Naval Air Weapons Station China Lake, California, delayed the live fire testing of the horizontal tail rotor drive shaft system by 6 months. The Navy completed this testing in December 2016. The Navy completed subsequent testing of the tail rotor gearboxes and transmissions using the same fixture in May 2017.
- Live fire ballistic testing of the main and tail rotor servos was completed in October 2017 at the manufacturer's facility in the United Kingdom. Post-ballistic endurance testing to assess residual flight capability of these components is scheduled to begin in December 2017.
- The Navy is modifying aircraft survivability equipment (ASE) to address cybersecurity requirements (data at rest protection), mitigate obsolescence (removable media and computer processors), and reduce life-cycle cost (via elimination of components). The Navy is upgrading the infrared countermeasure subsystem and adding hostile fire indication.
- Due to ASE program delays, the Navy has deferred deployment and testing of the updated ASE and it will not be available for IOT&E. The Navy will use legacy ASE during IOT&E and will employ legacy ASE for Initial Operational Capability, which is projected for late 2019. The Navy intends to examine updated ASE in FOT&E and retrofit it to the fleet as it becomes available.
- The Program Office completed Revision C of the U.S. Marine Corps CH-53K Heavy-Lift Replacement Program Test and Evaluation Master Plan (TEMP) to reflect programmatic changes and updates to the cybersecurity test strategy for Milestone C. Revisions included new emphasis on cybersecurity including incorporation of a Cooperative Vulnerability and Penetration Assessment and an Adversarial Assessment. DOT&E approved Revision C of the TEMP on February 23, 2017.
- The Navy is continuing testing in accordance with the DOT&E-approved TEMP and a DOT&E-approved 2010 Alternative LFT&E plan.

Assessment

- The OA indicated that the CH-53K has the capability to support the Amphibious Pre-Assault/Raid Operations mission, the aircraft's most stressing mission profile.
- The CH-53K demonstrated 84.8 percent mission reliability during testing up through the OA, which is greater than the required value of approximately 83.0 percent at that point in its projected reliability growth.
- The original test flight schedule is 10 percent complete as of September 2017 and continues to slip due to technical problems discovered during testing.
- Pressure is increasing to meet a late December 2019 Initial Operational Capability (IOC), but current projections estimate that the planned 6-month IOT&E will have started 1 month prior to this desired IOC. Schedule compression has the potential to adversely affect training for the IOT&E aircrews and maintainers.
- Design of the CH-53K is not finalized. Sikorsky is working on but has not yet resolved problems discovered in developmental testing.

- The aircraft pitot-static system is giving unreliable airspeed indications in various flight regimes. Sikorsky is investigating relocating the pitot-static sensors but has not finalized a solution. The flight control computers receive airspeed inputs from the pitot-static system and airspeed is a vital input parameter for the algorithms used to aid control of the aircraft.
- Service life projections for the main rotor gearbox are falling short of the requirement. Sikorsky is pursuing solutions involving modification of internal gears and their interfaces.
- Engine #2 and auxiliary power unit hot gas impingement on the aircraft structure during some flight regimes has not been solved. On several test flights, telemetry indicated temperatures on the composite skin of the aircraft were approaching structural limits. This necessitated termination of some maneuvers to prevent aircraft damage.
- Testing has revealed anomalies in the CH-53K tail boom design. The tail structure has experienced unexpected vibrations and resonances, and redesign efforts are in progress to mitigate vibration-induced damage to hydraulic lines and other components in the tail.
- The tail rotor flex beam, which connects the tail rotor blade to the hub, has experienced material delamination and cracking. A redesign of the flex beam is in progress.
- Main rotor dampers are overheating. The contractor has proposed a new rotor damping configuration involving lower damping action, which has been installed on EDM-1. Sikorsky is gathering and analyzing flight test data, but evaluation of the change's effectiveness is not complete throughout the CH-53K flight envelope.
- Sikorsky has not finalized the fuel system configuration; the original design called for a suction-only fuel feed to reduce vulnerability to ballistic threats and the contractor has not identified a non-boost pump solution. If boost pumps are required, additional live fire testing may be required.
- The #2 engine bay is experiencing high temperatures that could jeopardize components in that bay. The contractor has not yet identified a permanent solution.
- Under certain wind conditions while hovering, the #2 engine ingests hot gasses from the #1 and/or #2 engine exhausts. This can reduce #2 engine available power, which could prevent lifting the 27,000-pound external load. This can be avoided by the pilot turning the helicopter if circumstances permit. The CH-53E experiences similar degradations under similar hover conditions.

- Live fire testing against the threshold threats is not complete. The Navy's analysis, incorporating the data available to date, indicates that the CH-53K is more survivable than the legacy CH-53E against small-arms, automatic weapons fire, and legacy man-portable air defense system threats. However, the CH-53K may not meet the CH-53K Survivability KPP without mitigations, which the Navy is investigating.
- Live fire testing against objective threats is not funded, but the Navy must complete this testing for an adequate survivability assessment against expected threats. Component tests for the main rotor assembly and tail rotor hub are also scheduled to occur after IOC as part of this Phase II testing. As a result, any deficiencies identified after IOC will need to be addressed later with engineering change proposals.

Recommendations

- Status of Previous Recommendations. The Navy has completed the FY15 recommendations. The Navy should continue to address the following FY16 recommendations.
  1. Finalize the CH-53K configuration while remediating problems identified in developmental testing.
  2. Continue testing and finalize the CH-53K design.
  3. Consider re-baselining the program to an event-based schedule instead of fixed calendar dates, thereby providing sufficient time for training and operational testing.
- FY17 Recommendations. The Navy should:
  1. Ensure live fire testing against objective threats is fully funded and accelerated to minimize the probability of problem discovery post-IOC, which would need to be addressed with engineering change proposals.
  2. Continue to investigate mitigations to improve CH-53K survivability.
  3. Address all recommendations in DOT&E's February 2017 OA and LFT&E report.

Coastal Battlefield Reconnaissance and Analysis (COBRA) System

Executive Summary

- The Coastal Battlefield Reconnaissance and Analysis (COBRA) Block I system completed the first of five periods of IOT&E using a DOT&E-approved test plan to evaluate the system's capability to detect and classify mine lines, minefields, and obstacles on the beach zone in daylight.
- COBRA Block I provides an operational capability for beach reconnaissance. The system did not meet the Block I Capability Production Document threshold requirements for one class of targets but provides marginal capability that is better than any existing beach reconnaissance capability.
- The Navy declared COBRA Block I Initial Operational Capability (IOC) in July 2017 based on IOT&E Period One and developmental testing.
- The Navy was not able to complete planned IOT&E periods in FY17 due to lack of an available Littoral Combat Ship (LCS) platform.

System

- The COBRA system is a mission payload on the MQ-8B Fire Scout unmanned air system (UAS), which can be embarked on an LCS or other air-capable ships. The COBRA system is a component of the mine countermeasures (MCM) mission package (MP) when employed from LCS.
- The COBRA program is using evolutionary acquisition and incremental development to meet overall mine and obstacle reconnaissance requirements.
  - Block I capability is intended to provide tactical reconnaissance for detection and location of unburied mine lines, minefields, and obstacles on the beach in daylight. The MQ-8B Fire Scout currently serves as the Block I sensor platform. The Navy declared Block I system IOC in July 2017.
  - Block II is intended to enhance the COBRA system sensor to provide daytime and nighttime detection and location of unburied mine lines, minefields, and obstacles in the beach and surf zones. The Navy expects Block II to reach IOC in FY22.
  - As currently envisioned, Block III will add the capability to detect buried mines in the beach and surf zones. The Block III IOC date has not yet been established.
- The COBRA Block I system consists of the COBRA Airborne Payload Subsystem (CAPS) and Post Mission Analysis (PMA) subsystem.
  - CAPS consists of a multi-spectral camera, installed on an MQ-8B Fire Scout as a modular payload. The system saves collected multi-spectral imagery of the target area to a Data Storage Unit (DSU) for post-mission analysis.

  - Upon aircraft recovery, the DSU is removed from CAPS and connected to the PMA subsystem. When the PMA operator has completed analysis of the data, the processed imagery is forwarded to the Mine Warfare (MIW) Environmental Decision Aids Library (MEDAL) for message formatting and further dissemination to the Mine Countermeasures Commander and other operational commanders via tactical data networks.
- The COBRA system is dependent on the UAS and shipboard systems to perform its mission.
  - Shipboard operators use the Tactical Common Data Link (TCDL) to communicate with CAPS from the MQ-8B Mission Control System (MCS) while the MQ-8B Fire Scout is in flight.
  - On LCS, MEDAL resides in the mission package application software (MPAS). The PMA subsystem and MPAS, in turn, reside on the mission package computing environment (MPCE), which provides operator control, computing, networking, and storage infrastructure.
- The COBRA system provides the sensing capability for Joint Direct Attack Munition (JDAM) Assault Breaching System (JABS), a component of the Assault Breaching System, which can be used to neutralize mines and obstacles on the beach prior to an amphibious assault. The COBRA system precision location capability supports JABS targeting or identification of clear lanes to bypass mines and obstacles.
- The COBRA system provides beach reconnaissance capability for the LCS Coastal Mine Reconnaissance Mission Module in the LCS MCM MP.

Mission

- The Joint Force Commander will use LCS units equipped with the COBRA Block I system as part of the MCM MP to conduct unmanned aerial tactical reconnaissance of potential landing sites for an amphibious assault.

- The Joint Force Commander will use LCS units equipped with the COBRA Block II system as part of the MCM MP to conduct daytime and nighttime unmanned aerial tactical reconnaissance of both beach and surf zones for potential landing sites for an amphibious assault.

Major Contractor
Areté Associates – Tucson, Arizona

Activity
- DOT&E approved a COBRA Block I Test and Evaluation Master Plan revision for IOT&E in May 2017.
- The COBRA Block I completed IOT&E Test Period One in accordance with a DOT&E-approved test plan. Fleet sailors operated the system from shore at NASA's test facility in Wallops Island, Virginia, in May 2017. The MQ-8B Fire Scout with the COBRA payload completed 21 missions to assess its performance against mine lines, mine fields, and obstacles emplaced on the nearby beach. After each flight, trained fleet operators completed post-mission analysis of the data.
- The Navy was unable to complete the remaining phases of IOT&E in FY17 as planned due to lack of an available LCS platform to complete testing.
- The Navy declared COBRA Block I IOC in July 2017 before completion of IOT&E based on the Navy's Operational Test and Evaluation Force (OPTEVFOR) quick look report on system performance during IOT&E Test Period One and the results of developmental testing.
- Depending on the availability of LCS platforms, the Navy plans to complete COBRA Block I IOT&E Test Period 2 by 2QFY18, which includes at-sea testing in Southern California. IOT&E Test Period 3 is a maintenance demonstration, which may be completed on LCS 2 after Test Period 2 if sufficient suitability data are not available from prior IOT&E periods. The Navy intends to complete IOT&E Test Period 4 in 4QFY18 and Test Period 5 in 1QFY19, which includes shore-based cybersecurity testing on LCS 2.

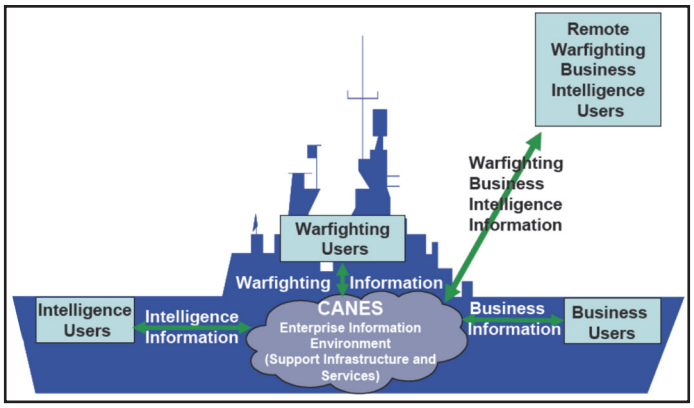
Assessment
- Test Period One of the COBRA Block I IOT&E provided the data to evaluate the search rate, percentage of targets (mine fields, mine lines, and obstacles) detected and classified, and the target location error rate.
- The Test Period One data were adequate to assess the effectiveness of the system to detect, classify, and localize mine lines, minefields, and obstacles on pure sand and on sand with beach vegetation.
- Test Period One data show that the COBRA Block I system performed reliably with relatively few operational mission failures of short duration. However, both MQ-8B Fire Scout test platforms were not operational for several days during this IOT&E period. MQ-8B troubleshooting and repairs required significant maintenance and technical support.
- Based on IOT&E Test Period One results, OPTEVFOR reported that the system is trending toward being operationally effective and suitable.
- COBRA Block I provides an operational capability for beach reconnaissance. The system did not meet the Block I Capability Production Document threshold requirements for one class of targets but provides marginal capability that is better than any existing beach reconnaissance capability.

Recommendations
- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendations. The Navy should:
  1. Complete the remaining periods of IOT&E, including LCS-based testing, cybersecurity testing, and the maintenance demonstration, if necessary.
  2. Fund and integrate the COBRA Block I system on a more robust and reliable platform to mitigate risks caused by poor MQ-8B Fire Scout operational reliability and availability observed during testing.
  3. Fund and develop the COBRA Block II system to provide nighttime and surf zone reconnaissance capability.

Consolidated Afloat Networks and Enterprise Services (CANES)

Executive Summary
- The Consolidated Afloat Networks and Enterprise Services (CANES) force-level variant is operationally effective and suitable, and not survivable in a cyber-contested environment, based on data from the FOT&E that ended in June 2017.
- USD(AT&L) approved full deployment of CANES on October 13, 2015, after DOT&E evaluated CANES for unit-level ships to be operationally effective, suitable, and survivable based on the data from the IOT&E.

System
- CANES is an enterprise information system consisting of computing hardware, software, and network services (e.g., phone, email, chat, video teleconferencing, web hosting, file transfer, computational resources, storage, and network configuration and monitoring). CANES is intended to replace legacy networks on ships, submarines, and shore sites.
- The CANES program mitigates hardware and software obsolescence on naval vessels and shore sites through the increased use of standard components and regularly scheduled hardware and software updates.
- The CANES network provides a single, consolidated physical network with logical sub-networks for Unclassified, Secret, Secret Releasable, and Top Secret security domains. It includes a cross-domain solution for information transfers across these security boundaries. This consolidation is intended to reduce the network infrastructure footprint on naval platforms and the associated logistics, sustainment, and training costs.
- CANES has three variants tailored to the employing platform: unit level for smaller ships such as destroyers and cruisers, force level for large deck ships such as aircraft carriers and large deck amphibious ships, and a submarine variant.



Mission
Naval Commanders and crews afloat and ashore use CANES to connect weapon systems, host applications, and share command and control, intelligence, and business information via chat, email, voice, and video in support of all naval and joint operations.

Major Contractors
- Northrop Grumman – Herndon, Virginia
- General Dynamics - Taunton, Massachusetts
- Serco – Reston, Virginia
- DRS Laurel Technologies – Johnstown, Pennsylvania

Activity
- The Navy's Operational Test and Evaluation Force (OPTEVFOR) completed the CANES force-level variant FOT&E in June 2017. The Navy could not execute the originally planned test schedule due to high-priority operational deployments of the designated test ships. As executed, the tests spanned from June 2015 to March 2017 on two different aircraft carriers. OPTEVFOR conducted the following events in support of the FOT&E:
  - A functional test onboard CVN 74 in August 2015.
  - A shortened Cooperative Vulnerability and Penetration Assessment (CVPA) on CVN 74 in December 2015 to identify and fix cybersecurity vulnerabilities before the ship deployed for an operational mission.
  - A second CVPA on the equipment brought onboard the CVN 74 by the air wing and destroyer squadron in June 2016.
  - The final CVPA onboard CVN 74 in November 2016, but the ship was not available for the follow-on Adversarial Assessment (AA). Normally, a cyber test team conducts a CVPA and waits until the Program Office and the user fix vulnerabilities discovered during the CVPA before conducting an AA. For this test, OPTEVFOR conducted the CVPA on CVN 74, but conducted the AA on CVN 71. The cyber test team conducted a short CVPA on CVN 71 prior to commencing the AA.

- OPTEVFOR did not conduct cybersecurity testing for the CANES Top Secret/Sensitive Compartmented Information (TS/SCI) enclave.
- As conducted, the FOT&E was adequate to evaluate operational effectiveness, operational suitability, and survivability pending cybersecurity testing of the TS/SCI enclave. DOT&E issued a report on the FOT&E on September 25, 2017.

Assessment

- The force-level CANES variant is operationally effective. CANES provides enterprise services, application hosting, network communications, and network management capabilities that support force-level missions.
- The force-level CANES variant is operationally suitable. CANES met reliability, availability, and maintainability requirements and received good usability scores. However, the Program Office should expand training and documentation to cover more topics such as monitoring the network, determining network status, assessing proposed configuration changes, and cybersecurity.
- The force-level CANES variant is not survivable. Cybersecurity vulnerabilities identified and fixed on CVN 74 still remained as vulnerabilities on CVN 71.
- The Navy does not assign a dedicated network manager on ships. A dedicated network manager with adequate cybersecurity training could monitor the network and provide the ship a means of detecting cybersecurity intrusions and taking appropriate actions.

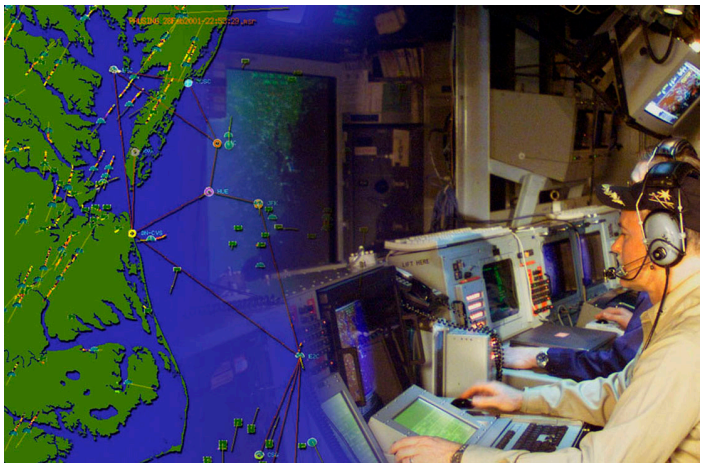
Recommendations

- Status of Previous Recommendations. There are no outstanding previous recommendations.
- FY17 Recommendations. The Navy should:
  1. Correct all deficiencies identified in the force-level FOT&E on all Navy ships.
  2. Assign dedicated network managers on all combatant ships and provide them with cybersecurity training.
  3. Conduct cybersecurity testing of the CANES TS/SCI enclave.

Cooperative Engagement Capability (CEC)

Executive Summary
- The Navy's Operational Test and Evaluation Force (OPTEVFOR) continued FOT&E of the Cooperative Engagement Capability (CEC) USG-2B with the Aegis Baseline 9.C1 Combat System in May 2017. Preliminary indications are that the CEC USG 2B, as integrated in the Aegis Baseline 9.C1 Combat Systems, remains operationally effective and suitable and continues to perform comparably to previous CEC USG-2 and USG-2A variants.
- DOT&E will provide assessments of the CEC USG-2B operational effectiveness and suitability in 2018.

System
- CEC is a real-time sensor-netting system that enables high-quality situational awareness and integrated fire control capability.
- There are four major U.S. Navy variants of CEC:
  - The USG-2/2A is used in selected Aegis cruisers and destroyers, *San Antonio* (LPD 17)-class and LHD amphibious ships, and *Nimitz* (CVN 68)-class aircraft carriers.
  - The USG-2B, an improved version of the USG-2/2A, is used in CVN 68 and *Gerald R. Ford* (CVN 78)-class aircraft carriers, *Zumwalt* (DDG 1000)-class destroyers, selected Aegis cruisers/destroyers, and selected amphibious assault ships.
  - The USG-3 is used in the E-2C Hawkeye 2000 aircraft.
  - The USG-3B is used in the E-2D Advanced Hawkeye aircraft.
- The two major hardware pieces are the Cooperative Engagement Processor, which collects and fuses sensor data, and the Data Distribution System, which exchanges data between participating CEC units.
- The CEC increases Naval Air Defense capabilities by integrating sensors and weapon assets into a single, integrated, real-time network that:



  - Expands the battlespace
  - Enhances situational awareness
  - Increases depth-of-fire
  - Enables longer intercept ranges
  - Improves decision and reaction times

Mission
Naval Commanders use units equipped with CEC to:
- Improve battle force air and missile defense capabilities by combining data from multiple battle force air search sensors on CEC-equipped units into a single, real-time, composite track picture.
- Provide accurate air and surface threat tracking data to ships equipped with the Ship Self-Defense System.

Major Contractor
Raytheon Integrated Defense Systems Co. – St. Petersburg, Florida

Activity
OPTEVFOR continued FOT&E of the CEC USG-2B with the Aegis Baseline 9.C1 Combat System in May 2017 in accordance with DOT&E-approved test plans. The FOT&E is expected to complete in mid-2018.

Assessment
- Preliminary CEC test results indicate that the CEC USG-2B, as integrated with the Aegis Baseline 9.C1 Combat System, remains operationally effective and suitable and continues to perform comparably to previous CEC USG-2 and CEC USG-2A variants. DOT&E will provide an assessment of the CEC USG-2B's operational effectiveness and suitability in 2018.

Recommendations
- Status of Previous Recommendations. The Navy has not satisfied the following previous recommendations to:
  1. Demonstrate corrections to the problem that degrades the USG-3B CEC's Track File Concurrence in a phase of FOT&E.
  2. Implement changes to the USG-3B CEC interface with the E-2D mission computer that would allow data from

the E-2D's APY-9 radar to be used by the USG-3B CEC without first requiring the creation of an E-2D Mission Computer track.

3. Correct the cause of the electromagnetic interference between the USG-3B CEC and the E-2D radar altimeter and demonstrate the corrections in a phase of FOT&E.
4. Take action on the recommendations contained in DOT&E's classified report to Congress on the CEC USG-3B FOT&E.
5. Update the CEC Test and Evaluation Master Plan to include details of:
   - FOT&E of corrections made to the CEC USG-3B
   - FOT&E of the CEC USG-2B with the Aegis Baseline 9.C Combat Systems
   - FOT&E of the CEC USG-2B with the DDG 1000 Combat System
   - FOT&E of the CEC USG-2B with the CVN 78 Combat System
   - FOT&E of USG-3B CEC to demonstrate the system's ability to support the E-2D's Theater Air and Missile Defense and Battle Force Command and Control missions
6. Investigate and correct the integration problems with legacy Aegis baseline combat systems operating in a CEC network and demonstrate the correction in a phase of FOT&E.

- FY17 Recommendations. None.

CVN 78 *Gerald R. Ford*-Class Nuclear Aircraft Carrier

Executive Summary

- The Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted a DOT&E-approved operational assessment from September 2015 through July 2017. The assessment was originally scheduled to end in mid-2016 after CVN 78 completed Builder's Sea Trials and Acceptance Trials, but the slip in CVN 78 delivery date led to a delay in the completion of the operational assessment. Testing is now complete.
- DOT&E's assessment of CVN 78 remains consistent with previous assessments. Poor or unknown reliability of the newly designed catapults, arresting gear, weapons elevators, and radar, which are all critical for flight operations, could affect the ability of CVN 78 to generate sorties, make the ship more vulnerable to attack, or create limitations during routine operations. The poor or unknown reliability of these critical subsystems is the most significant risk to CVN 78. Based on current reliability estimates, CVN 78 is unlikely to be able to conduct the type of high-intensity flight operations expected during wartime.
- CVN 78 is unlikely to achieve its Sortie Generation Rate (SGR) (number of aircraft sorties per day) requirement. The threshold requirement is based on unrealistic assumptions including fair weather and unlimited visibility, and that aircraft emergencies, failures of shipboard equipment, ship maneuvers, and manning shortfalls will not affect flight operations. DOT&E plans to assess CVN 78 performance during IOT&E by comparing it to the demonstrated performance of the *Nimitz*-class carriers as well as to the SGR requirement.
- The Navy previously identified an inability to readily electrically isolate Electromagnetic Aircraft Launching System (EMALS) and Advanced Arresting Gear (AAG) components to perform maintenance. This limitation will preclude some types of EMALS and AAG maintenance during flight operations, decreasing their operational availability.
- The Navy demonstrated, in developmental testing, corrections to previously discovered deficiencies. EMALS testing in 2015 discovered excessive airframe stress during launches of F/A-18E/F and EA-18G with wing-mounted 480-gallon external fuel tanks (EFTs). The Navy discovered similar problems with 330-gallon EFTs on the F/A-18A-D. Additionally, end-of-stroke dynamics with heavy wing stores were discovered for the F/A-18E/F and EA-18G, which would limit maximum launch speed. Preliminary developmental test results indicate that these problems are resolved.
- The Navy continued performance testing of the AAG at a jet car track site at Joint Base McGuire-Dix-Lakehurst, New Jersey. This testing examined the performance of the redesigned arresting gear to meet the system specifications. Runway Arrested Landing Site (RALS) testing with manned aircraft commenced in 2016 and completed over 350 aircraft arrestments as of August 2017. RALS testing supported development of the F/A-18E/F limited envelope Aircraft Recovery Bulletin required for the first arrestments onboard CVN 78, which were completed on July 28, 2017.

- The CVN 78 design is intended to reduce manning. The Navy analysis indicates the ship is sensitive to manpower fluctuations. Workload estimates for the many new technologies such as catapults, arresting gear, radar, and weapons and aircraft elevators are not well understood. Some of these concerns have required redesignation of some berthing areas and may require altering standard manpower strategies to achieve mission accomplishment. The CVN 78 berthing capacity is 4,660; this is more than 1,100 fewer than *Nimitz*-class carriers. Recent estimates of expected combined manning of CVN 78, its air wing, embarked staffs, and detachments range from 4,656 to 4,758. The estimates do not include Service Life Allowance for future crew growth. Consequently, CVN 78 is expected to be short of berthing spaces.
- The CVN 78 combat system for self-defense is derived from the combat system on current carriers and is expected to have similar capabilities and limitations. The program is integrating the ship's Dual Band Radar (DBR) with the combat system, which continues to undergo developmental testing. Testing has uncovered tracking, clutter/false track, track continuity, and engagement support problems affecting air traffic control and self-defense operations. The Navy is investigating solutions to these problems, but as the IOT&E approaches, the likelihood that these problems will persist into IOT&E increases.
- CVN 78 is exhibiting more significant electromagnetic compatibility problems than other Navy ships. The Navy is continuing to characterize the problems and develop

mitigation plans, but current restrictions and performance of various systems will limit CVN 78 operations.
- The development and testing of EMALS, AAG, DBR, and the Integrated Warfare System will continue to drive the *Gerald R. Ford* timeline as it progresses toward IOT&E.

System
- The CVN 78 *Gerald R. Ford*-class aircraft carrier program is a new class of nuclear-powered aircraft carriers. It has the same hull form as the CVN 68 *Nimitz* class, but many ship systems, including the nuclear plant and the flight deck, are new.
- The newly designed nuclear power plant is intended to operate at a reduced manning level that is 50 percent of a CVN 68-class ship and produces significantly more electricity. CVN 78 will incorporate EMALS (electromagnetic, instead of steam-powered catapult launchers) and AAG. CVN 78 also will have a smaller island with a DBR (phased-array radars, which replaces/combines several legacy radars used on current aircraft carriers and serves in air traffic control and ship self-defense).
- The Navy intends for the Integrated Warfare System to be adaptable to technology upgrades and varied missions throughout the ship's projected operating life, including increased self-defense capabilities compared to current aircraft carriers.
- In addition to the self-defense features (hard- and soft-kill), the ship has the following survivability features:
  - Improved protection for magazines and other vital spaces as well as the inclusion of shock-hardened systems/components intended to enhance survivability.
  - Installed and portable damage control, firefighting, and dewatering systems intended to support recoverability from peacetime shipboard fire and flooding casualties and from battle damage incurred during combat.
- The Navy redesigned weapons stowage, handling spaces, and elevators to reduce manning, increase safety, and increase throughput of weapons.
- CVN 78 has design features intended to enhance its ability to launch, recover, and service aircraft, such as a slightly larger flight deck, dedicated weapons handling areas, and an increased number of aircraft refueling stations. The Navy set the SGR requirement for CVN 78 embarked aircraft at 160 sorties per day (12-hour fly day) and to surge to 270 sorties per day (24 hour fly day) as compared to the CVN 68 *Nimitz*-class SGR of 120 sorties per day/240 sorties per 24-hour surge.
- The Consolidated Afloat Networks and Enterprise Services (CANES) program replaces five shipboard legacy network programs to provide a common computing environment for command, control, intelligence, and logistics.
- CVN 78 is intended to support the F-35 and future weapons systems over the expected 50-year ship lifespan. CVN 78 includes a new Heavy underway replenishment system that will transfer cargo loads of up to 12,000 pounds. This Heavy replenishment system is only installed on one supply ship, USNS *Arctic*, with no current plan for more.
- The Navy intends to achieve CVN 78 Initial Operational Capability in FY18 after successful completion of Post Shakedown Availability and Full Operational Capability in FY21 after successful completion of IOT&E and Type Commander certification.

Mission

Carrier Strike Group Commanders will use CVN 78 to:
- Conduct power projection and strike warfare missions using embarked aircraft
- Provide force and area protection
- Provide a sea base as both a command and control platform and an air-capable unit

Major Contractor

Huntington Ingalls Industries, Newport News Shipbuilding – Newport News, Virginia

---

Activity
- A TEMP 1610 revision is under development to address problems with the currently approved TEMP 1610, Revision B. The Program Office is in the process of refining the Post Delivery Test and Trials schedule to further integrate testing and to include the Full Ship Shock Trial (FSST).
- The Navy intends to conduct a live test to demonstrate the SGR with six consecutive 12-hour fly days followed by two consecutive 24-hour fly days. DOT&E concurs with this live test approach; however, the Navy plan for extrapolating the 8 days of live results to the 35-day design reference mission on which the SGR requirement is based is yet to be decided. OPTEVFOR is working with the Program Office to identify required upgrades for the Seabasing/Seastrike Aviation Model to perform this analysis.
- The ship was delivered May 31, 2017, and commissioned July 22, 2017. Slips in the delivery affected schedules for the FSST and the at-sea OT&E of CVN 78. The FSST is planned for late CY19, followed by CVN 78's first Planned Incremental Availability (PIA). The initial operational testing won't occur until after the first PIA. The Program Office is planning for two back-to-back phases of initial operational testing. The first phase examines basic ship functionality as the ship prepares for flight operations; the second phase focuses on flight operations once the ship and crew are ready. The Navy plans to start the first phase of operational testing in early FY21 and complete the second phase of operational testing in FY22, prior to the first deployment of CVN 78. To save resources and lower test costs, the test phases are aligned

with standard carrier training periods as CVN 78 prepares for its first deployment.

- The Navy continues to plan the CVN 78 shock trial for CY19. The Navy has held meetings regularly to discuss shock trial logistics, environmental requirements, instrumentation, and related analyses.

EMALS

- The Navy conducted four F/A-18F launches from CVN 78, the first at-sea EMALS aircraft launches.
- As of July 2017, the program has conducted 3,801 dead loads (non-aircraft, weight equivalent sled) and 523 aircraft launches at the land-based test site.
- EMALS testing in 2015 discovered excessive airframe stress during launches of F/A-18E/F and EA-18G with wing-mounted 480-gallon EFTs. The Navy discovered similar problems with 330-gallon EFTs on the F/A-18A-D. Additionally, end-of-stroke dynamics with heavy wing stores were discovered for the F/A-18E/F and EA-18G, which would limit maximum launch speed.

AAG

- The Navy conducted four F/A-18F arrestments on CVN 78, the first at-sea AAG arrestments.
- The Navy continues to test the AAG on a jet car track at Joint Base McGuire-Dix-Lakehurst, New Jersey. Earlier testing prompted system design changes that the program is now testing. The jet car track testing examined the F/A-18E/F performance envelope with the new design. Overall, land-based jet car track testing has accomplished a total of 1,598 dead load arrestments as of August 31, 2017. Testing at RALS supported development of the limited envelope Aircraft Recovery Bulletin needed for the first at-sea arrestments on CVN 78.

CANES

- The Navy completed the performance and suitability portions of the CANES follow-on operational testing of the force-level CANES configuration used on the *Nimitz* and *Ford* classes. The cybersecurity testing of this variant concluded in 3QFY17. The results of the cybersecurity test are classified and available separately.

DBR

- The radar consists of fixed array antennas both in the X- and S-bands. The X-band radar is the Multi-Function Radar (MFR) and the S-band radar is the Volume Search Radar (VSR).
- The Navy has tested a production array MFR and an Engineering Development Model array of the VSR at the Surface Combat System Center at Wallops Island, Virginia. Integration testing of DBR has concluded at Wallops Island and the program is in the process of installing the MFR on the Self-Defense Test Ship (SDTS) for further CVN 78 testing.
- Limited testing of the production DBR has begun on CVN 78 in the shipyard, in-port in Norfolk, Virginia, and at sea. The at-sea testing has been limited by problems with DBR reliability, uncommanded system resets, and problems with the radar's power supply onboard CVN 78.

Electric Plant

- Following a series of transformer and voltage regulator problems, which damaged two main turbine generators, the Navy decided to accept the ship with only three of the four main turbine generators operating after repairing only one of the two damaged generators. The ship is currently conducting underway testing in this configuration and the remaining damaged main turbine generator will need to be repaired or replaced during the ship's post-shakedown availability (PSA).

Manning

- CVN 78 has been manned in the shipyard and during initial at-sea periods, and the Navy is working with the ship's personnel to refine manpower, personnel, training, and education planning.

Electromagnetic Compatibility

- Preliminary electromagnetic interference (EMI) and radiation hazard (RADHAZ) testing has been conducted by Naval Surface Warfare Center, Dahlgren Division (NSWCDD) and Naval Air Systems Command (NAVAIR). Further testing and mitigation is planned both at sea and in port throughout shakedown and the post-shakedown availability (PSA).

Assessment

- The delays in the ship delivery have pushed both phases of initial operational testing until after the FY20 PIA period. As noted in previous annual reports, the CVN 78 test schedule has been aggressive, and the development and testing of EMALS, AAG, DBR, and the Integrated Warfare System are driving the ship's schedule independent of the requirement to conduct the FSST. The delay in the ship's delivery and development have added about 2 years to the timeline. Given all of the above, it is clear that the need to conduct the FSST has not been a factor delaying the ship's first deployment to FY22.
- CVN 78 has many new critical systems, such as EMALS, AAG, AWE, and DBR; since these systems have not undergone shock trials on other platforms, their ability to withstand shock is unknown. The program plans to complete component shock trials on EMALS, AAG, and the Advanced Weapons Elevators (AWE) during CY19, but because of a scarcity of systems, qualification testing of DBR is behind and will probably not be completed before the FSST.

Reliability

- CVN 78 includes several systems that are new to aircraft carriers; four of these systems stand out as being critical to flight operations: EMALS, AAG, DBR, and AWEs. Overall, the poor reliability demonstrated by AAG and EMALS and the uncertain reliability of DBR and AWEs pose the most significant risk to CVN 78 IOT&E. The Navy is testing all four of these systems for the first time in their shipboard configurations aboard CVN 78. Reliability estimates derived from test data for EMALS and AAG are discussed in the following subsections. For DBR and AWE, only engineering reliability estimates have been provided.

EMALS

- EMALS testing to date has demonstrated that EMALS should be able to launch aircraft planned for the CVN 78 air wing. However, the system demonstrated poor reliability during developmental testing suggesting operational difficulties lie ahead for meeting requirements and in achieving success in combat.
- In its current design, EMALS is unlikely to support high-intensity operations expected in combat. As of June 2017, the program estimates that EMALS has approximately 455 Mean Cycles Between Critical Failures (MCBCF) in the shipboard configuration, where a cycle represents the launch of one aircraft. While this estimate is above the rebaselined reliability growth curve, the rebaselined curve is well below the requirement of 4,166 MCBCF. At the current reliability, EMALS has a 9 percent chance of completing the 4-day surge and a 70 percent chance of completing a day of sustained operations as defined in the design reference mission without a critical failure.
- The reliability concerns are exacerbated by the fact that the crew cannot readily electrically isolate EMALS components during flight operations due to the shared nature of the Energy Storage Groups and Power Conversion Subsystem inverters onboard CVN 78. The process for electrically isolating equipment is time-consuming; spinning down the EMALS motor/generators takes 1.5 hours by itself. The inability to readily electrically isolate equipment precludes EMALS maintenance during flight operations, reducing the system operational availability.
- The Navy demonstrated, in developmental testing, corrections to previously discovered deficiencies related to end-stroke dynamics and excessive airframe stress discovered during EMALS testing in 2015. This technical solution needs to be fully integrated into the EMALS software and re-tested.

AAG

- Testing to date demonstrated that AAG should be able to recover aircraft planned for the CVN 78 air wing, but the poor reliability demonstrated so far suggests AAG will have trouble meeting operational requirements.
- The Program Office redesigned major components that did not meet system specifications during land-based testing. In June 2017, the Program Office estimated that the redesigned AAG had a reliability of approximately 19 Mean Cycles Between Operational Mission Failures (MCBOMF) in the shipboard configuration, where a cycle represents the recovery of one aircraft. This reliability estimate is well below the rebaselined reliability growth curve and well below the 16,500 MCBOMF specified in the requirements documents. In its current design, AAG is unlikely to support routine flight operations. At the current reliability, AAG has less than a 0.001 percent chance of completing the 4-day surge and less than a 0.200 percent chance of completing a day of sustained operations as defined in the design reference mission. For routine operations, AAG would only have a 53 percent chance of completing a single 12 aircraft recovery cycle and a 1 percent chance of completing a typical 84 aircraft recovery day.
- The reliability concerns are worsened by the current AAG design that does not allow Power Conditioning Subsystem equipment to be electrically isolated from high power buses, limiting corrective maintenance on below-deck equipment during flight operations. This reduces the operational availability of the system.

DBR

- Previous testing of Navy combat systems similar to that of CVN 78 revealed numerous integration problems that degrade the performance of the Integrated Warfare System. Many of these problems are expected to exist on CVN 78. Current test results reveal problems with tracking and supporting missiles in flight, excessive numbers of clutter/ false tracks, and track continuity concerns. The Navy recently extended DBR testing at Wallops Island until 4QFY17; however, more test-analyze-fix cycles are likely to be needed to develop and test DBR fixes so it can properly perform air traffic control and engagement support on CVN 78.
- In limited at-sea operations, DBR exhibited frequent uncommanded system resets, and has had problems with the power supply system. These problems combined significantly limited operation and testing during the limited at-sea periods available so far.
- Beyond the above mentioned concerns, the Navy has only engineering analysis of DBR reliability. The reliability of the production VSR equipment in the shipboard DBR system has not been assessed. While the Engineering Development Model (EDM) VSR being tested at Wallops Island has experienced failures, it is not certain whether these EDM VSR failure modes will persist during shipboard testing of the production VSR. Reliability data collection will continue at Wallops Island and during DBR operations onboard CVN 78.

SGR

- CVN 78 is unlikely to achieve its SGR requirement. The target threshold is based on unrealistic assumptions including fair weather and unlimited visibility, and that aircraft emergencies, failures of shipboard equipment, ship maneuvers, and manning shortfalls will not affect flight operations. DOT&E plans to assess CVN 78 performance during IOT&E by comparing it to the SGR requirement as well as to the demonstrated performance of the *Nimitz*-class carriers.
- During the 2013 operational assessment, DOT&E conducted an analysis of past aircraft carrier operations in major conflicts. The analysis concludes that the CVN 78 SGR requirement is well above historical levels and that CVN 78 is unlikely to achieve that requirement.
- There are also concerns with the reliability of key systems that support sortie generation on CVN 78. Poor reliability of these critical systems could cause a cascading series of delays during flight operations that would affect CVN 78's

ability to generate sorties, make the ship more vulnerable to attack, or create limitations during routine operations. The poor or unknown reliability of these critical subsystems will be the most significant risk to the successful completion of CVN 78 IOT&E. The analysis also considered the operational implications of a shortfall and concluded that as long as CVN 78 is able to generate sorties comparable to *Nimitz*-class carriers, the operational capabilities of CVN 78 will be similar to that of a *Nimitz*-class carrier.

Electric Plant

- The Navy manufactured and tested a full-scale qualification unit of the shipboard Electrical Plant and components in a land-based facility in 2004. This test revealed no problems with the design of the original transformers or any other part of the main turbine generator. Following an initial transformer failure, which was determined to be caused by a material failure, the Navy decided to replace the transformers with an existing design used in other Navy applications. The Navy did not perform sufficient land-based testing on the alternate transformer to validate that no system design flaws or vulnerabilities with the revised voltage regulating system design existed. The Navy considered the risk was low and did not want to further delay ship delivery for the testing. However, voltage regulating system design flaws resulted in damage to a second main turbine generator following a subsequent transformer failure. This incident delayed the ship's delivery as well as both live fire and operational testing and currently the ship is operating on three of the four main turbine generators as a direct result of the second failure.

Manning

- Based on earlier Navy analysis of manning and the Navy's early experience with CVN 78, several areas of concern have been identified. The Navy is working with the ship's crew to resolve these problems.
- Based on current expected manning, the berthing capacity for officers and enlisted will be exceeded by approximately 100 personnel with some variability in the estimates. This also leaves no room for extra personnel during inspections or exercises, requiring the number of evaluators to be limited or the timeframe to conduct the training to be lengthened. This shortfall in berthing is further exacerbated by the 246 officer and enlisted billets (roughly 10 percent of the crew) identified in the Manning War Game III as requiring a face-to-face turnover. These turnovers will not all happen at one time, but will require heavy oversight and will limit the amount of turnover that can be accomplished at sea and especially during evaluation periods.
- Manning must be supported at the 100 percent level, although this is not the Navy's standard practice on other ships, and the Navy's personnel and training systems may not be able to support 100 percent manning. The ship is extremely sensitive to manpower fluctuations. Workload estimates for the many new technologies such as catapults, arresting gear, radar, and weapons and aircraft elevators are not yet well understood. Finally, the Navy is considering placing the ship's seven computer networks under a single department. Network management and the correct manning to facilitate continued operations is a concern for a network that is more complex than historically seen on Navy ships.

Electromagnetic Compatibility

- Developmental testing has identified significant EMI and radiation hazard problems. The Navy is continuing to characterize and develop mitigation plans for the problems, but some operational limitations and restrictions are expected to persist into IOT&E and deployment. The Navy will need to develop capability assessments at differing levels of system utilization in order for commanders to make informed decisions on system employment.

Recommendations

- Status of Previous Recommendations. The Navy should continue to address the seven remaining FY10, FY11, FY13, FY14, FY15, and FY16 recommendations.
  1. Finalize plans that address CVN 78 Integrated Warfare System engineering and ship self-defense system discrepancies prior to the start of IOT&E.
  2. Provide scheduling, funding, and execution plans to DOT&E for the live SGR test event during the IOT&E.
  3. Continue to work with the Navy's Bureau of Personnel to achieve adequate depth and breadth of required personnel to sufficiently meet Navy Enlisted Classification fit/fill manning requirements of CVN 78.
  4. Conduct system of systems developmental testing to preclude discovery of deficiencies during IOT&E.
  5. Address the uncertain reliability of EMALS, AAG, DBR, and AWE. These systems are critical to CVN 78 flight operations, and are the largest risk to the program.
  6. Begin tracking and reporting on a quarterly basis system reliability for all new systems, but at a minimum for EMALS, AAG, DBR, and AWE.
  7. Submit a TEMP for review and approval by DOT&E incorporating the Deputy Secretary's direction to conduct the FSST before CVN 78's first deployment.
- FY17 Recommendations. The Navy should:
  1. Resolve how SGR estimates from the live SGR test will be extended to the 35-day design reference mission.
  2. Continue to characterize the electromagnetic environment onboard CVN 78 and develop operating procedures to maximize system effectiveness and maintain safety. As applicable, the Navy should utilize the lessons learned from CVN 78 to inform modifications to CVN 79 and beyond.

DDG 51 Flight III Destroyer/Air and Missile Defense Radar (AMDR)/Aegis Combat System

Executive Summary

- On November 21, 2016, the Deputy Secretary of Defense (DEPSECDEF) directed the Navy to fully fund the Aegis Self-Defense Test Ship (SDTS) and the aerial targets required for testing the DDG 51 Flight III, Air and Missile Defense Radar (AMDR), and Evolved Seasparrow Missile (ESSM) Block 2 programs. The Navy initially complied with the direction but subsequently removed all funding for the Aegis SDTS and the required aerial targets.
- On May 4, 2017, the DEPSECDEF directed the Navy to reinstate the funding for the Aegis SDTS and associated test firings in compliance with the previous November 2016 guidance. The Navy has not yet complied.

System

- The DDG 51 Flight III Destroyer is a combatant ship intended to be equipped with the:
  - AMDR three-dimensional (range, altitude, and azimuth) multi-function radar
  - Aegis Combat System used for air warfare missions and self-defense against anti-ship cruise missiles (ASCMs)
  - AN/SQQ-89 undersea warfare suite that includes the AN/SQS-53 sonar
  - MH-60R helicopter that supports undersea warfare
  - Close-In Weapon System for ship self-defense
  - Five-inch diameter gun for surface warfare and land attack
  - Vertical Launch System that can launch Tomahawk; Standard Missiles 2, 3, and 6; and ESSM Blocks 1 and 2
- The Navy is developing the AMDR to provide simultaneous sensor support of integrated air and missile defense (IAMD) and air defense (including self-defense) missions. IAMD and air defense missions require extended detection ranges and increased radar sensitivity against advanced threats with high speeds and long interceptor fly-out times. The three major components of AMDR are:
  - The AMDR S-band radar intended to provide IAMD, search, track, cueing, missile discrimination, air defense non-cooperative target recognition, S-band missile communications, surveillance capability for ship self-defense and area air defense, and S-band kill assessment support functions.
  - The AMDR X-band radar – intended to provide horizon and surface search capabilities, navigation, and periscope detection/discrimination functions – is delayed. In the interim, the legacy AN/SPQ-9B radar will provide these functions.
  - The AMDR Radar Suite Controller is intended to provide radar resource management and coordination and an open interface with the ship's combat system.

- The Aegis Combat System is an integrated naval weapons system that uses computers and radars to provide an advanced command and decision capability and a weapons control system to track and guide weapons to destroy enemy targets.
- The ESSM, cooperatively developed among 13 nations, is a medium-range, ship-launched, self-defense guided missile designed to defeat ASCM, surface, and low-velocity air threats. There are two variants of ESSM:
  - ESSM Block 1 is a semi-active radar-guided missile that is currently in-service.
  - ESSM Block 2 is in development and intended to provide semi-active radar guidance as well as active radar guidance.
- In comparison to the previous DDG 51 version (Flight IIA), Flight III includes, in addition to the upgraded combat system and the AMDR, the following modifications:
  - Upgraded fire extinguishing systems
  - Air conditioning plant upgrades
  - Upgraded electric generators and power conversion modules
- DDG 51 Flight III is also structurally different from the prior DDG 51 version. The design will add starboard enclosures, a stack of small boats, and additional structure in the fantail to increase reserve buoyancy and help compensate for additional weight increase. It will also include structural modifications to increase plate thicknesses to lower the ship's center of gravity and enhance girder strength.
- In addition to the self-defense features discussed above, the ship has the following survivability features:
  - Improved ballistic protection for magazines and other vital spaces as well as the inclusion of some shock-hardened systems/components to enhance survivability.

- Various installed and portable damage control, firefighting, and dewatering systems.

Mission

Naval Commanders will use the DDG 51 Flight III destroyer equipped with the Aegis Combat System and AMDR to provide joint battlespace threat awareness and defense capability to counter current and future threats in support of:

- Area air defense (to include self-defense with the ESSM) to counter advanced air and cruise missile threats and increase ship survivability
- Detecting, tracking, discriminating, and providing missile engagement support (including kill assessment) to counter ballistic missile threats
- Countering surface threats through surface surveillance, precision tracking, and missile and gun engagements
- Conducting undersea warfare with periscope detection and discrimination
- Detecting and tracking own-ship gun projectiles to support surface warfare and naval surface fire support

Major Contractors

- DDG 51 Flight III Destroyer major contractors are:
  - General Dynamics Marine Systems Bath Iron Works – Bath, Maine
  - Huntington Ingalls Industries – Pascagoula, Mississippi
- AMDR: Raytheon – Marlborough, Massachusetts
- Aegis Combat System: Lockheed Martin Marine Systems and Sensors – Moorestown, New Jersey
- ESSM Blocks 1 and 2: Raytheon – Tucson, Arizona

Activity

- On November 21, 2016, the DEPSECDEF directed the Navy to fully fund the Aegis SDTS and the aerial targets required for testing the DDG 51 Flight III, AMDR, and ESSM Block 2 programs. The Navy initially complied with the direction but subsequently removed all funding for the Aegis SDTS and the required aerial targets.
- On May 4, 2017, the DEPSECDEF directed the Navy to reinstate the funding for the Aegis SDTS and associated test firings in compliance the previous guidance. The Navy has not yet reinstated the funding.

Assessment

- Absent an AMDR- and Aegis-equipped SDTS, the Navy's operational test programs for the AMDR, Aegis Combat System, ESSM Block 2, and DDG 51 Flight III destroyer programs will not be adequate to fully assess their capabilities, in particular those associated with self-defense. They would also not be adequate to test the following Navy-approved DDG 51 Flight III, AMDR, Aegis Combat System, and ESSM Block 2 requirements.
  - The AMDR Capability Development Document (CDD) describes AMDR's IAMD mission, which requires AMDR to support simultaneous defense against multiple ballistic missile threats and multiple advanced ASCM threats. The CDD also includes an AMDR minimum track range requirement as part of the IAMD Key Performance Parameter.
  - The DDG 51 Flight III destroyer has a survivability Key Performance Parameter directly tied to meeting a self-defense requirement threshold against ASCMs described in the Navy's Surface Ship Theater Air and Missile Defense Assessment document of July 2008.
  - The ESSM Block 2 CDD has a requirement to provide self-defense against incoming ASCM threats in clear and jamming environments. The CDD also includes an ESSM Block 2 minimum intercept range Key Performance Parameter.
- Use of manned ships for operational testing with threat representative ASCM surrogates in the close-in, self-defense battlespace is not possible due to Navy safety restrictions because targets and debris from intercepts pose an unacceptable risk to personnel at ranges where some engagements will take place. The November 2013 mishap on USS *Chancellorsville* (CG 62) involving an ASCM surrogate target resulted in even more stringent safety constraints.
  - In addition to stand-off ranges, safety restrictions require that ASCM targets not be flown directly at a manned ship, but at some cross-range offset, which unacceptably degrades the operational realism of the test.
  - Similar range safety restrictions preclude manned ship testing of five of the seven self-defense ASCM scenarios included in the Navy-approved requirements document for the Aegis Modernization Advanced Capability Build 20 Combat System upgrade and will severely limit the operational realism of the two scenarios that can be flown against a manned ship. Safety restrictions also preclude testing of the AMDR minimum track range requirement against threat representative ASCM threat surrogates at the land-based AMDR Pacific Missile Range Facility test site.
  - To overcome these safety restrictions for the LHA 6, Littoral Combat Ship, DDG 1000, LPD 17, LSD 41/49, and CVN 78 ship classes, the Navy developed an Air Warfare/Ship Self-Defense Enterprise Modeling and Simulation (M&S) test bed, which uses live testing on the SDTS in the close-in battlespace with targets flying realistic threat profiles and manned ship testing for other battlespace regions, as well as soft-kill capabilities, to validate and accredit the M&S test bed. The Navy should do the same for the DDG 51 Flight III destroyer with its AMDR, as side-by-side comparison between credible live

fire test results and M&S test results form the basis for the M&S accreditation. Without an SDTS with AMDR and an Aegis Combat System, there will not be a way to gather all of the operationally realistic live fire test data needed for comparison to accredit the M&S test bed.

- Since Aegis employs ESSMs in the close-in, self-defense battlespace, understanding ESSM's performance is critical to understanding the self-defense capabilities of the DDG 51 Flight III destroyer.
  - Past DOT&E annual reports have stated that the ESSM Block 1 operational effectiveness has not been determined. The Navy has not taken action to adequately test the ESSM's operational effectiveness.
  - The Navy intends to conduct phases of the ESSM Block 2 IOT&E in conjunction with the DDG 51 Flight III destroyer, AMDR, and Aegis Combat System operational testing.
  - Specifically, because safety limitations preclude ESSM firing in the close-in, self-defense battlespace, there are very few test data available concerning ESSM's performance on Aegis ships against supersonic ASCM surrogates.
  - Any data available regarding ESSM's performance against supersonic ASCM surrogates are from a Ship Self-Defense System-based combat system configuration, using a completely different guidance mode or one that a different radar suite supports.
- The cost of building and operating an Aegis SDTS is estimated to be about $350 Million, compared to the estimated $14 Billion cost of the AMDR development/procurement and the estimated $45 Billion cost of the additional 22 or more DDG 51 Flight III ships that are planned for acquisition. Additionally, the cost of the ships that the DDG 51 Flight III destroyer is expected to protect is approximately $450 Billion in new ship construction over the next 30 years. Failure to adequately test the self-defense capability of DDG 51 Flight III destroyers means their survivability and that of a significant number other of ships the DDG-51 Flight III destroyers are intended to defend will be unknown. It is essential that the Navy program now fund the tests, targets, and Aegis Combat System equipment needed to conduct realistic self-defense testing using an AMDR- and Aegis-equipped SDTS.
- The modifications planned for DDG 51 Flight III are substantial enough to justify an assessment of ship survivability. To assess the effects of those modifications on ship survivability, the DDG 51 Flight III LFT&E strategy should include at least component shock qualification tests, a Total Ship Survivability Trial, a shock trial, and a plan to validate simulation tools used in the survivability assessment. The Navy has not yet developed an LFT&E Strategy for the program.

Recommendations

- Status of Previous Recommendations. The Navy has not addressed the following previous recommendations. The Navy should:
  1. Program for and fully fund an SDTS equipped with the AMDR, ESSM Block 2, and DDG 51 Flight III Aegis Combat System in time to support the DDG 51 Flight III destroyer and ESSM Block 2 IOT&Es.
  2. Modify the AMDR, ESSM Block 2, and DDG 51 Flight III Test and Evaluation Master Plans (TEMPs) to include a phase of IOT&E using an SDTS equipped with the AMDR and DDG 51 Flight III Combat System.
  3. Modify the AMDR, ESSM Block 2, and DDG 51 Flight III TEMPs to include a credible M&S effort that will enable a full assessment of the AMDR, ESSM Block 2, and DDG 51 Flight III Combat System's self-defense capabilities.
  4. Comply with the DEPSECDEF direction to develop and fund a plan, to be approved by DOT&E, to conduct at-sea testing of the self-defense of the DDG 51 Flight III destroyer with the AMDR, ESSM Block 2, and Aegis Combat System.
  5. Provide DOT&E the DDG 51 Flight III LFT&E Strategy for review and approval in coordination with the TEMP.
  6. Comply with the DEPSECDEF direction to work with DOT&E to develop an integrated test strategy for the DDG 51 Flight III, AMDR, Aegis Modernization, and ESSM Block 2 programs, and document that strategy into draft TEMPs for those programs to be provided to DOT&E.
- FY17 Recommendation.
  1. The Navy should program funds in the Future Years Defense Plan to complete all activities and procurement required to conduct adequate operational testing in FY24 of the DDG 51 Flight III, AMDR, and ESSM Block 2's self-defense capabilities on an Aegis-equipped SDTS.

Expeditionary Sea Base (T-ESB) (Formerly Mobile Landing Platform Afloat Forward Staging Base (MLP(AFSB))

Executive Summary

- In October 2017, DOT&E published a classified combined IOT&E and LFT&E report assessing T-ESB operational capability. This report was based on the IOT&E completed in August 2016 and the LFT&E, which included a Total Ship Survivability Trial (TSST), completed in August 2016.
- In August 2017, the Navy commissioned USS *Lewis B. Puller* (ESB 3), formerly USNS *Lewis B. Puller* (T-ESB 3), the first T-ESB. The Navy conducted all test activities discussed in this report on T-ESB 3; therefore, for consistency, this report refers to the ship as T-ESB.
- The T-ESB is operationally effective and suitable in supporting airborne mine countermeasures (AMCM) missions in a non-hostile environment.
- The T-ESB met the Navy's requirement to transit 9,500 nautical miles (nm) at 15 knots while fully loaded with an AMCM helicopter squadron including all countermeasures equipment.
- Self-defense capability is limited to crew-served weapons only. The T-ESB was designed to operate in a non-hostile environment with low/negligible threats to the ship. However, mine countermeasure (MCM) operations may require the ship to operate close to littoral threat areas. The lack of self-defense capability renders the ship dependent upon other naval combatants and joint forces for protection in the littoral operating environment.
- The T-ESB LFT&E program was adequate to support the DOT&E survivability assessment, and recommendations are published in the classified IOT&E and LFT&E report.

System

- T-ESB is a heavy-lift ship based primarily on the British Petroleum *Alaska*-class oil tanker design. The cargo area has been modified with a large mission deck, elevated flight deck (with aircraft hangar facilities), and military accommodations and workspaces for 250 personnel. The ship utilizes the same base ship as the Expeditionary Transfer Dock (T-ESD) class.
- The Navy built T-ESB to support AMCM missions, hosting up to four helicopters, MCM equipment, and associated support equipment.
- The ship is crewed with both Military Sealift Command (MSC) and U.S. Navy personnel.
- The Navy intends for T-ESB to replace USS *Ponce*, an *Austin*-class Amphibious Transport Dock commissioned in 1971. However, while USS *Ponce* is able to support the legacy triad of MCM forces – airborne, surface, and explosive ordnance disposal (EOD) along with the coordination staffs – the Navy built T-ESB to support only the AMCM mission.

- The Navy modified the ship to support Special Operations Forces (SOF) missions.
- The T-ESB design incorporates survivability features evaluated through the LFT&E program, to include:
  - Distributed firefighting equipment (in the form of a fire main and aqueous film-forming foam) and distributed damage control lockers/repair stations
  - Retractable bow thruster for station-keeping and limited emergency propulsion
  - Emergency electrical power to selective ship loads by way of the Emergency Diesel Generator (EDG)
  - A carbon dioxide gaseous flooding system in main engineering, EDG spaces, and spaces with high risk of fuel-induced fires
  - An aviation crash locker, due to T-ESB's more aviation-focused mission, to handle shipboard aviation casualties
  - A seawater sprinkling system for the protection of magazines and other high-risk spaces in the forward portion of the ship

Mission

Combatant Commanders use the T-ESB to support AMCM operations, to support SOF during Helicopter Assault Force and Boat Assault Force operations, to host explosive ordnance demolition teams, and as a strategic landing platform to support crisis response, counter-piracy operations, maritime security operations, and humanitarian aid/disaster relief missions.

Major Contractor

Base ship and T-ESB mission package: General Dynamics National Steel and Shipbuilding Company (NASSCO) – San Diego, California

Activity

- The Navy completed SOF upgrades on T-ESB 3 during Post Shakedown Availability (December 12, 2016, through April 30, 2017). NASSCO performed the work in Norfolk, Virginia, and the Navy conducted certification tests. Following these tests, the Navy deployed the ship. No operational test was conducted.
- In May 2017, the Navy's Operational Test and Evaluation Force published a classified IOT&E report on T-ESB.
- The Navy completed and delivered the T-ESB Final Survivability Assessment Report (FSAR) to DOT&E in August 2017.
- In August 2017, the Navy commissioned USS *Lewis B. Puller* (ESB 3), formerly USNS *Lewis B. Puller* (T-ESB 3), the first T-ESB.
- In October 2017, DOT&E published a classified combined IOT&E and LFT&E report on T-ESB based on post-delivery test and trials as well as the IOT&E and LFT&E that were completed in August 2016. IOT&E included cyber testing; LFT&E included a TSST.
- NASSCO plans to deliver two more T-ESB ships: hull 4 in March 2018 and hull 5 in May 2019. It delivered the first T-ESB (hull 3) in June 2015.

Assessment

- The T-ESB is operationally effective and suitable for supporting AMCM missions in a non-hostile environment.
  - The ship demonstrated high operational availability during testing, experiencing only four operational mission failure events and meeting the Navy's requirement for Mean Time Between Critical Failures.
  - The T-ESB demonstrated the ability to successfully support both day and night launch and recovery operations of AMCM aircraft, fueling at sea, and vertical replenishment operations.
  - The T-ESB met the Navy's requirements for the stowage, handling, and maintenance of four MH-53 helicopters as well as the mine-sweeping equipment sets needed to support AMCM operations.
  - The ship met the Navy's endurance requirements, exceeding the requirement to transit more than 9,500 nm at 15 knots without refueling.
  - By design, the ship has a 10 day capacity for chill/freeze/dry stores needed to support embarked military personnel. If fully manned, including AMCM squadron personnel, the ship would require chill/freeze/dry stores resupply twice during a 9,500 nm transit.
  - The ammunition magazines accommodate AMCM ordnance.
  - The aircraft maintenance shops surrounding the hangar bay lack air conditioning, which may limit the length of work days when operating in warm climates that may introduce heat stress conditions.
  - Per the Navy's requirement, the ship is not configured to concurrently accommodate explosive ordnance detachment personnel and equipment, the MCM staff required to coordinate the operations, and an AMCM helicopter squadron during MCM operations. Consequently, additional ships would be required to accommodate these personnel and their equipment during MCM operations.
- The T-ESB is survivable against typical commercial ship hazards such as groundings, collisions, raking, and fires. In expected, non-permissive environments (e.g., littorals), the T-ESB is largely dependent upon other naval combatants and joint forces for protection. Lack of military survivability capabilities introduces the following shortfalls:
  - The ship does not have chemical, biological and radiological defense capability, including a countermeasure wash-down capability.
  - The ship lacks a self-defense capability against likely threats in the littoral operating environment. Self-defense is limited to crew-served weapons only.
- The TSST revealed ship design deficiencies associated with emergency lighting, personnel egress, and the watertight and interior doors. The trial also identified limitations with ship communications systems that challenged damage control effectiveness as well as the coordination of Navy and MSC crews.
- Cybersecurity test results and analysis are provided in DOT&E's classified IOT&E and LFT&E report.
- After T-ESB 3 received the SOF upgrade, Naval Air Systems Command (NAVAIR) certified the ship to have a maximum of four aircraft on the flight deck at any time with the limitation that only two aircraft are permitted to operate (engage rotors) simultaneously. NAVAIR certified ScanEagle as the only unmanned air vehicle approved to operate on this platform. The Navy demonstrated the crew's ability to deploy a Combat Craft Assault boat, an asset needed for SOF missions.

Recommendations

- Status of Previous Recommendations: The Navy has not addressed the FY15 recommendation to install a separate Ship Service Diesel Generator to minimize periods of under-loading of the Main Diesel Generators.
- FY17 Recommendations. The Navy should:
  1. Conduct FOT&E to determine the effectiveness of T-ESB to conduct SOF missions.
  2. Improve the ship's self-defense capabilities.
  3. Fix or mitigate all identified cybersecurity vulnerabilities as identified in the DOT&E report and conduct a follow-on cybersecurity test.
  4. Mitigate the effect of casualties and improve ship recoverability by incorporating redundancies in the distribution of medical equipment, firefighting, and egress systems.
  5. Modify firefighting documentation and training to coordinate efforts among the MSC crew, military detachment, and aviation detachment to improve ship recoverability.
  6. Consider the complete list of recommendations in DOT&E's classified IOT&E and LFT&E report.

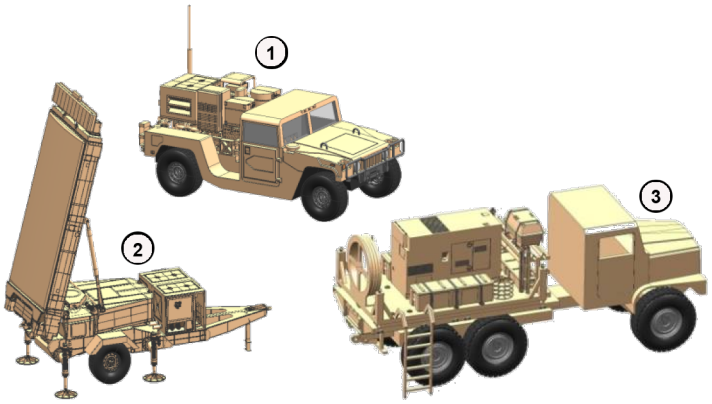
Ground/Air Task Oriented Radar (G/ATOR)

Executive Summary

- The Marine Corps Program Executive Office (PEO) Land Systems (LS) is proceeding with early deployment for a limited number of Ground/Air Task Oriented Radar (G/ATOR) Block 1 and Block 2 systems in FY18. DOT&E endorsed the PEO LS early deployment plans in February 2014. These systems will use a Gallium Arsenide receiver/transmitter configuration.
- In March 2014, PEO LS completed Milestone C and authorized the acquisition of low-rate initial production (LRIP) systems.
- The Block 1 Developmental Test (DT) 1C is complete and the Block 2 DT 1D is underway. A total of four LRIP systems support these tests.
- DT 1C littoral testing at Marine Corps Outlying Field (MCOLF) Atlantic, North Carolina, was limited in scope; however, G/ATOR demonstrated the Block 1 ability to detect and track aircraft targets in the littoral environment and demonstrated its ability to support the intended mission areas.
- During DT 1C, the Program Management Office (PMO) led and the Marine Corps Operational Test and Evaluation Activity (MCOTEA) observed a Cooperative Vulnerability and Penetration Assessment (CVPA) and a limited Adversarial Assessment (AA). Though the CVPA and AA identified cyber vulnerabilities, they were not sufficient to support a full assessment.
- IOT&E of G/ATOR in a new Gallium Nitride receiver/transmitter configuration is scheduled for FY19.

System

- G/ATOR is a short- to medium-range, air-cooled, phased-array radar under development for the Marine Corps. It is intended to replace five current radar systems and augment the AN/TPS-59 long-range radar. A total of 57 G/ATOR systems are planned for procurement.
- The PEO LS is developing G/ATOR in three blocks.
  - Block 1 develops the basic hardware and provides Air Defense/Surveillance Radar (AD/SR) capability. It replaces the AN/UPS-3, AN/MPQ-62, and AN/TPS-63 radar systems.
  - Block 2 adds a ground counterbattery/counter-fire mission capability and replaces the AN/TPQ-46 radar system.
  - Block 3 was a series of enhancements, including Identification Friend or Foe Mode 5/S, that are instead being incorporated into other blocks. The term Block 3 is no longer used.
  - Block 4 replaces the AN/TPS-73 radar system for air traffic control capability, which will be a future development effort.



1 - Communications Equipment Group (CEG)
2 - Radar Equipment Group (REG)
3 - Power Equipment Group (PEG) on MTVR pallet
MTVR - Medium Tactical Vehicle Replacement

- The G/ATOR baseline system configuration is comprised of three subsystems:
  - The Radar Equipment Group consists of the phased-array radar mounted on an integrated trailer. The trailer is towed by a Medium Tactical Vehicle Replacement.
  - The Power Equipment Group includes a 60-kilowatt generator and associated power cables mounted on a pallet. The generator pallet is carried by a Medium Tactical Vehicle Replacement.
  - The Communications Equipment Group provides the ability to communicate with and control the radar and is mounted inside the cargo compartment of a High Mobility Multi-purpose Wheeled Vehicle.
- The first six LRIP systems have receiver/transmitter modules built using Gallium Arsenide. Subsequent systems, representing the majority of the production buy, will have receiver/transmitter modules built using Gallium Nitride, which is more power efficient and reduces system costs.

Mission

The Marine Air-Ground Task Force (MAGTF) commander will employ G/ATOR within the Air Combat Element (ACE) and the Ground Combat Element (GCE). Within the ACE, G/ATOR will provide enhanced situational awareness and additional capabilities to conduct short- to medium-range radar surveillance and air defense, and air traffic control missions. Within the GCE G/ATOR will provide ground weapons locating capability for conduct of counter-battery/counter-fire missions.

Major Contractor

Northrop Grumman Electronic Systems – Linthicum, Maryland

Activity

- The G/ATOR program completed Milestone B and entered the Engineering and Manufacturing Development phase in August 2005 as an Acquisition Category II program. However, in October 2011, the Navy redesignated G/ATOR as an Acquisition Category IC program due to increases in the amount of Research, Development, Test, and Evaluation funding required to meet mandatory Force Protection requirements.
- In March 2014, PEO LS completed Milestone C for Block 1 and Block 2 and authorized the acquisition of LRIP systems. Northrop Grumman Electronic Systems delivered four G/ATOR LRIP systems in February, April, August, and September 2017, and intends to deliver two more systems before the end of CY17.
- Using a G/ATOR LRIP system, the Marine Corps conducted DT 1C from May 2017 to September 2017 at NASA Wallops Flight Facility, Virginia; Marine Corps Air Station (MCAS) Cherry Point, North Carolina; MCOLF Atlantic, North Carolina; and MCAS Yuma, Arizona.
- The Marine Corps began DT 1D on September 25, 2017, with an expected completion in 2QFY18. DT 1D is being conducted at Yuma Proving Grounds, Arizona; Marine Corps Air Ground Combat Center, Twentynine Palms, California; and White Sands Missile Range, New Mexico.
- The Marine Corps conducted interoperability testing on G/ATOR LRIP systems at Wallops Island and MCAS Cherry Point. Data were also collected in a littoral environment at MCOLF Atlantic.
- During DT 1C, the PMO led and the Marine Corps Information Assurance Red Team performed a CVPA and limited AA.
- Since the Marine Corps was collecting data in an operationally realistic environment, DOT&E approved DT 1C and DT 1D as integrated tests with MCOTEA observation. Further, DOT&E approved data to be used to support upcoming FY18 operational assessments (OAs).
- The Marine Corps has conducted DT 1C and DT 1D information technology testing to date in accordance with a DOT&E-approved test plan.
- The OA for Block 1 began September 2017 at MCAS Yuma and will support an early deployment decision in 2QFY18.
- The OA for Block 2 is scheduled to begin during 3QFY18 and will support an early deployment decision in 4QFY18.
- IOT&E of G/ATOR Block 1 and Block 2 in a new Gallium Nitride receiver/transmitter configuration is scheduled for FY19.

Assessment

- During interoperability testing with the Composite Tracking Network (CTN) system while integrated into a Cooperative Engagement Capability Network, G/ATOR maintained connectivity. In addition, G/ATOR maintained connectivity with the Phase 2 Common Aviation Command and Control System and CTN while operating within the Tactical Air Operations Center.
- Littoral testing at MCOLF Atlantic was limited in scope, testing G/ATOR with scheduled aircraft sorties as well as aircraft targets of opportunity. G/ATOR was able to detect and track these targets in the littoral environment, demonstrating its support of the following mission areas: surveillance, positive control of friendly aircraft, and intercept of hostile aircraft and missiles.
- The CVPA and limited AA helped to characterize system cyber vulnerabilities. However, they were not conducted under operationally realistic conditions and did not assess operator responses to various cyber-attacks in end-to-end scenarios and therefore cannot support a full assessment.

Recommendations

- Status of Previous Recommendations. As a result of the findings of a Blue Ribbon Panel on the reliability of G/ATOR, the Program Office has re-evaluated the G/ATOR reliability program and the system's reliability growth curves consistent with the prior recommendation.
- FY17 Recommendations.
  1. The PMO should continue to monitor G/ATOR reliability and availability during developmental testing in preparation for the upcoming OAs as well as the IOT&E currently scheduled for FY19.
  2. In order to fully assess G/ATOR capabilities, MCOTEA should ensure that the Marine Corps Information Assurance Red Team conducts a CVPA and an AA on both the Block 1 and Block 2 systems in an operationally realistic environment in support of IOT&E. The CVPA and AA should also assess operator responses to various cyber-attacks in end-to-end scenarios.

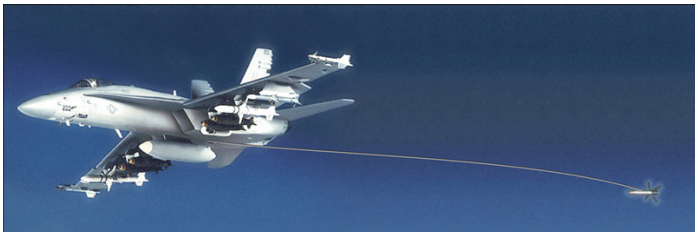
Integrated Defensive Electronic Countermeasures (IDECM)

Executive Summary

- The Navy's Operational Test and Evaluation Force released the classified Integrated Defensive Electronic Countermeasure (IDECM) Block IV (IB-4) Operational Assessment report on February 27, 2017.
- DOT&E released the classified IB-4/Software Improvement Program (SWIP) Operational Assessment report on June 12, 2017.
- IB-4 is effective and suitable on the F/A-18 E/F.
- IB-4 is not effective and not suitable on the F/A-18 C/D Legacy Hornets because of Environmental Control System compatibility problems.
- SWIP is in developmental test with a planned fielding date of 3QFY18.
- DOT&E removed IDECM from the oversight list on June 21, 2017.

System

- The IDECM system is a self-protect electronic countermeasure suite on F/A-18 Strike Fighter aircraft that defends against radio frequency-guided threats. IDECM is comprised of on- and off-board components. The onboard components receive and process radar signals and can employ on- and/or off-board jamming components in response to identified threats.
- There are four IDECM variants: Block I (IB-1), Block II (IB-2), Block III (IB-3), and Block IV (IB-4). All the variants include an onboard radio frequency receiver and jammer.
  - IB-1 (fielded FY02) combined the legacy onboard receiver/jammer (ALQ-165) with the legacy (ALE-50) off-board towed decoy.
  - IB-2 (fielded FY04) combined an improved onboard receiver/jammer (ALQ-214) with the legacy (ALE-50) off-board towed decoy.
  - IB-3 (fielded FY11) combined the improved onboard receiver/jammer (ALQ-214) with a new (ALE-55) off-board fiber-optic towed decoy that is more integrated with the ALQ-214.
  - IB-4 (fielded FY16 on F/A-18 E/F) replaces the onboard receiver/jammer (ALQ-214(V)3) with a lightweight, repackaged onboard jammer (ALQ-214(V)4)). IB-4 (ALQ-214(V)5) (currently in developmental testing) is intended to replace the ALQ-126B on F/A-18 C/D to provide advanced, carrier capable jamming for the first time to the F/A 18 C/D.



- IB-4 hardware will run enhanced onboard software known as SWIP. SWIP will give IDECM a new deny/delay capability to enhance survivability against modern radio frequency threat systems. IB-4 with SWIP is still in developmental testing.
- The F/A-18 E/F installation includes off-board towed decoys. The F/A-18 C/D installation includes only the onboard receiver/jammer components and not the towed decoy.

Mission

- Combatant Commanders will use IDECM to improve the survivability of Navy F/A-18 strike aircraft against radio frequency-guided threats while flying air-to-air and air-to-ground missions.
- The Navy intends to use the IB-4 complex jamming capabilities to increase survivability against modern radar-guided threats.

Major Contractors

- ALE-55: BAE Systems – Nashua, New Hampshire
- ALQ-214: Harris – Clifton, New Jersey
- ALE-50: Raytheon Electronic Warfare Systems – Goleta, California

Activity

- The Navy released the classified IDECM IB-4 Operational Assessment report on February 27, 2017. DOT&E released the classified IB-4/SWIP Operational Assessment report on June 12, 2017.
- The Navy conducted all testing in accordance with a DOT&E-approved test plan.
- DOT&E removed IDECM from its oversight list in June 2017.

IB-4

- The Navy fielded IB-4 for F/A-18 E/F in FY16.
- IB-4 operational testing for F/A-18 C/D is incomplete due to Environmental Control System compatibility problems. The remainder of operational testing may not be completed on Marine Corps F/A-18 C/D legacy Hornets (until the FY20 timeframe). The Navy will continue to study the correct fielding plan for IDECM on F/A-18 C/D Legacy Hornets.

SWIP

- SWIP is in developmental test. The Navy plans to field SWIP in 3QFY18.

Assessment

IB-4

- IB-4 is effective and suitable on the F/A-18 E/F.
- IB-4 is not suitable and not effective on the F/A-18 C/D Hornets due to Environmental Control System compatibility problems. The Navy will not field IB-4 on F/A-18 C/D aircraft.

SWIP

- Assessment results are included in the classified DOT&E Operational Assessment report.

Recommendations

- Status of Previous Recommendations. The Navy addressed previous FY16 recommendations.
- FY17 Recommendations. All recommendations can be found in DOT&E's classified Operational Assessment report from June 2017.

LHA 6 New Amphibious Assault Ship (formerly LHA(R))

Executive Summary

- In FY17, the Navy completed a multi-phased IOT&E focused on LHA 6's ability to support amphibious warfare (AMW) operations, ship self-defense (including cybersecurity), mobility, and supporting characteristics. LHA 6 deployed in July 2017 with a Marine Expeditionary Unit (MEU) Aviation Combat Element (ACE) that includes AV-8B Harrier aircraft. The Navy will not complete the operational evaluation of the ship's ability to support a complement of 20 F-35B Joint Strike Fighter (JSF) aircraft until FY20.
- The Navy and Marine Corps conducted the OT-C4 phase of IOT&E, which focused on the AMW mission, in conjunction with scheduled pre-deployment fleet exercises as a substitute for a dedicated IOT&E period.
- The Navy and Marine Corps demonstrated the ability to land, service, and launch all required aircraft on LHA 6. The ship conducted an F-35B developmental test event that demonstrated the ship's ability to support landings and take-offs. However, the Navy and Marine Corps have not conducted a multi-day amphibious operation sufficient to assess the ship's ability to support all required AMW mission activities.
- The Navy conducted the OT-C3 phase of IOT&E. This phase included tests of the gun weapon systems against small boat raids and low slow flying unmanned aerial vehicles (UAVs) and a demonstration of the chemical warfare detection, protection, and recovery system. The results of the gun system tests are classified. The chemical warfare agent dispersion was not conducted in accordance with the DOT&E-approved test plan.
- In February 2017, the Navy conducted the second part of LHA 6 IOT&E phase OT-C5, the Adversarial Assessment (AA), which evaluated LHA 6 cybersecurity. The results of the testing are classified. This assessment was limited to 7 of 83 networked systems onboard, and excluded the hull, mechanical, and electrical (HM&E) systems and the Navigation Sensor System Interface (NAVSSI). The testing identified deficiencies that could adversely affect operational effectiveness in a cyber-contested environment.
- The Navy completed the Total Ship Survivability Trial (TSST) in April 2017 to assess damage effects and the crew's ability to recover the ship after an operationally representative weapon engagement. The trial was executed with the ship configured for combat, including a standard MEU ACE. While crew recovered the ship following the simulated casualty, significant personnel casualties were expected for the threats evaluated. The TSST also showed that the ability to maintain certain mission capabilities was degraded.
- DOT&E published a classified Early Fielding Report in November 2017 detailing early observations from the IOT&E and LFT&E of LHA 6. DOT&E will provide a full evaluation of LHA 6's effectiveness, suitability, and survivability after all data are received from the Navy and the ship self-defense testing is completed.

System

- LHA 6 is the lead ship of this new class of large-deck amphibious assault ships designed to support a notional mix of MEU ACE fixed- and rotary-wing aircraft consisting of 12 MV-22 Ospreys, 6 F-35B JSFs (Short Take-Off/Vertical Landing (STOVL) variant), 4 CH-53Es, 7 AH-1s/UH-1s, and 2 Navy MH-60 Search and Rescue aircraft, or an alternate loadout of 20 F-35Bs and 2 MH-60 Search and Rescue aircraft. Key ship features and systems include the following:
  - A greater aviation storage capacity and an increase in the size of the hangar bay to accommodate the enhanced aviation maintenance requirements for the MEU ACE with embarked F-35B and MV-22. Additionally, two maintenance areas with high-overhead clearance have been incorporated in the hangar bay to accommodate maintenance on MV-22s in the spread configuration (wing spread, nacelles vertical, and rotors spread).
  - The ship does not have a well deck. Aviation assets must be used to transfer personnel and equipment to and from the beach.
  - Shipboard medical spaces were reduced in size by approximately two thirds compared to contemporary LHDs to accommodate the expanded hangar bay.
- The LHA 6 combat system used for defense against air threats and small surface threat craft includes the following major components:
  - The Ship Self-Defense System (SSDS) MK 2 Mod 4B supporting the integration and control of most other combat system elements
  - The AN/SPS-48E and AN/SPS-49A air search radars and the AN/SPQ-9B horizon search radar

  - USG-2 Cooperative Engagement Capability real-time sensor netting system
  - The Rolling Airframe Missile and the Evolved Seasparrow Missile (ESSM), with the NATO Seasparrow MK 9 Track Illuminators
  - The AN/SLQ-32B(V)2 electronic warfare system with the Nulka electronic decoy-equipped MK 53 Decoy Launching System
  - The Phalanx Close-In Weapon System Block 1B and the MK 38 Mod 2 Gun Weapon System
- Two marine gas turbine engines, two electric auxiliary propulsion motors, and two controllable pitch propellers provide propulsion. Six ship service diesel generators provide electric power.
- Command, control, communications, computers, and intelligence (C4I) facilities and equipment support Marine Corps Landing Force operations. The Navy will not install the Consolidated Afloat Networks and Enterprise Services (CANES) on the LHA 6 before FY22, but the LHA 7 design and beyond will deploy with CANES incorporated.
- To reduce vulnerability and enhance recoverability following threat impact, the ship has the following survivability features:
  - Improved ballistic protection for magazines and other vital spaces as well as the inclusion of some shock hardened systems/components
  - Various installed and portable damage control, firefighting, and dewatering systems
- The Navy will introduce a Flight 1 variant of the LHA(R) program with the third ship, LHA 8. It will gain a well deck for deploying surface connectors to move troops and equipment ashore, a modified flight deck, and smaller island intended to enable an aviation support capability similar to LHA 6.

Mission

The Joint Maritime Component Commander will employ LHA 6 to:

- Serve as the primary aviation platform within an Amphibious Ready Group providing space and accommodations for Marine Corps vehicles, cargo, ammunition, and more than 1,600 troops
- Serve as an afloat headquarters for an MEU, Amphibious Squadron, or other Joint Force commands using its C4I facilities and equipment to provide mission support
- Accommodate elements of a Marine Expeditionary Brigade when part of a larger amphibious task force
- Carry and discharge combat service support elements and cargo to sustain the landing force

Major Contractor

Huntington Ingalls Industries, Ingalls Shipbuilding Division – Pascagoula, Mississippi

---

Activity

- DOT&E published a classified Early Fielding Report in November 2017 detailing early observations from the IOT&E and LFT&E of LHA 6. DOT&E will provide a full evaluation of LHA 6's effectiveness, suitability, and survivability after all data are received from the Navy and the ship self-defense testing is completed.
- The Navy conducted LHA 6 IOT&E phase OT-C3 in January 2017. This phase included tests of the gun systems against small boat raids and low slow flying UAVs, and a demonstration of the chemical warfare detection, protection, and recovery system. The results of the gun system tests are classified.
- The Navy and Marine Corps Operational Test Agencies (OTAs) completed LHA 6 IOT&E phase OT-C4 – the AMW phase – in conjunction with three separate fleet training/certification exercises: Amphibious Squadron/MEU Integration Training (PMINT), Composite Training Unit Exercise, and Certification Exercise. These tests were conducted from April 3-14, May 1-17, and June 1-14, 2017, respectively.
- The Navy executed the TSST from March 29 to April 2, 2017, prior to the start of PMINT. The trial was executed with the ship configured for combat, including an MEU ACE. This event provided data to assess the ship's ability to recover and evacuate personnel from affected areas of the ship following damage from a threat weapon.
- To support the self-defense evaluation, the Navy's Operational Test and Evaluation Force (OPTEVFOR) began the Probability of Raid Annihilation (PRA) Modeling and Simulation (M&S) test bed phase of IOT&E in March 2017. Completion of this test phase is expected in December 2017.
- The Navy conducted the LHA 6 cybersecurity testing AA from February 20-24, 2017. The results of these tests are classified. OPTEVFOR conducted testing on 7 of 83 networked systems due to limited tester availability and did not perform testing on HM&E systems due to equipment safety concerns. The Navy did not permit any hands-on manipulation of HM&E or NAVSSI systems; instead, they intend to develop a stand-alone high-fidelity testing environment to allow evaluation of similar systems in a representative environment without the risk of corrupting installed shipboard systems.
- The Navy conducted all testing in accordance with the DOT&E-approved test plan, with the following exceptions:
  - In the OT-C3 phase of IOT&E, the Navy did not conduct the simulated chemical agent deployment in accordance with the DOT&E-approved test plan, as it was unable to certify a helicopter-borne sprayer in time for the testing. The method of agent dispersion was inadequate to meet

several goals of the test, and the test should be conducted in FOT&E in accordance with the approved test plan to obtain the required information.
  - Because the OTAs were not in charge of executing the pre-deployment exercises, the AMW phase of the LHA 6 IOT&E did not result in the movements of personnel, vehicle, and cargo outlined in the DOT&E-approved test plan.
- The Navy is developing an LHA(R) Test and Evaluation Master Plan (TEMP) Revision B to address design modifications to LHA 8, including the addition of the well deck and changes to the flight deck, the island configuration, the combat system, medical spaces, fuel tanks, and supporting spaces. The impacts of evolutionary changes of Marine Corps aircraft, surface connectors, and vehicles will also be considered.
- The Navy does not intend to conduct the Advanced Mine Simulation System (AMISS) trial, which would be used to characterize the mine susceptibility of the LHA 6, as agreed to in the DOT&E-approved TEMP Revision A. To date, the Navy has not presented a valid alternative to conducting the AMISS trial.

Assessment

- LHA 6 demonstrated the ability to support AMW mission tasks: load and unload cargo and vehicles from aircraft, launch and recover aircraft, and muster and load marines. However, the movement of marines, cargo, and vehicles during testing failed to generate the operational tempo (OPTEMPO) required by the OTAs for an adequate operational test. Early analysis indicates limited aircraft availability may have been a factor in the OPTEMPO during pre-deployment exercises, but analysis is still ongoing. If the Navy and Marine Corps desire to combine pre-deployment exercises with IOT&E for future amphibious ship programs, this shortcoming must be mitigated.
- The Navy and Marine Corps demonstrated the ability to land, service, and launch all required aircraft on LHA 6, including MV-22, AV-8B, CH-53E, AH-1, UH-1, and H-60.
- Developmental testing of the F-35B, executed from October to November 2016, shows that LHA 6 supports the conduct of take-offs and landings of STOVL aircraft. Operational testing of the F-35B onboard LHA 6 is currently scheduled for FY20.
- LHA 6 cybersecurity testing identified deficiencies that could adversely affect operational mission effectiveness in a cyber-contested environment.
- The Navy has proposed an M&S-based approach to characterizing the mine susceptibility of LHA 6 in lieu of executing the AMISS trial. DOT&E does not agree that this approach is adequate.
- The TSST demonstrated that ship recoverability design features would likely enable the ship crew to mitigate the damage spread and adequately recover the ship if hit by the threat weapons assessed as part of this trial. In some trial scenarios, numerous personnel casualties were expected because of the challenges associated with moving large numbers of people through restricted internal egress points. Some of the ship's vital systems were degraded or lost because of predicted damage to support systems including chilled water, electrical power, potable water, and compressed air. The Navy is assessing the resulting degradation of mission capability, and will provide these results in a future TSST and survivability assessment report.

Recommendations

- Status of Previous Recommendations. While the Navy addressed some of the previous recommendations, it has:
  1. Neither planned nor resourced the mine susceptibility trial for the LHA 6 using the AMISS.
  2. Not yet conducted cybersecurity testing of HM&E and navigation systems in a laboratory.
- FY17 Recommendations. The Navy should:
  1. Plan to conduct adequate chemical detection testing in FOT&E.
  2. Not repeat the LHA 6 AMW IOT&E execution. For future amphibious ship test programs in which the Navy desires to combine IOT&E with fleet pre-deployment exercises, organize a subset of days in which OTAs have control over mission planning, mission execution, and data collection to ensure execution of an adequate AMW IOT&E.

Littoral Combat Ship (LCS)

Executive Summary

- The Littoral Combat Ship (LCS) program conducted no operational testing of seaframes and mission package (MP) capabilities in FY17.
- The Coastal Battlefield Reconnaissance and Analysis (COBRA) Block I in the mine countermeasures (MCM) MP completed one of five phases of IOT&E in FY17.
- DOT&E published an assessment of the results of operational testing of the *Independence*-variant seaframe equipped with the Increment 2 surface warfare (SUW) MP in November 2016. The Navy did not conduct any additional testing or perform any modifications to the seaframe and SUW MP in 2017 that would affect the 2016 assessment.
- In March 2016, the Navy completed a partial update of the LCS Test and Evaluation Master Plan (TEMP) to support future operational testing of the seaframes and MPs. Since then, DOT&E and the Navy worked to extensively revise the TEMP by incorporating developmental and integrated testing as well as examining reductions in operational testing to accommodate the Navy's restricted program budget for LCS testing. DOT&E expects to approve the LCS Program TEMP Test and Evaluation Identification Number (TEIN) 1695 Revision B in 2QFY18.
- DOT&E published the LCS 4 Total Ship Survivability Trial (TSST) Report in September 2017. The report included recommendations the Navy should consider implementing on the *Independence* variant. DOT&E is awaiting the Navy delivery of the LCS 5 and LCS 6 Shock Trial reports. Shock trials on both variants occurred between June and September 2016 off the northeastern coast of Florida. Based on the analysis and testing performed by the Navy to date, DOT&E's assessment of the survivability of both LCS variants is unchanged from previous annual reports.

***Freedom* Variant (LCS 1)**

***Independence* Variant (LCS 2)**

System

Seaframes

- The LCS is designed to operate in shallow waters that limit the access of larger ships.
- The Navy is procuring two LCS seaframe variants:
  - The *Freedom* variant (odd-numbered ships) is a semi-planing monohull design constructed of steel (hull) and aluminum (deckhouse) with two steerable and two fixed-boost waterjets driven by a combined diesel and gas turbine main propulsion system.
  - The *Independence* variant (even-numbered ships) is an aluminum trimaran with two steerable waterjets driven by diesel engines and two steerable waterjets driven by gas turbine engines.
- Common design specifications include:
  - Sprint speed in excess of 40 knots, draft of less than 20 feet, and an unrefueled range in excess of 3,500 nautical miles at 14 knots.
  - Accommodations for up to 98 personnel.
  - A common Mission Package Computing Environment for use when an MP is embarked.
  - A Multi-Vehicle Communications System for simultaneous communications with multiple unmanned off-board vehicles.
  - Hangars sized to embark MH-60R/S helicopters and the MQ-8 Fire Scout.
  - MK 110 57 mm gun.
- Both variants include ballistic protection for magazines and other vital spaces, such as, installed and portable damage control, firefighting, and dewatering systems intended to support recoverability
- The designs have different core combat systems to provide command and control, situational awareness, and self-defense against anti-ship cruise missiles (ASCMs) and surface craft.
  - *Freedom* variant: COMBATSS-21, an Aegis-based integrated combat weapons system with a TRS-3D (AN/SPS-75) air and surface search radar (ASR); a Rolling Airframe Missile (RAM) system; a Terma Soft Kill Weapon System; and a DORNA Electro-Optical Device (EOD) gunfire control system with an

electro-optical/infrared sensor to target the MK 110 57 mm gun. Starting with LCS 17, *Freedom*-variant ships will be fitted with a TRS-4D ASR and the MK 15 Mod 31 SeaRAM system as the air defense hard-kill weapon system. The Navy is also developing plans to retrofit earlier *Freedom* seaframes with SeaRAM in the 2020 to 2025 timeframe.

- *Independence* variant: Integrated Combat Management System derived from the TACTICOS system with a Sea Giraffe (AN/SPS-77) ASR; one MK 15 Mod 31 SeaRAM system; the Automatic Launch of Expendables (ALEX) system for decoy countermeasures; and the SAFIRE electro-optical/infrared sensor to target the 57 mm gun.

Mission Packages

- LCS is designed to host specific warfare area mission modules (MMs) assembled and integrated into interchangeable MPs. The Navy plans to install individual MCM, SUW, and anti-submarine warfare (ASW) MPs semi-permanently on the seaframes, dedicating specific ships to specific missions. Twenty-four of the planned 28 ships will be formed into 6 divisions with 3 divisions on each coast; *Independence* variants on the west coast and *Freedom* variants on the east coast. The Navy plans to use the first four ships as test platforms.
- The component MMs making up the MPs are:

MCM MP

- Near Surface Detection MM: one Airborne Laser Mine Detection System (ALMDS) unit for employment on the MH-60S multi-mission helicopter.
- Remote Minehunting (RMH) MM: two minehunting sonar units and one MCM Unmanned Surface Vehicle (USV) for minehunting capabilities. The Navy is considering the AN/AQS-20C and AN/AQS-24C minehunting sonar systems for use in the RMH MM. The AN/AQS-24C is an upgrade to the airborne MCM minehunting sonar that is in fleet use now. The Navy expects to use a variant of the Unmanned Influence Sweep System (UISS) surface craft in development as the MCM USV.
- Buried Minehunting MM: two battery-powered, autonomous, Knifefish Unmanned Undersea Vehicles, employing a low frequency, broadband, synthetic aperture sonar to detect and classify volume and bottom mines in shallow water.
- Coastal Mine Reconnaissance MM: one COBRA Block I, Block II, or Block III system for integration with the MQ-8 Fire Scout. This capability is intended for daytime unmanned aerial tactical reconnaissance to detect and localize mine lines and obstacles in the beach zone (Blocks I and II) and the surf zone (Block II). The Navy expects the Block II system to add improved beach zone detection capability against small mines and add nighttime capability. Block III is intended to detect buried mines in the beach zone and surf zone.
- Airborne Mine Neutralization MM: two Airborne Mine Neutralization Systems (AMNS) units for employment on the MH-60S multi-mission helicopter.
- Near Surface Neutralization MM (projected for FY23): the Barracuda Mine Neutralization System (MNS) should begin developmental testing in FY22, and if successful, augment AMNS in other portions of the water column. The Navy plans to deploy Barracuda from LCS using the MCM USV.
- Unmanned Minesweeping MM: one UISS composed of one MCM USV and sweep gear to detonate acoustic-, magnetic-, and combined acoustic/magnetic-initiated volume and bottom mines.
- Aviation MM: consists of one MH-60S multi-mission helicopter with the AMCM mission kit and one MQ-8B or MQ-8C Fire Scout.

SUW MP

- Increments 1 and 2 included:
  - Gun MM: two MK 46 30 mm guns
  - Aviation Module: embarked MH-60S Armed Helicopter Weapon System
  - Maritime Security Module: two 11-meter rigid-hull inflatable boats (RHIBs) with launch and recovery equipment
- Increment 3 will add:
  - Surface-to-Surface Missile Module, employing the AGM-114L-8A Longbow HELLFIRE missile modified for the maritime environment
  - One MQ-8 Fire Scout to augment the Aviation Module

ASW MP

- Torpedo Defense and Countermeasures Module: lightweight towed torpedo countermeasure
- ASW Escort Module: Multi-Function Towed Array (MFTA) and variable depth sonar (VDS) with AN/SQQ-89A(V)15 Surface Ship Undersea Warfare Combat System. MFTA and VDS are intended to provide submarine search, detection, localization, and track capability. MFTA is also intended to detect incoming torpedoes and be a catalyst for LCS torpedo evasion.
- Aviation Module: embarked MH-60R and an MQ-8 Fire Scout. MH-60R provides organic submarine prosecution capability using MK 54 torpedoes.

Mission

- The Maritime Component Commander will employ LCS to conduct MCM, ASW, or SUW tasks depending on the MP installed in the seaframe. Because of capabilities inherent to the seaframe, commanders can employ LCS in a maritime presence role in any configuration. With the Maritime Security Module, installed as part of the SUW MP, the ship can conduct Maritime Security Operations including Visit, Board, Search, and Seizure of ships suspected of transporting contraband.
- The Navy can employ LCS alone or in company with other ships. The Navy Concept of Operations (CONOPS)

anticipates LCS will prepare the environment for joint force assured access to critical littoral regions by conducting MCM, ASW, and SUW operations, possibly under an air defense umbrella. However, the latest CONOPS observes, "The most effective near-term operational roles for LCS to support the maritime strategy are theater security cooperation and maritime security operations supporting deterrence and maritime security."

Major Contractors

- *Freedom* variant
  - Prime: Lockheed Martin Maritime Systems and Sensors – Washington, District of Columbia
  - Shipbuilder: Marinette Marine – Marinette, Wisconsin
- *Independence* variant
  - Prime for LCS 2 and LCS 4: General Dynamics Marine Systems Bath Iron Works – Bath, Maine
  - Prime for LCS 6 and subsequent even-numbered ships: Austal USA – Mobile, Alabama
  - Shipbuilder: Austal USA – Mobile, Alabama
- MPs
  - MP Integration contract awarded to Northrop Grumman – Los Angeles, California
  - VDS: Raytheon Company – Waltham, Massachusetts

Activity

LCS Program

- The Navy plans to field warfighting capability in multiple increments of each MP have changed. The Navy now intends to field a single increment of the ASW MP and complete the SUW MP with the introduction of the Surface-to-Surface Missile Module in Increment 3. Plans for the MCM MP are uncertain following the Navy's cancellation of the Remote Minehunting System and the development of several other minehunting and mine neutralization systems.
- The Navy expects to complete operational testing of both LCS seaframe variants with the SUW Increment 3 MP in FY18 and with the ASW MPs in FY20.
- DOT&E approved an update to the LCS TEMP in March 2016. Since that time, the Navy and DOT&E worked on updates to the TEMP, including operational and integrated testing plans, changes to reflect the Navy's evolving plans to acquire and field the MCM MP, air defense testing of seaframes, and plans to test a seaframe over-the-horizon SUW missile capability. DOT&E expects to approve LCS Program TEMP Revision B in 2QFY18.
- In November 2016, DOT&E published a classified Early Fielding Report on the *Independence*-variant seaframe equipped with the Increment 2 SUW MP.
- In September 2017, DOT&E published the LCS 4 TSST Report. Shock trials on LCS 5 and LCS 6 occurred between June and September 2016 off the northeastern coast of Florida. DOT&E is awaiting Navy delivery of the LCS 5 and LCS 6 shock trial reports.

Seaframe

- The Navy has not conducted any air warfare test events against ASCM surrogates planned as part of the Enterprise Air Warfare Ship Self-Defense TEMP or the LCS TEMP. The Navy's Program Executive Office for Integrated Warfare Systems has halted all work to develop a Probability of Raid Annihilation (PRA) Modeling and Simulation (M&S) suite of the ships' combat systems for FY18. Delaying these efforts postpones evaluation of LCS air warfare capabilities.
- The Navy revised the LCS Capability Development Document in April 2017, moving the requirement for an Over-the-Horizon Weapon System (OTH-WS) from the SUW MP to the seaframe. The Navy is selecting a vendor for the OTH-WS, an ASCM for all LCS seaframes regardless of the installed MP. Source selection is expected in mid-FY18, with Initial Operational Capability scheduled for FY20.
- In August 2017, the USS *Coronado* (*Independence* variant) fired a Harpoon missile that hit a surface target beyond visual range. An MQ-8B Fire Scout and an MH-60S helicopter provided targeting for this live fire event.
- DOT&E reviewed the Navy draft Detail Design Survivability Assessment Report (DDSAR) for the *Freedom* variant. The Navy plans to release the final document in late CY17.

MCM MP

- The Navy continues to plan for the LCS MCM MP IOT&E scheduled in FY20. The Navy's CONOPS and tactics, techniques, and procedures for employment of the LCS MCM MP capability in the intended operational environments are unknown.
- In May 2017, the Navy completed the first of five planned phases of IOT&E for COBRA Block I. The testing focused on the operational effectiveness of the system to detect and classify mine lines, minefields, and obstacles on the beach. Fleet sailors operated the system from a shore base during this phase of IOT&E. The remaining LCS-based phases of IOT&E could not be completed in FY17 because of higher priority operational commitments for in-service LCS seaframes. The Navy conducted the testing in accordance with a DOT&E-approved test plan.
- In November 2017, the Navy completed AMNS medium current developmental testing.
- The Navy continued development of the UISS TEMP in FY17 and intends to submit it for DOT&E approval in FY18. The Navy continued development of the UISS, expects to complete contractor testing in 1QFY18. The

Navy intends to conduct UISS developmental testing during the rest of FY18, concluding with an operational assessment (OA) on LCS 2 in 1QFY19.
- The MCM USV, the intended UISS tow vehicle, began builder's trials in 1QFY18. The Navy plans to conduct LCS launch and recovery testing and sweep testing from LCS 2 in southern California in late 3QFY18.
- The Navy continued development of the mine-like Navy Instrumented Threat Target (NAVITTAR), a key test resource for future developmental and operational testing of UISS and a potential training asset for the fleet.
- Until the MCM USV becomes available for testing, the Navy intends to conduct AN/AQS-20C developmental testing using manned surface platforms in FY18. The Navy is still developing a test strategy and TEMP to document required RMH MM testing.
- The Knifefish completed contractor testing and began Factory Acceptance Testing in September 2017. Sea acceptance testing is expected to begin in 1QFY18. The Navy intends to conduct developmental testing in early 2QFY18, followed by an OA in mid-2QFY18. However, the DOT&E OA report will likely not be available to inform the Navy Milestone C decision, scheduled for late 2QFY18.

SUW MP
- The Navy conducted preliminary developmental tests of the Longbow HELLFIRE missile to include missile firings from a barge at moving targets and a structural test firing aboard a *Freedom*-variant LCS.

ASW MP
- The Navy conducted no at-sea testing of the ASW MP in FY17.
- In March 2017, the Navy awarded a contract to develop the VDS. The vendor's proposal uses a single towline to deploy both VDS and MFTA. The vendor intends to deliver a test article in late 2018.
- In September 2015, the Navy completed a formal study that identified capability gaps in currently available torpedo surrogates and presented an analysis of alternatives for specific investments to improve threat emulation capability. The Navy has since taken the following actions to address the identified capability gaps:
  - The Navy received approximately $1.4 Million through an FY16 Resource Enhancement Project (REP) proposal to develop a threat-representative, high-speed quiet propulsion system.
  - The Navy received approximately $6.2 Million through an FY17 REP proposal to develop a General Threat Torpedo (GTT). The GTT expands upon the high-speed quiet propulsion system by developing threat representative tactics and countermeasure logic.

Assessment

Seaframes
- DOT&E provided early fielding reports of the *Freedom* variant in December 2015 and the *Independence* variant in November 2016. The Navy did not conduct any additional testing or perform any modifications to either LCS seaframe variant in 2017 that would affect these assessments.
- The Navy commissioned LCS *Freedom* in 2008, and LCS *Independence* in 2010. Both LCS seaframes have limited anti-ship missile self-defense capability. The Navy has not fully tested these combat systems and the Navy does not plan to conduct further air warfare operational testing of *Freedom* seaframes 1 through 15 in their current combat system configuration. The Navy has accepted the risk of continued operation with a combat system that is not operationally tested. DOT&E cannot fully assess the operational effectiveness and suitability of the combat system aboard each variant without further testing.
- The Navy halted all work to develop a PRA M&S suite of LCS combat systems in FY15 because some combat system element models (e.g., radars) were not available. The lack of combat system element models persists. The Navy has not funded the development of the LCS PRA combat system M&S suite in FY18.
- The Navy delivered draft versions of the *Freedom*- and *Independence*-variant Detail Design Integrated Survivability Assessment Reports, which include a summary of TSST data, assessment of ship vulnerabilities to air and underwater threats, and assessment of their compliance with survivability requirements.
- Survivability testing and preliminary analyses on both LCS variants continue to demonstrate that neither LCS variant is survivable in high intensity combat. Although the ships incorporate capabilities to reduce their susceptibility to attack, testing of analogous capabilities in other ship classes demonstrated that such capabilities have limited effectiveness in high intensity combat. As designed, the LCS lacks redundancy and the vertical and longitudinal separation of vital equipment found in other combatants. These features are required to reduce the likelihood that a single hit will result in loss of propulsion, combat capability, and the ability to control damage and restore system operation.
- The final survivability assessment of the LCS variants is ongoing and is largely dependent on Navy delivery and quality of shock trial reports, completion of FY16 surrogate test reports, and the final survivability analysis runs.
- Based on the testing and analysis performed by the Navy to date, the DOT&E assessment of the survivability of both LCS variants is unchanged.

MCM MP
- The first phase of COBRA Block I IOT&E provided data to evaluate the effectiveness of the system to detect, classify, and localize mine lines, minefields, and obstacles on pure sand and on sand with beach vegetation. The COBRA Block I system performed reliably with few operational mission failures. However, both MQ-8B Fire Scout test platforms were not operationally available for several days during this IOT&E period. MQ-8B troubleshooting and repairs required significant maintenance support.

- The UISS must be survivable in the intended operating environment to repeatedly sweep and detonate mines. The Navy plans to test UISS mission survivability, prior to full-rate production, using underwater explosive testing of the operational system are uncertain. Without this testing, the Navy risks acquiring a minesweeping system with limited survivability against the threats it is intended to counter.
- The Navy is deciding whether the RMH MM, a core capability for the LCS MCM MP, will integrate the AN/AQS-20C or AN/AQS-24C minehunting sonar system with the MCM USV tow craft. The MCM USV is still under development, and must be further modified to serve as the tow craft in the RMH MM.
- Navy plans to develop, integrate, and test the RMH MM in the LCS MCM MP are not mature. A production-representative RMH MM is not expected to be available for test until the MP IOT&E and the Navy intends to operationally test RMH MM capability for the first time during the LCS MCM MP IOT&E scheduled in FY20. This testing strategy adds risk to successful completion of the LCS MCM MP IOT&E and delivery of its intended capability to the fleet.
- Despite having plans and funding to develop, integrate, and test multiple MM programs of record in the MCM MP, the Navy does not have approved CONOPS or tactics, techniques, and procedures to employ the family of MCM MP systems and capabilities to complete a combat mission. This information is essential for successful MP development, testing, and fleet employment.
- The slow pace of development, production, and validation of NAVITTAR, a mine like test resource, raises doubts as to whether accredited moored and bottom mine targets will be available in sufficient quantities to support planned operational testing of UISS in FY18.

SUW MP

- In December 2015, DOT&E issued a classified assessment of the *Freedom* variant with the Increment 2 SUW MP. The ship's mixed performance in live fire testing resulted in DOT&E deferring a determination of its effectiveness until the completion of Increment 3 SUW testing, scheduled for FY18. The Navy did not conduct any additional testing or perform any modifications to the seaframe and SUW MP in 2017 that would affect the 2015 assessment.
- In November 2016, DOT&E issued a classified assessment of the *Independence* variant with the Increment 2 SUW MP. The Navy did not conduct any additional testing or perform any modifications to the seaframe and SUW MP in 2017 that would affect the 2016 assessment.

ASW MP

- The observed operational availability of MFTAs in the fleet will reduce the percentage of time that LCS with the ASW MP is able to support the ASW mission. The MFTA is required for the LCS to conduct the ASW mission. Repair of a MFTA requires LCS to return to port to replace the MFTA with a spare. An effective ASW mission capability will depend on a logistics plan that includes pre-placement of MFTA spares in strategic locations and a tow design that supports replacement of the MFTA on the single VDS and MFTA towline.
- Current test surrogates have significant limitations representing threat torpedoes. Operational assessments of each LCS variant with the ASW MP using these test assets will not fully characterize the capability provided by an LCS to defeat incoming threat torpedoes. The Navy proposed development of a GTT addresses many shortfalls, but the capability to support realistic operational testing depends on future Navy decisions to procure a sufficient quantity of GTTs.

Recommendations

- Status of Previous Recommendations. The Navy has partially addressed one recommendation from the DOT&E FY16 Annual Report relating to MCM MP. DOT&E is not aware of any other actions taken by the Navy to address the recommendations relating to LCS seaframes, cybersecurity, and the MCM, SUW, and ASW MPs.
- FY17 Recommendations. The Navy should address the remaining FY16 recommendations and the following FY17 recommendations:

MCM MP

1. Complete the remaining COBRA Block I IOT&E phases that include LCS-based testing at sea and cybersecurity testing on LCS.
2. Fund and integrate the COBRA Block I system on a more robust and reliable platform to mitigate risks caused by poor MQ-8B Fire Scout operational reliability and availability observed during testing.
3. Complete the MCM MP CONOPS and the tactics, techniques, and procedures for employing the MCM MMs in expected combat environments.
4. Characterize RMH MM capabilities using the MCM USV and minehunting sonar in operational testing prior to conduct of the LCS MCM MP IOT&E.
5. Accelerate completion of development, production, and validation to support accreditation of NAVITTAR for use in planned UISS testing in FY18.
6. Fund and execute full system shock testing for the UISS prior to full-rate production to ensure the production-representative system is survivable in a combat environment.

ASW MP

7. Develop a logistics plan that includes pre-placement of MFTA spares in strategic location and ensure that the combined tow for the vertical depth sonar and MFTA supports replacement of the MFTA.

LFT&E

8. Address recommendations listed in the Navy and DOT&E LCS 4 TSST reports.

Future Operational Testing

9. Complete the air warfare testing of both seaframes, including development and execution of the LCS PRA testbed.

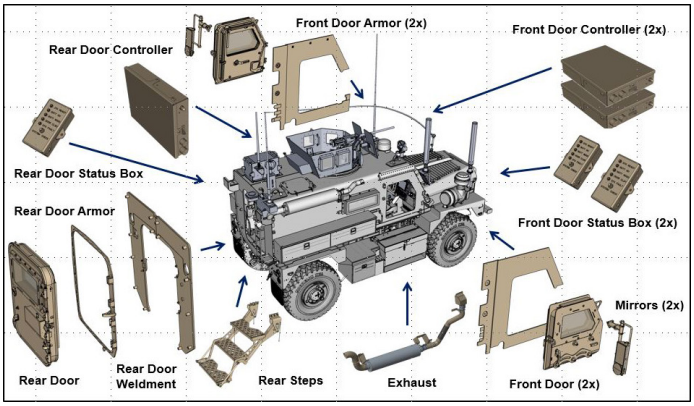
Mine Resistant Ambush Protected (MRAP) Family of Vehicles (FoV) Egress Upgrade – Marine Corps

Executive Summary

- The Marine Corps has made progress to retrofit all retained Mine Resistant Ambush Protected (MRAP) Cougar variants with egress upgrades to include power-assisted front and rear doors, redesigned rear steps, and a reconfigured exhaust system. These upgrades address crew egress deficiencies identified in Cougar live fire testing in FY16 and operational rollovers in Operation Enduring Freedom.
- In March 2017, the Marine Corps completed live fire testing of the Cougar MRAP upgraded with egress kits. The upgrades demonstrated improved ability of the crew to egress the vehicle post-attack as compared with the legacy system, while maintaining the required force protection and vehicle survivability performance.
- Automatic Fire Extinguishing System tests confirmed that the egress upgrades did not adversely affect the existing fire extinguishing performance.

System

- The MRAP Family of Vehicles (FoV) consists of medium-armored, all-wheel drive, tactical wheeled vehicles designed to provide protected mobility for soldiers and marines in a combat environment. Relative to the High Mobility Multi-purpose Wheeled Vehicle, MRAPs provide improved crew protection and vehicle survivability against IEDs, mines, small arms fire, rocket-propelled grenades, and explosively formed penetrators.
- The Marine Corps identified the need for an egress upgrade for its MRAP Cougar FoV through FY16 live fire testing and operational rollovers seen in Operation Enduring Freedom. The Marine Corps developed two Urgent User Needs Statements which were validated by the Marine Corps Requirements Oversight Council.



- The Marine Corps has made progress to retrofit all retained MRAP Cougar variants with egress upgrades. The egress upgrades for the category (CAT) I and II variants consist of new power-assisted front and rear doors, redesigned rear steps, and a reconfigured exhaust system. The Marine Corps funded design and production of 1,732 egress kits to be retrofitted on the MRAP Cougar enduring fleet. This purchase also includes kits for the Navy and Air Force.

Mission

Commanders will employ Marine units equipped with the MRAP Cougar to conduct mounted patrols, convoy protection, reconnaissance, communications, and command and control missions to support combat and stability operations in highly restricted rural, mountainous, and urban terrain.

Major Contractor

General Dynamics Land Systems – Ladson, South Carolina

Activity

- In March 2017, the Marine Corps Operational Test and Evaluation Activity (MCOTEA) completed the LFT&E of the Cougar MRAP upgraded with egress kits in accordance with the DOT&E-approved test plans.
- The test program, executed at Aberdeen Proving Ground, Maryland, included:
  - Developmental and system-level live fire testing to evaluate crew survivability and vehicle performance against underbody mine and side IED threats
  - Exploitation testing to identify vulnerabilities in the new door design against small arms and simulated fragments
  - Performance testing of the Automatic Fire Extinguishing System on the CAT I A1 and CAT II A1 variants.

Assessment

- The Cougar egress upgrade demonstrated improved door functionality following objective blast mine events as compared with the legacy system, increasing the ability of the crew to egress the vehicle, post-attack:
  - Live fire testing revealed door vulnerabilities in the initial design.
  - The Marine Corps mitigated the vulnerability by correcting the design deficiency, and demonstrated, through additional tests, the effectiveness of the system design changes.
- The Cougar egress upgrade did not adversely affect existing force protection and vehicle survivability performance; more specifically the Capability Production Document (CPD) 1.1

threshold-level protection for direct fire, indirect fire, and side IED threats and objective-level protection for underbody blast mines.
- The Cougar egress upgrade did not include any changes that adversely affected the effectiveness of the Automatic Fire Extinguisher System. The Automatic Fire Extinguishing System provided the required fire suppressant concentrations in the crew compartment.

Recommendations
- Status of Previous Recommendations. The program has addressed the previous recommendation regarding egress shortfalls identified in FY16.
- FY17 Recommendations. None

MK 54 Lightweight Torpedo and High-Altitude Anti-Submarine Warfare Capability (HAAWC)

Executive Summary

- The Navy continued development of hardware and software updates to the MK 54 Lightweight Torpedo. The new version, designated the MK 54 Mod 1 torpedo, is scheduled to begin OT&E in FY20.
- The Navy began MK 54 Mod 1 development in FY07 and started in-water developmental testing in November 2015. The Navy has shot 43 of the 84 MK 54 Mod 1 torpedoes in accordance with the developmental test plan. Testing is behind schedule due to poor weather, the loss of target services, and test torpedoes. The remainder of the developmental test events are planned for FY18 and FY19.
- The High-Altitude Anti-Submarine Warfare Weapons Capability (HAAWC) program, designed to deliver the MK 54 torpedo from the cruising altitude of a P-8A aircraft, completed initial contractor flight testing and is scheduled to complete safe separation testing of HAAWC from the P-8A in 2017. Initial integration testing began in 2016 and continued in 2017 with the first test release of a HAAWC from a P-8A planned for December 2017. The Navy has not approved a Test and Evaluation Master Plan (TEMP) for the HAAWC program. The Navy completed a HAAWC Milestone C acquisition decision in December 2017 without conducting an independent operational assessment.
- The LFT&E assessment of this weapon remains unchanged from 2016. The Navy should outline an evaluation plan that provides a more detailed assessment of the lethality criteria being used by the program.

System

- The MK 54 Lightweight Torpedo is the primary anti-submarine warfare (ASW) weapon used by U.S. surface ships, fixed-wing aircraft, and helicopters. The MK 54 must be compatible with analog or digital combat control systems and software variants installed on all ASW fixed- and rotary-wing aircraft and on surface ship combat control system variants used for torpedo tube or ASW rocket-launched torpedoes.
- The MK 54 combines the advanced sonar transceiver of the MK 50 torpedo with the legacy warhead and propulsion system of the older MK 46. MK 46 and MK 50 torpedoes are converted to an MK 54 via an upgrade kit.
- The Navy designed the MK 54 to operate in shallow-water environments and in the presence of countermeasures. The MK 54 sonar processing uses an expandable, open architecture system. It combines algorithms from the MK 50 and MK 48 torpedo programs with commercial off-the-shelf technology.
- The Navy has designated the MK 54 torpedo to replace the MK 46 torpedo as the payload section for the Vertical Launched Anti-Submarine Rocket for rapid employment by surface ships.

- The MK 54 Block Upgrade (BU) was a software upgrade to the MK 54 baseline torpedo designed to provide a small, shallow draft target capability and to correct deficiencies identified during the 2004 MK 54 IOT&E.
- The Navy is developing the MK 54 Mod 1. The MK 54 Mod 1 hardware upgrades the torpedo's sonar array from 52 to 112 elements, providing higher resolution. Associated software upgrades are designed to exploit these features to improve target detection, enhance false target rejection, and correct previously identified deficiencies.
- The HAAWC marries an adapter wing-kit to an MK 54 torpedo to allow long-range, high-altitude, GPS-guided deployment of the MK 54 by a P-8A Multi-mission Maritime Aircraft. A follow-on capability to receive in-flight targeting updates via Link 16 from the P-8A may be added in a later program phase. In-flight updates will not be available in the baseline HAAWC kit.

Mission

Commanders employ naval surface ships and aircraft equipped with the MK 54 torpedo to conduct ASW:

- For offensive purposes, when deployed by ASW aircraft and helicopters
- For defensive purposes, when deployed by surface ships
- In both deep-water open ocean and shallow-water littoral environments

- Against fast, deep-diving nuclear submarines and slow-moving, quiet, diesel-electric submarines

Major Contractors
- Raytheon Integrated Defense Systems – Tewksbury, Massachusetts
- Progeny Systems Corporation – Manassas, Virginia
- Boeing Company – St. Charles, Missouri
- Northrop Grumman – Annapolis, Maryland

Activity

MK 54 Mod 1
- During FY17, the Navy continued development of new MK 54 Mod 1 torpedo sonar section hardware and tactical software to address the performance shortfalls identified in the MK 54 (BU). The Navy plans to begin OT&E of the MK 54 Mod 1 in FY20.
- The Navy began MK 54 Mod 1 development in FY07 and started in-water developmental testing in November 2015. The Navy's developmental test plan calls for shooting 84 MK 54 Mod 1 torpedoes in 6 separate test events covering both deep- and shallow-water scenarios. The Navy only shot 43 torpedoes and is behind schedule due to poor weather and the loss of target services and test torpedoes. The Navy intends to complete the remainder of the developmental test events in FY18 and FY19. The Navy completed the following MK 54 Mod 1 developmental testing in FY17:
  - Four of four planned MK 54 Mod 1 events in shallow and deep water in October 2016.
  - Four of nine planned shallow-water test events in December 2016. The Navy halted testing due to poor weather.
  - Four of 10 planned shallow- and deep-water test events in April 2017. The Navy halted testing due to poor weather.
  - The six events delayed from April 2017 in June 2017. During the test, the Navy did not recover one test torpedo.
  - Nine of nine planned shallow-water test events in July 2017.
- The Navy completed a Milestone C acquisition decision in February 2016 for the MK 54 Mod 1 without an approved TEMP. The Navy approved the MK 54 Mod 1 Capability Development Document on September 26, 2016. The Navy approved the HAAWC requirements in a capability production document in June 2017. In FY17, the Program Office made progress in developing the MK 54 Mod 1 and the HAAWC TEMPs; however, neither document is ready for approval.
- In August 2017, the Navy intended to conduct a Surface Weapons Test (SWT) to test the MK 54 safety, arming device fuzing, and warhead reliability. Due to a series of target acoustic source failures, the Navy canceled the SWT.
- In FY17, DOT&E participated in two Resource Enhancement Program projects to develop critical assets for torpedo operational testing. One project develops the Submarine Launched Modular 3-inch Device (SLAM-3D) as a threat-representative surrogate torpedo countermeasure. The second project is an update to the Weapons Assessment Facility (WAF) hardware-in-the-loop modeling and simulation testbed located at the Naval Undersea Warfare Center in Newport, Rhode Island. The Navy intends for the project to improve the WAF for developing and testing torpedoes by improving target models and modeling of the ocean environment.
- In September 2015, the Navy conducted small-scale testing to characterize the warhead as a function of weapon standoff. The Navy delivered the final report in July 2017. In late FY16, the Navy conduced scaled warhead testing to assess the lethality of this weapon against operationally representative targets.

HAAWC
- In October and December 2016, Boeing continued contractor testing of HAAWC wing kits on a surrogate aircraft at Eglin AFB. In October 2016, the Navy started P-8A/HAAWC integration testing with P-8A ground and captive carriage flight tests to collect data from the P-8A weapons systems and evaluate the operator machine interface. The Navy continued integration testing and safe separation testing of the HAAWC on the P-8A aircraft in FY17. Safe separation testing is scheduled for completion in December 2017.
- In March 2017, the Navy's Commander Patrol and Reconnaissance Group canceled and withdrew the endorsement for the Navy's P-8A High-Altitude ASW Concept of Operations.
- The Navy is planning the first MK 54 HAAWC All-Up-Round (AUR) test from a P-8A in December 2017. During this developmental test, the Navy plans to launch four HAAWC AURs with Ballistic Air Test Vehicles (BATV). The Navy completed a HAAWC Milestone C acquisition decision in December 2017 without conducting an independent operational assessment. Integrated testing is planned for summer 2018, when the Navy plans to test in the final software configuration with a mix of HAAWC AURs with MK 54 Mod 0 exercise torpedoes and BATVs. Operational testing is planned for FY19.

Assessment
- In FY14, DOT&E assessed that the MK 54 (BU) torpedo is not operationally effective as an offensive ASW weapon.

- Some MK 54 (BU) operationally realistic scenarios were not assessed in previous testing due to the unavailability of target surrogates and the Navy's safety regulations for shooting against manned submarine targets. Due to resource constraints, the Navy has not developed adequate set-to-hit surrogate targets. Because of these test limitations, the Navy cannot adequately assess all components of the MK 54 Mod 1 kill chain. The Navy plans to conduct set-not-to-hit testing with manned submarines and limited set-to-hit testing with available static target surrogates to assess if the MK 54 Mod 1 improves performance and corrects MK 54 (BU) shortfalls. Despite test limitations, the Navy may be able to estimate an upper bound of MK 54 performance, but the test will not resolve performance knowledge gaps identified in previous testing for many operationally realistic scenarios.
- Completed developmental testing of the MK 54 Mod 1 demonstrated performance results similar to the MK 54 (BU); however, to date, the Navy has conducted most developmental testing using simple scenarios where the MK 54 previously demonstrated satisfactory performance. These simple developmental test scenarios are good regression testing that yield significant recorded test data; however, little data were obtained to assess MK 54 performance in challenging, operationally realistic scenarios. The Navy is planning additional in-water developmental testing to assess more challenging operational scenarios.
- The LFT&E assessment of this weapon remains unchanged from 2016.

Recommendations

- Status of Previous Recommendations. The following previous recommendations remain outstanding. The Navy should still:
  1. Conduct operationally realistic mobile target set-to-hit testing and minimize test limitations. The Navy has not developed a mobile target surrogate for set-to-hit testing. The Navy investigated possible surrogates, but the proposals are unfunded. The Navy should fund efforts to minimize these test limitations.
  2. Propose alternatives to minimize or eliminate the test and safety limitations that minimize operational realism in MK 54 testing.
  3. Complete development of the MK 54 Mod 1 TEMP.
  4. Evaluate and incorporate the 11 recommendations in the DOT&E MK 54 (BU) OT&E report to improve the effectiveness of the MK 54. Significant unclassified recommendations include:
     - Improve the target detection, localization, and track performance of ship and aircraft crews that employ the MK 54. While improving the sensor system capability on ships and aircraft is a longer range goal, updating the MK 54 employment tactics, training, and documentation could immediately improve overall crew proficiency and ASW effectiveness. The Navy has reported it has made progress in updating its tactics and documentation, but there has been no testing yet to verify the deficiencies have been resolved.
     - Improve the MK 54's effective target search and detection capability. The MK 54 should be able to effectively search the area defined by typical fire control solution accuracy, crew employment, and placement errors.
     - Reduce the complexity of the MK 54 employment options and required water entry points in existing tactical documentation. The Navy has reported it has made progress in updating its tactics and documentation, but there has been no testing yet to verify the deficiencies have been resolved.
  5. Complete the development and approval of HAAWC TEMP.
  6. Utilize developmental test scenarios that stress the MK 54 Mod 1 in scenarios where improvements are desired. When possible, these scenarios should be operationally realistic.
- FY17 Recommendation.
  1. The Navy should outline an evaluation plan that provides a more detailed assessment of the lethality criteria being used by the program.

MQ-4C Triton Unmanned Aircraft System

Executive Summary
The Navy updated and DOT&E approved the MQ-4C Triton Unmanned Aircraft System (UAS) Test and Evaluation Master Plan (TEMP) in January 2017 following instruction given in the August 2016 Milestone C Acquisition Decision Memorandum. The update reflects the realignment of the program's Acquisition Strategy with the development and fielding of the Multiple Intelligence (Multi-INT) configuration.

System
- The MQ-4C Triton is an intelligence, surveillance, and reconnaissance (ISR) UAS consisting of the high-altitude, long-endurance MQ-4C air vehicle; sensor payloads; and supporting ground control stations. The MQ-4C system is a part of the Navy Maritime Patrol and Reconnaissance family of systems with capabilities designed to complement the P-8A Poseidon Multi-mission Maritime Patrol aircraft. It will provide ISR data on maritime and land targets over wide areas of the open ocean and littorals.
- The MQ-4C air vehicle design is based on the Air Force RQ-4B Global Hawk air vehicle with significant modifications that include strengthened wing structures and an anti-ice and de-icing system.
- The Navy intends to establish an Early Operational Capability with the baseline configuration. Mission systems include a maritime surveillance radar to detect, classify, and track surface targets; an electro-optical/infrared (EO/IR) full motion video sensor; electronic support measures to detect, identify, and geolocate threat radars; and an Automatic Identification System (AIS) receiver to collect AIS broadcasts from cooperative maritime vessels.
- The Multi-INT configuration will support Initial Operational Capability (IOC). The Multi-INT configuration provides a signals intelligence capability, and includes sensors, supporting software and hardware, and changes to permit processing of Top Secret and Sensitive Compartmented Information. The Navy intends for the MQ-4C Multi-INT configuration to replace the EP-3 Aries II aircraft for most missions.
- Onboard line-of-sight and beyond line-of-sight communications systems provide air vehicle command and control and transmit sensor data from the air vehicle to ground control stations for dissemination to fleet tactical operation centers and intelligence exploitation sites.
- Future system upgrades planned for after IOC include an air traffic collision avoidance radar system.

Mission
- Commanders employ units equipped with MQ-4C to conduct long-endurance maritime surveillance operations and provide high- and medium-altitude intelligence collection.
  - MQ-4C operators will detect, classify, identify, track, and assess maritime and littoral targets of interest and collect imagery and signals intelligence information.
  - Operators disseminate sensor data to fleet units to support a wide range of maritime missions to include surface warfare, intelligence operations, strike warfare, maritime interdiction, amphibious warfare, homeland defense, and search and rescue.

Major Contractor
Northrop Grumman Aerospace Systems, Battle Management and Engagement Systems Division – Rancho Bernardo, California

Activity
- The Navy updated and DOT&E approved the MQ-4C TEMP in January 2017 following instruction given in the August 2016 Milestone C Acquisition Decision Memorandum. The update reflects the realignment of the program's Acquisition Strategy with the development and fielding of the Multi-INT configuration. As part of the realignment, the program has moved IOT&E from 4QFY17 to 2QFY21.
- The Navy plans to conduct an operational assessment (OA) of the MQ-4C Multi-INT configuration in 3QFY20 to support a Multi-INT Early Operational Capability in 4QFY20.

- The Navy plans to conduct an OA of the baseline configuration in FY18 to support early fielding of two MQ-4C aircraft in FY18.

Assessment

- In general, the system demonstrated positive trends for sensor performance and reliability during the FY16 OA supporting the Milestone C decision. However, the OA revealed deficiencies in the following areas: lack of Due Regard capability (capability to independently maintain prescribed minimum separation distances); poor EO/IR sensor control; poor Electronic Support Measures Interface; and difficulty managing the temperature of the radar. DOT&E's classified OA report, dated May 2016, provides specific information on these and other aspects of the assessment.
- The Due Regard capability provides critical mission capability for operation of the MQ-4C in civil and international airspace in support of global naval operations. Any limitation to this capability at IOT&E will reduce the effectiveness of the MQ-4C.

Recommendations

- Status of Previous Recommendations. The Navy still needs to address the following recommendations:
  1. Demonstrate any alternative means of compliance with the Due Regard requirement prior to IOT&E and conduct a Cooperative Vulnerability and Penetration Assessment (CVPA) sufficiently in advance of the Adversarial Assessment (AA) to allow the program to correct any discovered cybersecurity vulnerabilities.
  2. Conduct both the CVPA and AA prior to any early fielding of the MQ-4C.
  3. Resolve deficiencies documented in the DOT&E OA report prior to IOT&E, especially in the following areas: Due Regard capability; EO/IR sensor control; Electronic Support Measures Interface; and temperature management of the radar.
- FY17 Recommendations. None.

Navy Multiband Terminal (NMT)

Executive Summary

- The Navy's Operational Test and Evaluation Force (OPTEVFOR) planned an FOT&E from May 9 through June 8, 2016, but was unable to execute the test due to the Navy's conflicting operational requirements.
- In November 2016, the Navy Multiband Terminal (NMT) program manager and OPTEVFOR proposed a modified T&E approach to use available data from previous operational tests and conduct smaller, targeted test events as Navy shore, ship, and submarine assets became available.
- The Navy's FY16 and FY17 operational testing was adequate to determine the NMT is operationally effective and suitable in providing Advanced Extremely High Frequency (AEHF) satellite communications (SATCOM) to Navy shore sites, ships, and submarines in a non-contested-threat environment. The Navy Anti-Jam (AJ) and Low Probability of Intercept (LPI) testing was inadequate and the Navy still needs to perform threat testing to understand the NMT's performance in a contested environment.
- Based on the cyber-testing, the NMT is secure and isolated, limiting an adversary's attack options to gain access to the system.

System

- The NMT system is the next-generation maritime military SATCOM terminal for the Navy and its coalition partners; the Navy uses it for accessing protected and survivable SATCOM over the AEHF SATCOM constellation. In addition, NMT provides access to wideband communications through the Defense Satellite Communications System (DSCS) and Wideband Global SATCOM (WGS) constellations.
- The NMT is interoperable with the current and legacy service SATCOM terminals, including the Family of Advanced Beyond-line-of-sight Terminals, Secure Mobile Anti-jam Reliable Tactical Terminal, and the Follow-on Terminal.
- The program manager developed NMT variants for surface ships, submarines, and shore sites. The NMT system variants have two major component groups: the Communications Group and the Antenna Group.

Antenna Group

Communications Group

- The Communications Group provides the interface for all input/output devices, signal processing, timing, frequency generation, and antenna pointing control. The Communications Group consists of the following components:
  - Operator User Interface
  - Power Distribution Unit
  - Keyboard
  - EHF and Wideband drawers
  - Prime Power Interface
- The Antenna Group varies across different platforms and includes new, reused, and modified antennas to support the required Q- and Ka-Bands, as well as X-band with the Global Broadcast Service. The shore and ship Antenna Group provides antenna pointing, stabilization, and tracking.

Mission

The Navy Component Commander uses the NMT to provide secure, protected, and survivable connectivity across the spectrum of mission areas including land, air, and naval warfare; special operations; strategic nuclear operations; strategic defense; theater missile defense; and space operations and intelligence.

Major Contractor

Raytheon Net-Centric Systems – Marlboro, Massachusetts

Activity

- The Johns Hopkins Applied Physics Laboratory conducted an assessment of the NMT AJ and LPI capability primarily through modeling and simulation with supporting live test results using the USS *Cole* (DDG 67) in December 2013.
- DOT&E and OPTEVFOR determined the AJ and LPI modeling and simulation could not be accredited for OT&E use. The Navy deferred retesting the NMT's AJ and LPI capability until it can get funds in place to improve the model and simulation.
- The Navy program manager and OPTEVFOR conducted developmental and integrated testing aboard the USS *Wasp* (LHD 1), the USS *Mason* (DDG 87), USS *Helena* (SSN 725), and the Navy Computer and Telecommunications Area Master Station – Atlantic (NCTAMS LANT) from February 8 through March 4, 2016.
- OPTEVFOR planned an FOT&E from May 9 through June 8, 2016, but was unable to execute the test in accordance

with the DOT&E-approved test plan due to the Navy's conflicting operational requirements.
- The OPTEVFOR cybersecurity team supported by the Navy Information Operations Command conducted an NMT cybersecurity assessment in June 2016 at NCTAMS LANT in Norfolk, Virginia. The Navy cyber-team collected all DOT&E-required data.
- OPTEVFOR replanned the FOT&E for 4QFY16, but was again unable to obtain the necessary shore and ship types for a single test event, as originally planned.
- In November 2016, the NMT program manager and OPTEVFOR proposed a modified T&E approach to use available data from previous operational tests and conduct smaller, targeted test events as Navy shore, ship, and submarine assets became available.
- In February 2017, OPTEVFOR and the Joint Terminal Engineering Office jointly conducted NMT surface ship testing aboard the USS *Jason Dunham* (DDG 109) and the USS *Forrest Sherman* (DDG 98) passing mission data updates and tactical chat messaging.
- OPTEVFOR conducted NMT sub-surface testing in June 2017 by performing mission communications between the Commander, Submarine Force U. S. Pacific Fleet and the USS *Columbia* (SSN 771).
- OPTEVFOR performed further operational testing aboard the USS *Chung-Hoon* (DDG 93) from August 14-25, 2017, to collect data communication completion and latency metrics.

Assessment
- The Navy's operational testing was adequate to determine the NMT is operationally effective and suitable in providing AEHF communications to Navy shore sites, ships, and submarines in a non-contested-threat environment.
- The Navy AJ and LPI testing was inadequate and threat testing still needs to be performed to understand the NMT's performance in a contested environment.
- DOT&E and OPTEVFOR determined the AJ and LPI modeling and simulation could not be accredited for OT&E use. The Navy provided insufficient evidence that the Johns Hopkins Applied Physics Laboratory threat surrogate is sufficiently representative of valid threats and the comparison of live data to the model's predictions lacked credible statistical analysis.
- Based on the cyber-testing, the NMT is secure and isolated, limiting an adversary's attack options to gain access to the system
- The Air Force Operational Test and Evaluation Center with OPTEVFOR are planning to test NMT in the Air Force-led Enhanced Polar System Multi-Service Operational Test and Evaluation (MOT&E) in 3QFY18.

Recommendations
- Status of Previous Recommendations. The Navy has made satisfactory progress on all previous recommendations.
- FY17 Recommendation.
  1. The Navy should adequately test the NMT AJ and LPI capability in a future operational test event.

Offensive Anti-Surface Warfare (OASuW) Increment 1

Executive Summary
- The Navy plans to complete a Quick Reaction Assessment (QRA) of the Offensive Anti-Surface Warfare (OASuW) Increment 1 program for weapon employment on the B-1B aircraft in FY18 and the F/A-18E/F aircraft in FY19.
- The OASuW Increment 1 program conducted limited testing in FY17 with partially successful results. Modeling and simulation (M&S) performance is at risk with more details available at higher classification.
- The Integrated Test Event-1 (ITE-1) Long Range Anti-Ship Missile (LRASM), employed from a B-1B aircraft, successfully engaged the mobile ship target.

System
- The OASuW Increment 1 program is the first program in an incremental approach to produce an OASuW capability in response to a U.S. Pacific Fleet Urgent Operational Need generated in 2008.
- The OASuW Increment 1 is an accelerated acquisition program to procure a limited number of air-launched missiles to meet a near-term U.S. Pacific Fleet capability gap in 2018 by leveraging the Defense Advanced Research Projects Agency (DARPA) LRASM.
- LRASM, the weapon system for the OASuW Increment 1, is a 2,400-pound, long-range, conventional, air-to-surface, precision standoff missile. The Navy's F/A-18E/F or the Air Force's B-1B aircraft will launch LRASM.
- LRASM, designated the AGM-158C, is derived from the Joint Air-to-Surface Standoff Missile Extended Range (JASSM-ER) and will use the same 1,000-pound penetrator/blast fragmentation warhead and anti-jam GPS guidance system as JASSM-ER. Additionally, LRASM incorporates a radio frequency sensor (RFS) to guide to the target and an infrared (IR) seeker to locate specific aim points on the target.
- The launch platform(s) will launch LRASM against a target ship. LRASM will guide towards an initial target cue provided to the missile by the launch platform until the RFS identifies and locates the target ship. The missile will then home on the target ship until the IR seeker is able to detect and track the target. The IR seeker will provide terminal guidance to the selected aimpoint on the ship. LRASM is designed to operate individually or as part of a salvo.
- The Navy plans to pursue a competitive acquisition strategy for the OASuW Increment 2, which is intended to be an offensive system of systems solution leveraging OASuW Increment 1 technologies to meet future maritime threats beyond 2024. Due to removal of funding for Increment 2 in the 2018 President's Budget, the Navy is reevaluating its strategy for OASuW Increment 2.

Mission
Combatant Commanders will use units equipped with LRASM to destroy high-value, well-defended ships from standoff ranges.

Major Contractor
Lockheed Martin Missiles and Fire Control – Orlando, Florida

Activity
- DOT&E approved the Navy's test plan in August 2017 as adequate to assess QRA performance; however, DOT&E also directed the Navy to provide a detailed M&S accreditation plan and cybersecurity test plan for DOT&E review and approval.
- The Navy began flight testing and end-to-end M&S runs of the LRASM system in FY17.
- In FY16, the Navy completed the four planned Missile Avionics Suite (MAS) test events. MAS testing incorporated a helicopter-mounted IR seeker and Mission Control Unit (MCU) to facilitate IR seeker algorithm development and data collection to support M&S development.
- The Navy completed the last two Flying Test Bed (FTB) events in FY17 for a total of 54 test runs of the RFS, IR seeker, and MCU mounted in a Sabreliner 65 aircraft. The FTB testing will be used for technology maturation and in-flight data collection to support M&S activities.
- The Air Force completed two captive carry events on a B-1B aircraft to evaluate weapon integration, with a third planned for FY18.

- The Navy completed ntegrated modeling test event-1 (ITEM-1), which is the first end-to-end M&S test of the Kill Chain Testbed (KCT).
- The Navy and Air Force conducted the first free flight test of LRASM during ITE-1.
- In FY16, the Navy completed the sled tests to demonstrate the required warhead fuze delay and to assess the penetration and behavior of the weapon against intended ship targets. Analysis is ongoing to characterize the damage to the target as a function of weapon hit location.
- The Navy and Air Force conducted all testing in accordance with the DOT&E-approved Master Test Strategy.
- The Navy plans to complete a QRA of the OASuW Increment 1 program and declare Early Operational Capability (EOC) for weapon employment on the B-1B aircraft in FY18 and the F/A-18 aircraft in FY19. DOT&E will deliver an Early Fielding Report on both EOC decisions.

Assessment

- The OASuW Increment 1 program conducted limited testing in FY17, including the recent ITE-1 free flight test. All testing was done in accordance with the DOT&E-approved test plan and with partially successful results.
- Sled tests confirmed satisfactory interaction between the missile and the ship structure, including proper warhead fusing. A more detailed assessment of weapons effects and residual target mission capability will be provided after the completion of the lethality analysis in FY18.
- M&S goals for EOC are currently at risk due to difficulties in correctly modeling RFS performance and incomplete plan for accreditation. M&S outcomes will validate Key Performance Parameter achievement in this program. Further details are classified.
- The ITE-1 LRASM, employed from a B-1B aircraft, successfully engaged the mobile ship target.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY17 Recommendation.
  1. The Navy should accomplish cybersecurity testing of the weapon system in accordance with a DOT&E-approved cybersecurity test plan prior to EOC.

P-8A Poseidon Multi-Mission Maritime Aircraft (MMA)

Executive Summary

- The P-8A Engineering Change Proposal (ECP) 2 OT&E began in November 2016. Test events and data analysis are expected to continue through December 2017. Pending final DOT&E data analysis, preliminary test results indicate significant improvement in intelligence, surveillance, and reconnaissance (ISR) mission capabilities and successful integration of AGM-84D Block 1 advanced surface warfare (SUW) employment modes. Demonstrated P-8A air-to-air refueling capabilities support initial operational training and employment. P-8A Multi-static Active Coherent (MAC) sensor wide-area anti-submarine warfare (ASW) search test results are inconclusive because only 6 of 24 planned test events were accomplished, mainly due to lack of submarine target availability. DOT&E reviewed and approved a revised Navy proposal to complete P-8A MAC test events in future operational test periods.
- The Navy did not complete P-8A Increment 3 Test and Evaluation Master Plan (TEMP) development in FY17 due to program delays, budget uncertainty, and P-8A Increment 2 program delays. However, the Navy did complete detailed operational test plans for near-term Increment 3 ECP 4 and ECP 5 OT&E events in FY18 and FY19. These plans are adequate to evaluate initial Increment 3 capabilities. P-8A ECP 6 and ECP 7 detailed test strategy and TEMP development were deferred until final system operational requirements and capabilities are defined prior to the planned system critical design review in FY19.
- In FY17, the Navy initiated a re-evaluation of proposed high-altitude ASW operational concepts and requirements. Demonstration of an initial high-altitude sonobuoy employment capability is planned during the FY18 P-8A ECP 4 operational test event. High-Altitude ASW Weapon Capability (HAAWC) MK 54 torpedo developmental testing continued to progress in FY17. The Navy is scheduled to begin P-8A integration testing in FY18 leading to operational testing of the HAAWC system on the P-8A in FY19.
- In FY17, the Navy completed landing gear fatigue test assembly data analysis with no significant findings. Teardown of the full-scale aircraft fatigue test article will occur when all extended life test events are complete in January 2018. The program continues to review the full-scale test article data to refine fleet airframe inspection requirements and depot repair procedures to ensure the airframe meets the intended 25-year design life. To date, no significant long-term structural problems have been identified.

System

- The P-8A Poseidon Multi-mission Maritime Aircraft (MMA) design is based on the Boeing 737-800 aircraft with significant modifications to support Navy maritime patrol mission requirements. It is replacing the P-3C Orion.
- The P-8A incorporates an integrated sensor suite that includes radar, electro-optical, and electronic signal detection sensors to provide search, detection, location, tracking, and targeting capability against surface targets. An integrated acoustic sonobuoy launch and monitoring system provides search, detection, location, tracking, and targeting capability against submarine targets. Sensor systems also provide tactical situational awareness information for dissemination to fleet forces and ISR information for exploitation by the joint intelligence community.
- The P-8A carries MK 54 torpedoes and the AGM-84D Block 1C Harpoon anti-ship missile system to engage submarine and maritime surface targets.
- The P-8A aircraft incorporates aircraft survivability enhancement and vulnerability reduction systems. An integrated infrared missile detection system, flare dispenser, and directed infrared countermeasure system is designed to improve survivability against infrared missile threats. On- and off-board sensors and datalink systems are used to improve tactical situational awareness of expected threat systems. Fuel tank inerting and fire protection systems reduce aircraft vulnerability.
- The Navy is integrating the MAC sensor system into the P-8A to provide a wide-area, active ASW search capability.
- Planned future upgrades include the addition of the HAAWC MK 54 torpedo, AGM 84 Harpoon II+, MAC wide-area ASW search enhancements, signals intelligence sensors, and advanced mission system architectures and processing upgrades.

Mission

- Theater Commanders primarily use units equipped with the P-8A MMA to conduct ASW operations including the detection, localization, tracking, and destruction of submarine targets.
- Additional P-8A maritime patrol missions include:
  - SUW operations to detect, identify, track, and destroy enemy surface combatants or other maritime targets
  - ISR operations to collect and disseminate imagery and signals information for exploitation by the joint intelligence community
  - Command, control, and communication (C3) operations to collect and disseminate tactical situation information to fleet forces
  - Identification and precise geolocation of targets ashore to support fleet strike warfare missions

Major Contractor

Boeing Defense, Space, and Security – St. Louis, Missouri

Activity

- The P-8A ECP 2 OT&E, originally planned for early FY16, began in November 2016 following delays due to ASW software deficiencies discovered in developmental testing. P-8A ECP 2 OT&E events and data analysis are expected to continue through December 2017. This operational test includes evaluation of:
  - P-8A wide-area ASW search capability with the MAC sensor system
  - P-8A ISR mission capabilities following system improvements to address previous operational test failures
  - A system-level cybersecurity assessment
  - Air-to-air refueling capabilities
  - Advanced AGM-84 Block 1C Harpoon missile employment modes
  - Communication system enhancements
  - Operational availability with a fully mature logistics support system
  - Corrective actions for at least 37 significant operational deficiencies identified during previous test periods
- In April 2016, USD(AT&L) approved a revised Navy P-8A acquisition strategy that incorporated all P-8A Increment 3 capability requirements into the baseline P-8A program. These capabilities will now be developed and delivered as a series of ECPs (4 through 7). P-8A ECP 4 and ECP 5 are limited to software-based improvements to the P-8 AN/APY-10 radar, AGM-84D Block 2+ anti-ship missile integration, and communication system enhancements.
- The Navy did not complete P-8A Increment 3 (ECP 4 through 7) TEMP development in FY17 due to program delays, budget uncertainty, and P-8A Increment 2 program delays. However, the Navy did complete detailed operational test plans for near-term ECP 4 and ECP 5 OT&E events in FY18 and FY19. P-8A ECP 6 and ECP 7 TEMP and test design development was deferred until final system operational requirements and capabilities are defined prior to the planned system critical design review in FY19.
- The Navy continues to plan and progressively execute the P-8A MAC wide-area ASW search operational test events as defined in the 2013 P-8A TEMP. Some P-8A MAC test events were conducted in conjunction with the P-8A ECP 2 OT&E period. Future P-8A MAC test events are planned for the ECP 4, ECP 5, and ECP 7 operational test periods. Additional dedicated P-8A MAC test events may also be conducted as appropriate submarine targets become available.
- In FY17, the Navy initiated a re-evaluation of proposed high-altitude ASW operational concepts and requirements. HAAWC MK 54 torpedo system developmental testing continued to progress in FY17. Demonstration of an initial high-altitude sonobuoy employment capability is planned during the FY18 P-8A ECP 4 operational test event. Following a review of operational concepts and requirements, P-8A integration testing is scheduled to begin in FY18 leading to operational testing of the HAAWC MK 54 torpedo system on the P-8A in FY19.
- The Navy completed the distributed load, extended lifetime of fatigue and durability testing on P-8A full-scale test aircraft and is continuing extended lifetime testing. Full-scale aircraft testing is expected to be complete in January 2018 followed by teardown and final data analysis. The horizontal stabilizer subsystem completed three lifetimes of fatigue testing in FY17. Final teardown and data analysis for this subsystem is in progress.

Assessment

- Pending final DOT&E data analysis, preliminary P-8A ECP 2 test results indicate significant improvement in ISR mission capabilities and successful integration of AGM-84D Block 1 advanced employment modes. Demonstrated P-8A air-to-air refueling capabilities support initial operational training and employment. P-8A MAC ASW wide-area search test results were inconclusive because only 6 of 24 planned test events were accomplished, mainly due to lack of submarine target availability. DOT&E reviewed and approved a revised Navy proposal to complete P-8A MAC test events in future operational test periods.
- The plans for near-term P-8A Increment 3 ECP 4 and ECP 5 OT&E events are adequate to evaluate initial Increment 3 capabilities. These tests are on track to begin as scheduled in early FY 18.
- Operational testing of the emerging P-8A high-altitude ASW capability, including the HAAWC MK 54 torpedo system, is currently planned for FY19. However, the lack of clear

Navy high-altitude ASW concept of operations has delayed development of employment tactics and operational test plans.
- In FY17, the Navy completed landing gear fatigue test assembly data analysis with no significant findings. Teardown of the full-scale aircraft fatigue test article will occur when all extended life test events are complete in January 2018. The program continues to review the full-scale test article data to refine fleet airframe inspection requirements and depot repair procedures to ensure the airframe meets the intended 25-year design life. To date, no significant long-term structural problems have been identified.

Recommendations
- Status of Previous Recommendations. The Navy made progress on two of three FY16 recommendations. Corrective actions were implemented for at least 37 of 106 operationally significant system deficiencies identified in previous P-8A operational test reports. A more comprehensive P-8A cybersecurity assessment was conducted as part of the P-8A ECP 2 OT&E. The Navy did not complete development of a P-8A Increment 3 TEMP due to program funding uncertainty and delayed execution of the ECP 2 OT&E.
- FY17 Recommendations. The Navy should:
  1. Complete P-8A MAC ASW wide-area search operational testing as defined in the 2013 P-8A TEMP and the updated FY17 test execution strategy.
  2. Coordinate with DOT&E to develop a detailed P-8A Increment 3 ECP 6/7 test strategy prior to system critical design review in FY19.
  3. Conduct operational testing of the complete P-8A high-altitude ASW operational capability in conjunction with planned integration of the HAAWC MK 54 torpedo system.

Rolling Airframe Missile (RAM) Block 2

Executive Summary

- The Navy's Operational Test and Evaluation Force (OPTEVFOR) commenced the final IOT&E phase for the Rolling Airframe Missile (RAM) Block 2 program in March 2017 in accordance with a DOT&E-approved test plan. Testing consists of conducting RAM Block 2 Probability of Raid Annihilation (PRA) Modeling and Simulation Test Bed runs to gather RAM Block 2 operational effectiveness data. OPTEVFOR expects to complete this phase of IOT&E in December 2017.
- DOT&E intends to issue an IOT&E report once the Navy has conducted all RAM Block 2 PRA Test Bed runs and analysis is completed.

System

- The RAM, jointly developed by the United States and the Federal Republic of Germany, provides a short-range, lightweight self-defense system to defeat anti-ship cruise missiles (ASCMs). There are three RAM variants:
  - RAM Block 0 uses dual mode, passive radio frequency/infrared guidance to home in on ASCMs.
  - RAM Block 1A adds infrared guidance improvements to extend defenses against ASCMs that do not radiate radio frequencies.
  - RAM Block 2 incorporates changes to improve its kinematic capability and capability to guide on certain types of ASCM radio frequency threat emitters in order to defeat newer classes of ASCM threats. The warhead in Block 2 is the same as in Blocks 1 and 1A.
- The Navy can launch RAM Block 2 from the 21-round RAM Guided Missile Launch System resident on LPD 17, LHA 6, LSD 41/49, LCS *Freedom*, and CVN 68 ship classes. It can also be launched from the SeaRAM standalone self-defense system, which is composed of the Close-In Weapon System radar/electronic warfare sensor suite and command/decision capability combined with an 11-round missile launcher. The SeaRAM system is resident on selected Aegis DDG 51 destroyers and the LCS *Independence* ship class.

Mission

Commanders employ naval surface forces equipped with RAM to provide a defensive short-range, hard-kill engagement capability against ASCM threats.

Major Contractors

- Raytheon Missiles Systems – Tucson, Arizona
- RAMSys – Ottobrunn, Germany

Activity

OPTEVFOR commenced the final IOT&E phase for the RAM Block 2 program in March 2017 in accordance with a DOT&E-approved test plan. Testing consists of conducting RAM Block 2 PRA Modeling and Simulation Test Bed runs to gather RAM Block 2 operational effectiveness data. This IOT&E phase is expected to complete in December 2017.

Assessment

Analysis of completed RAM Block 2 PRA Test Bed runs is ongoing. DOT&E intends to issue an IOT&E report after the Navy has conducted all planned RAM Block 2 PRA Test Bed runs and analysis is completed.

Recommendations

- Status of Previous Recommendations. The Navy has not completed the following previous recommendations:
  1. Correct the identified integration deficiencies with the Ship Self-Defense System (SSDS)-based combat system and RAM Block 2. Demonstrate these corrections in a phase of operational testing.
  2. Correct the SSDS scheduling function to preclude interference with the RAM infrared guidance capability stemming from prior intercepts and warhead detonations. Demonstrate corrections in a phase of operational testing.
  3. Develop a Multi-Stage Supersonic Target adequate for use in a phase of RAM Block 2 FOT&E.
  4. Conduct FOT&E to determine the RAM Block 2 capability to home on and destroy helicopters, slow aircraft, and surface threats.
  5. Develop an improved steerable antenna system for its ASCM surrogates.
- FY17 Recommendations. None.

Ship Self-Defense for LHA 6

Executive Summary

- The Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted tracking exercises with low altitude aerial targets and surface targets on USS *America* (LHA 6) from January to February 2017. Test results identified system integration and training deficiencies.
- OPTEVFOR completed the cybersecurity IOT&E test phase in March 2017. The test results are classified.
- OPTEVFOR commenced the Probability of Raid Annihilation (PRA) Modeling and Simulation test bed phase of IOT&E in March 2017. Completion of this test phase is expected in December 2017.

System

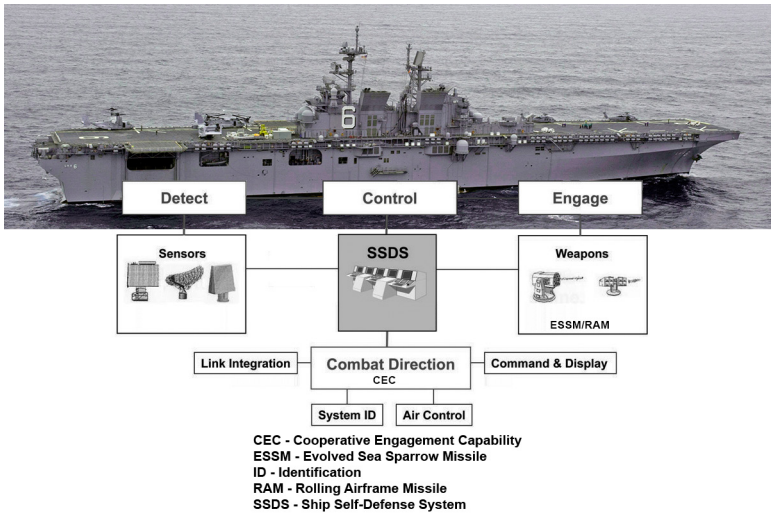
- Ship self-defense for LHA 6 is addressed by several legacy combat system elements (including the primary self-defense radars AN-SPS-49A(V)1, AN/SPS-48E(V)10, AN/SPS-73, AN/SPQ-9B, and the NULKA Active Electronic Decoy) and five acquisition programs:
  - Ship Self-Defense System (SSDS)
  - Rolling Airframe Missile (RAM)
  - Evolved Seasparrow Missile (ESSM)
  - Cooperative Engagement Capability (CEC)
  - Surface Electronic Warfare Improvement Program (SEWIP)

SSDS

- SSDS is a local area network that uses open computer architecture and standard Navy displays to integrate a surface ship's sensors and weapons systems to provide an automated detect-track-engage sequence for ship self-defense.
- SSDS MK 1 is the legacy command and control system for LSD 41/49-class ships.
- SSDS MK 2 has six variants:
  - Mod 1, used in *Nimitz* (CVN 68)-class aircraft carriers
  - Mod 2, used in *San Antonio* (LPD 17)-class amphibious ships
  - Mod 3, used in *Iwo Jima* (LHD 7)-class and *Makin Island* (LHD 8)-class amphibious ships
  - Mod 4, used in *America* (LHA 6)-class amphibious ships
  - Mod 5, used in *Whidbey Island* (LSD 41)-class and *Harpers Ferry* (LSD 49)-class amphibious ships
  - Mod 6, in development for *Gerald R. Ford* (CVN 78)-class aircraft carriers

RAM

- The RAM, jointly developed by the United States and the Federal Republic of Germany, provides a short-range, lightweight self-defense system to defeat anti-ship cruise missiles (ASCM).
- There are three RAM variants:



  - RAM Block 0 uses dual-mode, passive radio frequency/infrared guidance to home in on ASCMs.
  - RAM Block 1A adds infrared guidance improvements to extend defense against ASCMs that do not emit radar signals.
  - RAM Block 2 adds kinematic and guidance improvements to extend the capability of RAM Block 1A against newer classes of ASCM threats.

ESSM

- The ESSM, cooperatively developed among 13 nations, is a medium-range, ship-launched, self-defense guided missile intended to defeat ASCM, surface, and low-velocity air threats.
- The ESSM is currently installed on LHA 6 and LHD 8 amphibious ships, DDG 51 Flight IIA destroyers, and CVN 68-class aircraft carriers equipped with the SSDS MK 2 Mod 1 Combat System.
- There are two variants of ESSM:
  - ESSM Block 1 is a semi-active radar-guided missile that is currently in service.
  - ESSM Block 2 is in development and intended to have semi-active and active radar guidance.

CEC

- CEC is a sensor network with an integrated fire control capability intended to significantly improve battle force air and missile defense capabilities by combining data from multiple battle force air search sensors on CEC-equipped units into a single, real-time, composite track picture.
- The two major hardware pieces are the Cooperative Engagement Processor, which collects and fuses radar data, and the Data Distribution System, which distributes CEC data to other CEC-equipped ships and aircraft.

- CEC is an integrated component of, and serves as the primary air tracker for, non-LSD class ships equipped with SSDS MK 2.
- There are two major surface ship variants of CEC:
  - The CEC AN/USG-2/2A is used in selected Aegis cruisers and destroyers, LPD 17/LHD/LHA 6 amphibious ships, and CVN 68-class aircraft carriers.
  - The CEC AN/USG-2B, an improved version of the AN/USG-2/2A, is used in selected Aegis cruisers/destroyers, selected amphibious assault ships including the LHA 6 class, and CVN 68-class aircraft carriers.

SEWIP

- SEWIP is an evolutionary development program providing block upgrades to the AN/SLQ-32 electronic warfare system to address critical capability, integration, logistics, and performance deficiencies.
- There are three major SEWIP block upgrades:
  - SEWIP Block 1, used on LHA 6-class ships, replaced obsolete parts in the AN/SLQ-32 and incorporated a new, user-friendly operator console, an improved electronic emitter identification capability, and an embedded trainer.
  - SEWIP Block 2 incorporated a new receiver antenna system intended to improve the AN/SLQ-32's passive electronic warfare capability.
  - SEWIP Block 3 is in development and will incorporate a new transmitter antenna system intended to improve the AN/SLQ-32's active electronic warfare capability.

Mission

- Naval Component and Unit Commanders use SSDS, RAM, ESSM, SEWIP, CEC, and many legacy systems to accomplish ship self-defense missions.
- Naval surface units use the:
  - SSDS to provide automated and integrated detect to engage ship self-defense capabilities against ASCM, air, and surface threats
  - RAM to provide a short-range, hard-kill engagement capability against ASCM threats
  - ESSM to provide a medium-range, hard-kill engagement capability against ASCM threats
  - CEC to provide accurate air and surface threat tracking data to SSDS
  - SEWIP-improved AN/SLQ-32 as the primary electronic warfare sensor and soft-kill weapons system for air defense (to include self-defense) missions

Major Contractors

- SSDS (all variants): Raytheon – San Diego, California
- RAM and ESSM (all variants): Raytheon – Tucson, Arizona
- CEC (all variants): Raytheon – St. Petersburg, Florida
- SEWIP
  - Block 1: General Dynamics Advanced Information Systems – Fair Lakes, Virginia
  - Block 2: Lockheed Martin – Syracuse, New York
  - Block 3: Northrop Grumman – Baltimore, Maryland

Activity

- OPTEVFOR conducted tracking exercises with low altitude/low speed aerial targets and surface targets at the Naval Air Warfare Center, Point Mugu, California, from January to February 2017 in accordance with a DOT&E-approved test plan.
- OPTEVFOR commenced the PRA Modeling and Simulation test bed phase of IOT&E at the Naval Research Laboratory, Washington, District of Columbia, in March 2017 in accordance with a DOT&E-approved test plan. Completion of this test phase is expected in December 2017.
- OPTEVFOR completed the cybersecurity IOT&E test phase on the LHA 6 at Naval Base San Diego, California, in March 2017. The test results are classified.

Assessment

- Results of the January/February 2017 surface target tracking exercise identified integration deficiencies between the SSDS and the AN/SPS-73 radar. These deficiencies adversely affected the ability of the crew to maintain self-defense situational awareness against surface threats.
- Results of the January/February 2017 tracking exercises identified problems with the ship's sensors erroneously reporting dual tracks (two tracks for one target) and incorrect target positions. Preliminary analysis identified crew training deficiencies associated with radar sensor alignment and monitoring contributed to the problems.

Recommendations

- Status of Previous Recommendations. The Navy has satisfactorily addressed some previous recommendations. However, the Navy has not resolved the following previous recommendations related to LHA 6 ship self-defense:
  1. Optimize SSDS MK 2 weapon employment timelines to maximize weapon Probability of Kill.
  2. Develop an open-loop seeker subsonic ASCM surrogate target for ship self-defense combat system operational tests.
  3. Correct the identified SSDS MK 2 software reliability deficiencies.
  4. Correct the identified SSDS MK 2 training deficiencies.
  5. Develop and field deferred SSDS MK 2 interfaces to the Global Command and Control System – Maritime and the TPX-42A(V) command and control systems.
  6. Improve the ability of legacy ship self-defense combat system sensor elements to detect threat surrogates used in specific ASCM raid types.
  7. Improve SSDS MK 2 integration with the MK 9 Track Illuminators to better support ESSM engagements.

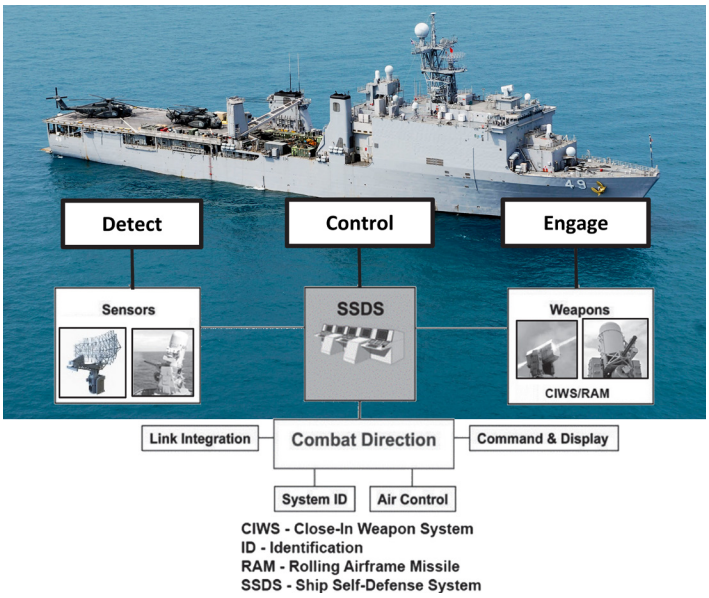
8. Develop combat system improvements to increase the likelihood that ESSM and RAM will home on their intended targets.
9. Correct the cause of the ESSM missile failures and demonstrate the correction in a future phase of operational testing.
10. Investigate means to mitigate the chances of an ESSM pre-detonating on debris before approaching its intended target.
11. Investigate why target emitters continue to be reported as valid by the AN/SLQ-32 electronic warfare system with the SEWIP Block 1 upgrade after the target is destroyed. Test any corrections in a future operational test phase.
12. Correct the SSDS scheduling function to preclude interference with the RAM infrared guidance stemming from prior intercepts and warhead detonations. Demonstrate corrections in a phase of operational testing.
13. Correct integration problems with the SSDS-based combat system and the AN/SPQ-9B radar to ensure that all valid AN/SPQ-9B detections are used by the combat system when tracking targets. Demonstrate the corrections in a phase of operational testing.
14. Update the LHA 6 and SSDS Test and Evaluation Master Plans to include at-sea and PRA test bed operational test phases to enable evaluation of the ship self-defense capabilities of LHA 8 equipped with the new Enterprise Air Surveillance Radar.
15. Continue to take action on the classified recommendations contained in the March 2011 and November 2012 DOT&E reports to Congress on the ship self-defense mission area.
16. Provide a plan of action and milestones for introduction and operational testing of Fire Control Loop Improvement Program (FCLIP) improvements.
17. Investigate and correct the combat system time synchronization problem that prevented the launch of a full salvo of ESSMs.
18. Investigate and correct the SSDS processing of threat surrogate emitters and sensor detection deficiency.
19. Develop an adequate Multi-Stage Supersonic Target (MSST) and electronic warfare target surrogates for operational testing.

- FY17 Recommendations. The Navy should:
  1. Correct the integration deficiencies between SSDS and the AN/SPS-73 radar that adversely affected the crew's ability to maintain self-defense situational awareness against surface threats.
  2. Provide ship crews with adequate radar sensor alignment and monitoring training.

Ship Self-Defense for LSD 41/49

Executive Summary

- The Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted one missile firing exercise in December 2016 from the Self-Defense Test Ship (SDTS) on the Naval Air Warfare Center – Weapons Division, Point Mugu, California, test range. This test was the first of a series of nine planned missile/gun firings to operationally test the self-defense capabilities of the *Whidbey Island* (LSD 41)-class and *Harpers Ferry* (LSD 49)-class amphibious ships.
- DOT&E provided a classified Early Fielding Report for the Ship Self-Defense capability of the LSD 41/49 ship class to Congress in November 2017 because the Navy deployed three LSD 41/49 class ships in FY17 without completing the planned operational testing. The report stated that there is a paucity of operational test results to support an evaluation of the self-defense capabilities of LSD 41/49-class ships equipped with the Ship Self-Defense System (SSDS) MK 2 Mod 5 Combat System, and that the Navy is deploying those ships with unknown self-defense capabilities.



System

- Several legacy combat system elements (including the primary self-defense radars, AN/SPS-49A(V)1, and Close-in Weapon System) and three acquisition programs address surface ship self-defense for LSD 41/49-class ships. The three acquisition programs are:
  - SSDS
  - Rolling Airframe Missile (RAM)
  - Surface Electronic Warfare Improvement Program (SEWIP)

SSDS

- SSDS is a local area network that uses open computer architecture and standard Navy displays to integrate a surface ship's sensors and weapons systems to provide an automated detect-track-engage sequence for ship self-defense.
- SSDS MK 1 is the legacy command and control system for LSD 41/49-class ships.
- SSDS MK 2 has six variants:
  - Mod 1, used in *Nimitz* (CVN 68)-class aircraft carriers
  - Mod 2, used in *San Antonio* (LPD 17)-class amphibious ships
  - Mod 3, used in *Iwo Jima* (LHD 7)-class and *Makin Island* (LHD 8)-class amphibious ships
  - Mod 4, used in *America* (LHA 6)-class amphibious ships
  - Mod 5, used in *Whidbey Island* (LSD 41)-class and *Harpers Ferry* (LSD 49)-class amphibious ships
  - Mod 6, in development for *Gerald R. Ford* (CVN 78)-class aircraft carriers

RAM

- The RAM, jointly developed by the United States and the Federal Republic of Germany, provides a short-range, lightweight self-defense system to defeat anti-ship cruise missiles (ASCMs).
- There are three RAM variants:
  - RAM Block 0 uses dual-mode, passive radio frequency/infrared guidance to home in on ASCMs.
  - RAM Block 1A adds infrared guidance improvements to extend defense against ASCMs that do not emit radar signals.
  - RAM Block 2 adds kinematic and guidance improvements to extend the capability of RAM Block 1A against newer classes of ASCM threats.

SEWIP

- SEWIP is an evolutionary development program providing block upgrades to the AN/SLQ-32 electronic warfare system to address critical capability, integration, logistics, and performance deficiencies.
- There are three major SEWIP block upgrades:
  - SEWIP Block 1, used on LSD 41/49-class ships, replaced obsolete parts in the AN/SLQ-32 and incorporated a new, user-friendly operator console, an improved electronic emitter identification capability, and an embedded trainer.
  - SEWIP Block 2 incorporated a new receiver antenna system intended to improve the AN/SLQ-32's passive electronic warfare capability.

- SEWIP Block 3 is in development and will incorporate a new transmitter antenna system intended to improve the AN/SLQ-32's active electronic warfare capability.

Mission
- Naval Component and Unit Commanders use SSDS, RAM, SEWIP, and other legacy systems, to accomplish ship self-defense missions.
- Naval surface units use the:
  - SSDS to provide automated and integrated detect to engage ship self-defense capabilities against ASCM, air, and surface threats
  - RAM to provide a short-range hard-kill engagement capability against ASCM threats
  - SEWIP-improved AN/SLQ-32 as the primary electronic warfare sensor and soft-kill weapons system for air defense (to include self-defense) missions

Major Contractors
- SSDS (all variants): Raytheon – San Diego, California
- RAM (all variants): Raytheon Missile Systems – Tucson, Arizona; RAMSys – Ottobrunn, Germany
- SEWIP
  - Block 1: General Dynamics Advanced Information Systems – Fair Lakes, Virginia
  - Block 2: Lockheed Martin – Syracuse, New York
  - Block 3: Northrop Grumman – Baltimore, Maryland

Activity
- OPTEVFOR conducted one missile firing exercise in December 2016 from the SDTS on the Naval Air Warfare Center – Weapons Division test range in accordance with a DOT&E-approved test plan. This test was the first of nine planned missile firings to operationally test the self-defense capability of the LSD 41/49-class amphibious ships. Results of the missile firing test are classified.
- DOT&E provided a classified SSDS MK 2 Mod 5 early Fielding Report to Congress in November 2017 because the Navy deployed three LSD 41/49-class ships in FY17 without completing the planned operational testing.
- The Navy plans to conduct only one LSD 41/49-class missile firing exercise from the SDTS in FY18. There are no plans for additional missile firings before FY20. Five additional LSD 41/49-class ships are scheduled to deploy in FY19 and FY20.
- The first SSDS MK 2 Mod 5-equipped LSD 41/49 ship deployed in late 2016. Two SSDS MK 2 Mod 5-equipped LSD 41/49 ships deployed in FY17. At least one more LSD 41/49 deployment is planned in FY18.

Assessment
- With only one of the nine required missile/gun firing operational tests completed, there is a paucity of operational test results to support an evaluation of the self-defense capabilities of the LSD 41/49-class ships.
- SDTS scheduling constraints are delaying completion of the remaining eight required missile/gun firing operational tests until FY20 at the earliest. By that time, 8 of the 12 LSD 41/49 ships equipped with the SSDS MK 2 Mod 5 Combat System will have deployed.
- The Navy is deploying LSD 41/49 ships with uncharacterized self-defense capabilities.

Recommendations
- Status of Previous Recommendations. The Navy has not addressed the previous recommendation to complete all planned operational tests of the LSD 41/49 ship class equipped with the SSDS MK 2 Mod 5 Combat System as soon as possible and prior to further ship deployments.
- FY17 Recommendations. None.

SSN 774 *Virginia*-Class Submarine

Executive Summary

- The Navy deployed the first *Virginia*-class Block III submarine, USS *North Dakota* (SSN 784), in May 2015, with only limited developmental testing of the platform's major subsystem upgrades. Major testing phases included developmental testing of the new Large Aperture Bow (LAB) sonar array, testing of the system to support weapon system accuracy (this included sonar performance assessments), testing of the weapon system interfaces, and a limited operational assessment phase to support deployment certification.
- DOT&E submitted a classified Early Fielding Report in September 2015 detailing the results of the testing to date. DOT&E concluded that:
  - The changes to the *Virginia*-class Block III submarine do not appear to improve or degrade the system's ability to conduct submarine missions.
  - The LAB array used on the *Virginia*-class Block III submarine has the potential to perform as an adequate replacement for the spherical array used on previous *Virginia*-class variants.
  - System reliability meets the Navy's thresholds.
- The Navy commenced operational testing of the *Virginia*-class Block III submarine in June 2017 that included anti-submarine warfare, anti-surface warfare, strike warfare, and mobility in support of the intelligence collection mission area. The Navy expects to complete operational testing in November 2017. DOT&E assessment of the *Virginia*-class Block III submarine is ongoing. DOT&E will submit a classified FOT&E report in FY18.
- The Navy submitted the *Virginia* Block III Vulnerability Assessment Report for DOT&E review in August 2017. The Navy expects to publish a final report by January 2018.

System

- The *Virginia*-class submarine is the Navy's latest fast-attack submarine and is capable of targeting, controlling, and launching MK 48 Advanced Capability torpedoes and Tomahawk cruise missiles.
- The Navy is procuring *Virginia*-class submarines incrementally in a series of blocks; the block strategy is for contracting purposes, not necessarily to support upgrading capabilities.
  - Block I (hulls 1-4) and Block II (hulls 5-10) ships were built to the initial design of the *Virginia* class.
  - Block III (hulls 11-18) and Block IV (hulls 19-28) ships, starting with SSN 784, include the following affordability enhancements:

    - A LAB array in place of the spherical array in the front of the ship
    - Two *Virginia* payload tubes replace the 12 vertical launch tubes; each payload tube is capable of storing and launching 6 Tomahawk land-attack missiles used in strike warfare missions
  - Block V and beyond will increase strike payload capacity from 12 to 40 Tomahawk land-attack missiles by adding a set of 4 additional payload tubes in an amidships payload module, capable of storing and launching 7 Tomahawk missiles each, as well as providing the potential to host future weapons and unmanned systems.

Mission

The Operational Commander will employ the *Virginia*-class Block III submarine to conduct open-ocean and littoral covert operations that support the following submarine mission areas:

- Strike warfare
- Anti-submarine warfare
- Intelligence, surveillance, and reconnaissance
- Mine warfare
- Anti-surface warfare
- Naval special warfare
- Battle group operations

Major Contractors

- General Dynamics Electric Boat – Groton, Connecticut
- Huntington Ingalls Industries, Newport News Shipbuilding – Newport News, Virginia

Activity

- In September 2015, DOT&E submitted a classified Early Fielding Report on the first *Virginia*-class Block III submarine due to submarine deployment prior to the completion of operational testing.
- In September and October 2016, the Navy conducted a cybersecurity assessment of the *Virginia*-class Block III submarine.
- In February and April 2017, the Navy conducted operational testing of the strike warfare capabilities of the *Virginia*-class Block III submarine.
- In June 2017, the Navy conducted a comprehensive operational test of the *Virginia*-class Block III submarine. The Navy evaluated the Block III submarine in the following mission areas:
  - Surface warfare, including torpedo employment, against U.S. naval vessels in open-ocean near Fort Pierce, Florida.
  - Mobility is support of intelligence collection in a high density contact environment off the coast of Port Everglades, Florida. The focus of this test was the crew's capability to maintain situational awareness both when the submarine was deep and when the submarine was at periscope depth among a large number of surface ships.
  - Anti-submarine warfare, inclusive of submarine search through prosecution, against a high-end nuclear submarine in the Port Everglades Operating Area. Testing included a detection/classification range comparison test between the Block I/II spherical array and the Block III LAB array, as well as a search rate test against a high-end threat nuclear submarine surrogate.
- To date, the Navy completed testing in accordance with a DOT&E-approved Test and Evaluation Master Plan (TEMP) and test plans.
- In October 2017, the Navy completed test strategy and test design development for operational test of the *Virginia*-class Block V submarine. The Navy expects to submit the *Virginia*-class Block V submarine TEMP for approval in FY18.
- In August 2017, the Navy submitted the *Virginia* Block III Vulnerability Assessment Report for DOT&E review.
- The Navy scheduled the remaining operational test event, a maximum Tomahawk Land Attack Missile alignment, in November 2017.
- The Navy completed the shock qualification testing for the *Virginia* Common Weapons Launcher and the *Virginia* Payload Tube hatch in late 2014, but has since redesigned a subcomponent of the hatch. General Dynamics Electric Boat requested hatch shock qualification with a noted exception of the modified component. The Navy continues to evaluate the subcomponent redesign and has not determined a method to approve the exception.
- The Navy continued its verification, validation, and accreditation (VV&A) of the Transient Shock Analysis modeling methods used for the design and shock qualification of the *Virginia*-class Block III items. The Navy expects to complete this effort in 2QFY18.

Assessment

- The September 2015 DOT&E classified Early Fielding Report details the effects of new major system components with respect to the intended mission during the early deployment. The report concluded the following:
  - The changes to the *Virginia*-class Block III submarine do not appear to improve or degrade the system's ability to conduct submarine missions.
  - The LAB array demonstrates the potential to perform as an adequate replacement for the legacy spherical array.
  - The sonar Light Weight Wide Aperture Array experienced a hardware fault which limited the ability to assess effectiveness of the system.
  - Developmental testing of the system indicates that system software reliability meets the Navy's thresholds. Testers could not evaluate hardware reliability because of limited time.
- The FOT&E assessment of the *Virginia*-class Block III submarine remains ongoing. DOT&E will submit a classified FOT&E report in FY18.
- DOT&E review of the draft *Virginia* Block III Vulnerability Assessment Report is in progress. The Navy expects to publish the report by January 2018.

Recommendations

- Status of Previous Recommendations. The following are recommendations that remain from FY16. The Navy should:
  1. Test against a diesel submarine threat surrogate in order to evaluate the *Virginia*-class submarine's capability, detectability, and survivability against modern diesel-electric submarines.
  2. Conduct an FOT&E to examine the *Virginia*-class submarine's susceptibility to airborne anti-submarine warfare threats such as Maritime Patrol Aircraft and helicopters.
  3. Complete the verification, validation, and accreditation of the Transient Shock Analysis method used for *Virginia*-class Block III items.
  4. Complete the FOT&E event to determine the *Virginia*-class submarine's susceptibility to low-frequency active sonar and the submarine's ability to conduct anti-surface ship warfare in a low-frequency active environment. This testing should include a *Los Angeles*-class submarine operating in the same environment to enable comparison with the *Virginia*-class submarine.
  5. Investigate and implement methods to aid Special Operations Forces in identifying the submarine during operations in conditions of low visibility.
  6. Address the three classified recommendations listed in the September 2015 Block III *Virginia* class Early Fielding Report.
- FY17 Recommendations. None.

Standard Missile-6 (SM-6)

Executive Summary
- Standard Missile-6 (SM-6) Block I (BLK I) has attained Initial Operational Capability; Full Operational Capability is expected in FY18.
- In FY17, the Navy conducted FOT&E to demonstrate a correction to the classified performance deficiency initially reported in DOT&E's classified "Standard Missile-6 (SM-6) Beyond Low-Rate Initial Production Report" issued in May 2015. These Verification of Corrected Deficiency (VCD) events demonstrated that the intended correction mitigated the effects of the deficiency but did not eliminate it. The testing identified two concerns that contributed to the deficiency not being completely eliminated:
  - A classified concern with the missile Target Detection Device
  - A classified concern with the missile active seeker
- In FY17, as part of FOT&E, the Navy conducted SM-6 BLK I modeling and simulation (M&S) to demonstrate interoperability with the Aegis Baseline 9 combat system.
- The Navy commenced operational testing of SM-6 BLK IA, a pre-planned product improvement of the SM-6 BLK I missile, in September 2017. The SM-6 BLK IA testing consists of seven SM-6 BLK IA firings against subsonic and supersonic aerial targets and M&S runs for the record. The Navy intends to complete operational testing in FY18.
- The Navy conducted two SM-6 Dual 1 salvo firings against Ballistic Missile Defense (BMD) targets.

System
- SM-6 BLK I and BLK IA are the latest evolution of the Standard Missile family of fleet air defense missiles.
- The Navy employs the SM-6 from Aegis-equipped cruisers and destroyers (i.e., *Ticonderoga*-class cruisers and *Arleigh Burke*-class destroyers).
- The SM-6 seeker and terminal guidance electronics derive from technology developed in the Advanced Medium-Range Air-to-Air Missile program.
- SM-6 retains the legacy Standard Missile semi-active radar homing capability.
- SM-6 receives midcourse flight control from the Aegis Weapon System (AWS) via ship's radar; terminal flight control is autonomous via the missile's active seeker or supported by the AWS via the ship's illuminator.
- The Navy intends the SM-6 BLK IA upgrade to provide improved performance against advanced threats.
- SM-6 Dual I capability is being added to provide Sea-Based Terminal BMD capability against short-range ballistic missiles.

- The Navy upgraded the SM-6 to add an anti-surface target capability but it has not yet operationally tested the capability.

Mission
- The Joint Force Commander/Strike Group Commander will employ naval units equipped with the SM-6:
  - For air defense against fixed-/rotary-winged targets and anti-ship missiles operating at altitudes ranging from very high to sea-skimming
  - As part of the Navy Integrated Fire Control – Counter Air From the Sea (NIFC-CA FTS) operational concept to provide extended range over-the-horizon capability against at-sea and overland threats
  - As part of the NIFC – Collateral (NCC) operational concept to provide extended-range capability against surface targets
- The Joint Force Commander/Strike Group Commander will use SM-6 Dual I to provide Sea-Based Terminal capability against short- and medium-range ballistic missiles in their terminal phase of flight, anti-ship cruise missiles, and all types of aircraft.

Major Contractor
Raytheon Missile Systems – Tucson, Arizona

Activity

- In FY17, the Navy conducted multiple test phases for SM-6. The Navy conducted the FOT&E and BMD tests in accordance with DOT&E-approved test plans.
- SM-6 BLK I has attained Initial Operational Capability, and Full Operational Capability is expected in FY18.
- SM-6 BLK I FOT&E
  - Two SM-6 BLK I FOT&E VCD events in April 2017 successfully intercepted a target employing countermeasures.
  - One SM-6 BLK I FOT&E VCD event in April 2017 failed to intercept a target employing countermeasures.
  - At the conclusion of SM-6 BLK I FOT&E live flight testing, DOT&E satisfactorily resolved the Launch Availability Key Performance Parameter.
- SM-6 BLK I M&S FOT&E
  - The Navy commenced SM-6 BLK I M&S FOT&E in September 2017. The Navy intends to demonstrate SM-6 BLK I compatibility with the Aegis Baseline 9 combat system during the FOT&E.
  - The Navy intends to complete testing in early FY18.
- SM-6 BLK I Developmental Testing
  - One SM-6 BLK I Developmental Test Software Alignment event in April 2017 demonstrated that the missile successfully acquired, tracked, and intercepted a high altitude, high closing velocity target.
  - One SM-6 BLK I Developmental Test Software Alignment event in April 2017 intended to demonstrate the missile's ability to intercept a high altitude, high closing velocity target. The test failed because the missile failed to launch.
- NIFC-CA FTS SM-6 Tests
  - The Navy attempted to execute SM-6 BLK I NIFC-CA FTS event AS-04 in March 2017, but a target failure precluded the event. AS-04 is rescheduled for FY18.
  - The Navy successfully executed SM-6 BLK I NIFC-CA FTS event LFT-05 in May 2017. The SM-6 BLK I successfully intercepted a target. The Navy's first attempt of LFT-05, in December 2016, was unsuccessful.
- SM-6 BLK I BMD Testing
  - During FTM-27 Event 1, in December 2016, an Aegis Baseline 9.C1 destroyer (which hosts the Aegis BMD 5.0 Capability Upgrade) engaged a complex medium-range ballistic missile target with a salvo of two SM-6 Dual I missiles. FTM-27 Event 1 was the first demonstration of Aegis BMD Sea-Based Terminal capability against complex ballistic missile targets.
  - During FTM-27 Event 2, in August 2017, an Aegis Baseline 9.C1 destroyer engaged a complex medium-range ballistic missile target with a salvo of two SM-6 Dual I missiles. The test, which was a follow-on from FTM-27 Event 1, further demonstrated aspects of the Baseline 9.C1 Sea-Based Terminal engagement capability.
- SM-6 BLK 1A Developmental Testing
  - The Navy conducted developmental testing of pre-planned product improvements to the SM-6 BLK I missile (i.e., SM-6 BLK IA). The Navy successfully executed SM-6 BLK IA Guided Test Vehicle (GTV) event 3b (GTV-3b) in June 2017 after two prior failures (GTV-3 in August 2016 and GTV-3a in November 2016).
  - The Navy conducted a failure review board of the failed GTV-3a event before proceeding with the GTV-3b event.
- SM-6 BLK IA Operational Testing
  - The Navy commenced operational testing of the SM-6 BLK IA and successfully conducted two flight tests in September 2017.
  - Operational testing continues in FY18 to complete planned live flight-testing and M&S runs for the record.
- DOT&E will publish an FOT&E report in FY18 that addresses all SM-6 BLK I live fire tests and M&S tests. This report will focus on SM-6 BLK I performance when employed from Aegis Baseline 9 ships.
- DOT&E will publish an SM-6 BLK IA report once testing is complete in FY18.

Assessment

- As reported in DOT&E's memorandum, "Post Initial Operational Test and Evaluation Observations and Assessment of Standard Missile-6 Block I Suitability," dated December 2016, DOT&E considers the previously reported uplink/downlink antenna shroud reliability deficiency resolved.
- The Navy developed specific software improvements to SM-6 BLK I to mitigate the classified performance deficiency discovered during IOT&E and in DOT&E's classified IOT&E report. VCD FOT&E events conducted by the Navy demonstrated that the software improvements work as intended and lessen the severity of the deficiency, but the improvements did not resolve the deficiency in all instances. The testing identified two concerns that contributed to the deficiency not being fully resolved.
  - Testing revealed a classified concern with the missile's Target Detection Device.
  - Testing revealed a classified concern with the missile's active seeker.
- NIFC-CA FTS event LFT-5 further demonstrates the NIFC-CA FTS capability, but – as with previous NIFC-CA FTS tests – the Navy did not conduct the test under operationally realistic conditions. Moreover, the Navy's test scenarios are not sufficiently challenging to demonstrate the NIFC-CA FTS requirements defined in the Navy's September 2012 NIFC-CA FTS Testing Capability Definition Letter. Nevertheless, the Navy has deployed the NIFC-CA FTS capability as a tactical option in fleet air defense. DOT&E reported on NIFC-CA FTS in the classified "Aegis Weapon System Baseline 9A Early Fielding Report" issued in July 2015, and will continue to report on NIFC-CA FTS in future Aegis Weapon System assessments.
- During SM-6 BLK 1A event GTV-3a, the SM-6 BLK IA experienced an inflight failure that prevented the target from intercepting its intended target. The failure delayed the start of SM-6 BLK IA operational testing.

- The Launch Availability Key Performance Parameter was unresolved in SM-6 BLK I IOT&E. During SM-6 BLK I FOT&E, the Navy fired, without failure, seven missiles that met the required storage requirements. While these results were not sufficient to state that BLK I meets its required Launch Availability with high statistical confidence, the results were sufficient to indicate no significant problem exists with storage reliability.

Recommendations

- Status of Previous Recommendations.
  - The Navy is addressing the previous recommendations from FY14 to 1) complete corrective actions of the classified performance deficiency discovered during IOT&E and 2) develop a flight test program to test those corrective actions.
  - The Navy has not addressed the FY15 recommendation to provide DOT&E an operational test concept and operational test plan for NIFC-CA FTS Increment 2; DOT&E rescinded this recommendation as the Navy integrated NIFC-CA FTS as a tactical option in fleet air defense. DOT&E removed the NIFC-CA FTS program from T&E oversight and it will be tested as a normal tactic in future Aegis/SM-6 testing.
- FY17 Recommendation.
  1. The Navy should continue investigating the classified performance deficiency discovered during IOT&E, perform corrective actions, and verify corrective actions with flight tests. This includes correcting the two new problems encountered during FY17 SM-6 BLK I VCD tests.

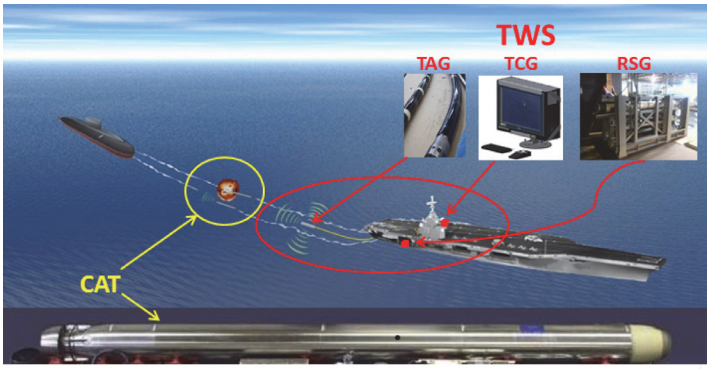
Surface Ship Torpedo Defense (SSTD) System: Torpedo Warning System (TWS) and Countermeasure Anti-Torpedo (CAT)

Executive Summary

- During FY17, USS *Dwight D. Eisenhower* and USS *George H. W. Bush* completed deployments and USS *Nimitz* started a deployment with the Torpedo Warning System (TWS) and Countermeasure Anti-Torpedo (CAT) system. Like previous carrier deployments, the Towed Active Acoustic Source (TAAS) engineering developmental model was not reliable and the *Dwight D. Eisenhower*, *George H. W. Bush*, and *Nimitz* deployed with a passive-only TWS array. Prime contractor personnel deployed aboard the carriers to operate and maintain the TWS system, train Navy operators, and collect system data.
- In 4QFY16, the Navy reduced the FY18 and beyond funding for TWS and CAT, resulting in the suspension of contractor development and government developmental test and evaluation after FY17. The Navy funded the program to sustain the existing permanent TWS and CAT installations.
- In October 2017, the Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted a third Quick Reaction Assessment (QRA) in conjunction with contractor testing. The combined QRA and contractor tests demonstrated the ability of TWS, under optimal conditions and when manned by qualified sailors and contractors, to successfully alert on an inbound threat torpedo and the CAT system's ability to successfully engage a torpedo. The testing also demonstrated that the Navy has made significant improvements to the reliability of the TAAS.

System

- Surface Ship Torpedo Defense (SSTD) is a system of systems that includes two new sub-programs: the TWS (an Acquisition Category III program) and CAT (plans to become an acquisition program in FY17 were delayed). Combined, TWS and CAT are referred to as the Anti-Torpedo Torpedo Defensive System (ATTDS).
- TWS is being built as an early warning system to detect, localize, classify, and alert on incoming threat torpedoes and consists of three major subsystems:
  - The Target Acquisition Group consists of a towed acoustic array, tow cable, winch, power supply, and signal processing equipment. Data from the array and the ship's radar system are processed into contact tracks and alerts to be forwarded to the Tactical Control Group. The Navy intends for the array to be capable of both passive and active sonar operations.
  - The Tactical Control Group consists of duplicate consoles on the bridge and Combat Direction Center (on CVNs) that displays contacts, issues torpedo alerts to the crew, and automatically develops CAT placement presets using information sent from the Target Acquisition Group. The operator uses these displays to manage the threat engagement sequence and command CAT launches.
  - The Ready Stow Group will consist of the steel cradles housing the CATs. The permanent system consists of four steel cradles and associated electronics, each housing six anti-torpedo torpedoes (ATTs) at different locations (port/starboard and forward/aft on CVNs).
- CAT is a hard-kill countermeasure intended to neutralize threat torpedoes and consists of the following:
  - The ATT is a 6.75-inch diameter interceptor designed for high-speed and maneuverability to support rapid engagement of a threat torpedo.
  - The All-Up Round Equipment consists of a nose sabot, ram plate, launch tube, muzzle cover, breech mechanism, and energetics to encapsulate and launch the ATT.
  - A Stored Energy Propulsion System powers the tactical CAT. A battery-powered electric motor CAT exists for test purposes only. Engineering Development Model-2 is the current hardware version of the CAT.
- The Navy developed a temporary version of TWS and CAT (designated a roll-on/roll-off system) in addition to the permanent-installation version. The Navy intends for the roll-on/roll-off version to provide the same functionality as the permanent one.
  - The Navy replaced the Ready Stow Group steel cradles with two lighter-weight and aluminum Launch Frame Assemblies that each hold four CATs.



CAT - Countermeasure Anti-Torpedo
RSG - Ready Stow Group
TAG - Target Acquisition Group
TCG - Tactical Control Group
TWS - Torpedo Warning System

- The processing required for the Target Acquisition Group and the Tactical Control Group resides in two cabinets contained in a container express box located on the CVN hangar deck.
- The towed acoustic array, tow cable, and winch are permanently installed on the carrier's fantail. The other components of the system, including the operator displays and fire enable switch, reside in the container express box located on the hangar deck.

Mission

Commanders of nuclear-powered aircraft carriers and Combat Logistic Force ships will use the SSTD system to defend against incoming threat torpedoes.

Major Contractors

TWS

- Ultra Electronics-3Phoenix (Prime Contractor) – Chantilly, Virginia, and Wake Forest, North Carolina
- Alion Science and Technology (Acoustics and testing consultant) – New London, Connecticut
- In-Depth Engineering (Tactical Control Group software development) – Fairfax, Virginia
- Pacific Engineering Inc. (Ready Stow Group manufacture) – Lincoln, Nebraska
- Rolls-Royce (Winch manufacture) – Ontario, Canada
- Teledyne (Towed Array manufacture and assembly) – Houston, Texas

CAT

- Pennsylvania State University Applied Research Laboratory (ATT Systems) – State College, Pennsylvania
- Pacific Engineering Inc. (Canister fabrication) – Lincoln, Nebraska
- SeaCorp (All Up Round Equipment fabrication and assembly) – Middletown, Rhode Island

---

Activity

- In 4QFY16, the Navy reduced the FY18 and beyond funding for the TWS and CAT systems, resulting in the suspension of contractor development and government developmental test and evaluation after FY17. The Navy funded the program to sustain the existing permanent TWS and CAT installations.
- During FY17, USS *Dwight D. Eisenhower* and USS *George H. W. Bush* completed deployments, and USS *Nimitz* started a deployment with the TWS and CAT systems. The *Dwight D. Eisenhower* deployed with the temporary roll-on/roll-off version while the *George H. W. Bush* and *Nimitz* deployed with the permanent version of the systems. Like previous carrier deployments, the TAAS engineering developmental model was not reliable and the *Dwight D. Eisenhower*, *George H. W. Bush*, and *Nimitz* deployed with a passive-only TWS array prototype. Contractor personnel deployed aboard the carriers to operate and maintain the TWS system, train Navy operators, and to collect system data. The Navy Program Office intends the *Dwight D. Eisenhower* to be the last carrier to deploy with the temporary installation, and intends to install the permanent version of the TWS and CAT early fielded hardware on selected CVNs before their next deployments.
- In October and December of 2016, TWS contractors conducted dynamic tow (October) and static (December) testing on the TAAS. The Naval Surface Warfare Center, Carderock Division, Acoustic Research Detachment performed the test at Lake Pend Oreille in Bayview, Idaho.
  - The purpose of the testing was to verify reliability improvements to the TAAS, characterize its operational parameters, and collect data to support ongoing development of the active torpedo detection, classification, and localization processing systems.
  - The dynamic testing included over 11,000 active TAAS pings during 29.5 hours of full array (TAAS mated to the TWS passive array) towing. Two TAAS array amplifiers failed during the tow test; one due to a manufacturing defect, while the other was likely due to an over-current transient on the array.
  - The static testing included over 18,000 active TAAS pings with tactical waveforms during 18 hours of testing with no component failures.
- In May 2017, the Navy conducted static TAAS array tank testing at the Naval Undersea Warfare Center in Keyport, Washington, to characterize TAAS array currents at various array frequencies and waveforms and to observe the onset of array cavitation at representative water temperatures and pressures. These tests collected data to determine the optimum frequency, waveform, and power levels for search during tactical operations and to improve array reliability. The testing included approximately 7,600 active TAAS pings without any component failures.
- In May 2017, the Navy stopped development of its Integrated Evaluation Framework (IEF), which the Navy uses to support Test and Evaluation Master Plan (TEMP) and test plan development. The Navy has been working on versions of its IEF and TEMP since accomplishing a conditional TWS Milestone B decision in 2011, and had intended to make the CAT system an acquisition program in FY17.
- In October 2017, OPTEVFOR conducted a third QRA in conjunction with contractor testing performed by the Naval Undersea Warfare Center Division in Keyport, Washington, the Pennsylvania State University Applied Research Laboratory, and the major system contractors. The Navy installed the TWS and CAT systems onboard the USNS *Benavidez*

(T-AKR 306); the QRA occurred at the Canadian Forces Maritime Experimental and Test Ranges (CFMETR) near Nanoose Bay, British Columbia. The purpose of the testing was to demonstrate the TWS's torpedo alert and CAT salvo prosecution capabilities, and demonstrate the performance of the TAAS against quieter and slower torpedoes. Due to reliability problems with test target surrogates, test equipment, and CAT hardware, the Navy was not able to execute the test scenarios per the contractor test plans or the DOT&E-approved test plans. For the QRA, the Navy completed two salvo events and one non-salvo event. The contractor testing completed five TWS detection events, which included one salvo event.

- Previous QRAs in 2014 and 2015 demonstrated initial TWS and CAT system capabilities and identified significant areas of risk for early fielding aboard aircraft carriers. DOT&E will issue an update to the 2015 Early Fielding Report when analysis of the October 2017 testing is complete,

Assessment

- The contractor tests showed that the TAAS meets the technical performance specifications set forth in the Navy's System Requirements Document. Although TAAS in water and pinging test time is too limited to predict its reliability for deployment, completed testing shows that the developers made significant progress in correcting over-current conditions, which had caused amplifier component failures, and in improving TAAS reliability.
- The October 2017 combined QRA and contractor tests demonstrated the ability of the TWS and its operator to successfully alert on an inbound threat torpedo under optimal but operationally relevant conditions, and the CAT system's ability to engage a threat torpedo. The contractor test events also demonstrated the ability of the TAAS to detect moderately quiet and slower torpedoes.
  - Due to reliability problems with test target surrogates, test equipment, and CAT hardware, and the limited scope and number of CAT test events, it is unknown if the CAT systems can defend against a salvo of threat torpedoes. Detailed results and analysis for each event will be provided in DOT&E's Early Fielding Report.
  - As with the previous QRAs and contractor testing, these events were highly structured due to torpedo peacetime firing policy safety restrictions and acoustic range operating procedures, and were not conducted using operationally realistic threat torpedoes and ATT depth profiles. Furthermore, the small number of test runs allowed for demonstrations of capability and problem identification, but was not sufficient to characterize the performance of these systems in other likely operationally realistic scenarios.
  - The TWS system did not generate false target alerts during these test events. However, CFMETR and its surrounding waters were largely clear of non-participating ship traffic. Therefore, it was difficult to assess the number of false alerts the system would have generated in an operationally relevant, noisy environment, such as a congested shipping lane. Likewise, limited data are available to assess the operator's ability to manually generate alerts or to reject false alerts.
  - Safety considerations, implemented to prevent a collision between the threat torpedo surrogates, the ATTs, and the deep draft tow ship prevented assessment of TWS alertment capabilities for threats operating at representative depths and limited the assessment of the ATTs' ability to complete the target intercept. Testing and data collection near the surface is necessary to develop torpedo defense capability. The Navy could accomplish this testing safely by using a shallow draft tow ship. Likewise, ATT to target intercept data near the surface could be safely collected, but would risk the ATTs colliding with the surrogate targets.
  - The Navy has not accredited the surrogate torpedo targets used for testing as representative of any real-world threat torpedo. The surrogate targets are older U.S. torpedoes and training targets that were designed to operate at deeper depths than many threat anti-surface torpedoes. Acoustic measurements have not been completed at representative threat torpedo operating depths; therefore, the acoustic noise strength of the surrogates operating at anti-surface torpedo depths is unknown and could be noisier or quieter than threats. Given the large variation of threat torpedo noise and speed signatures, measuring the surrogate's acoustic signature would enable developers and testers to characterize the performance of the TWS and TAAS against quiet or noisy and slower or faster torpedo threats. This signature data are needed for both TWS and TAAS development and operational testing.
  - The Navy's decision to add a highly trained contractor and an acoustic operator to supplement the automated detection and alerting functions of TWS improved threat detection performance during all completed test events. The majority of the TWS's detection and alerting capability and timely operator initiation of the ATT engagement was improved as a result of contractor acoustic operators monitoring the TWS displays to provide early alerts on threat torpedoes. However, the test areas did not offer the same number of opportunities for false alerts as expected in the threat area; therefore, it is not known if the presence of the operator could also reduce the false alarm rate.
  - During the QRA and contractor tests, there were no hardware or software failures in the TWS system. This included over 45 hours of TAAS operations, and five array deployments and retrievals. Some of the CATs and CAT launchers experienced prelaunch failures. Details will be provided in DOT&E's Early Fielding Report.
  - The test showed that the Navy's TWS and CAT contractors are making progress towards developing capabilities to meet the systems' operational requirements.
- The Program Office's focus on preparing to deploy and maintain systems on carriers and limited budget has hampered their development of more extensive system detection, tracking, and alerting software; operator tactics, techniques,

and procedures; and assessments of system availability and reliability. The Navy's Program Office and contractors hoped to obtain data from CVN deployments to support TWS development, assessing and mitigating false alerts, and assessing and improving TWS system reliability, but carrier operations precluded deploying the TWS array for the majority of their underway operations. Therefore, contractors deployed on the carriers collected little real-world operational data.

- Additional information concerning the testing of the fielded TWS and CAT performance is included in DOT&E's April 2014 and March 2015 classified Early Fielding Reports.

Recommendations

- Status of Previous Recommendations. The Navy made significant progress in improving TAAS reliability. However, the Navy has made limited progress on other recommendations. The lack of progress is due to the loss of funding to conduct further TWS and CAT development and the program's focus on maintaining and repairing fielded systems. Significant outstanding recommendations include:
  1. Adequately resource the TWS program to build dedicated test assets and conduct adequate dedicated contractor and developmental testing.
  2. Adequately resource the Program Office and its contractors to conduct TWS and CAT system development and testing.
  3. Complete the TEMP for the TWS and CAT system and an LFT&E strategy for the ATT lethality as soon as possible.
  4. Conduct testing in challenging, threat representative environments.
  5. Conduct CAT testing using operationally realistic threat target profiles closer to the surface to assess CAT terminal homing, attack, and fuzing within the lethality range of the warhead.
  6. Investigate test methods designed to reduce or eliminate the safety limitations that have previously prevented testing against operationally realistic target scenarios. The Navy should consider using geographic separation, range boundaries, and shallow draft ships for future TWS and CAT testing.
  7. Investigate and implement the outstanding recommendations in the classified March 2015 DOT&E Early Fielding Report.
  8. Measure the signatures of available surrogates at representative threat torpedo depths and speeds. The Navy should also determine the adequacy of available torpedo surrogates to represent threat torpedoes.
- FY17 Recommendations. The Navy should:
  1. Restore resources to complete development and testing of the torpedo defense capability. If the Navy deploys the system, the Program Office should be resourced to complete contractor development and government testing while maintaining deployed systems.
  2. Direct the use of the already deployed systems during transits and operations in order to collect operationally meaningful data for continued system and tactics development.
  3. Investigate and fix the test target surrogate and launcher reliability problems. Failure of target surrogates during testing is a recurring problem.
  4. Investigate and fix the reliability problems with the CATs and CAT launchers.

Tactical Tomahawk Missile and Weapon System

Executive Summary

- In FY17, the Navy successfully concluded Tactical Tomahawk Weapon Control System (TTWCS) operational test event OT-D-8. Testing included cybersecurity events, a reliability/maintainability maintenance demonstration, a non-firing strike group scenario, modeling and simulation, and a live fire flight test event.
- Upon completion of the Operational Test Launch program in 2013, DOT&E removed the Tomahawk Weapon System (TWS) from operational testing oversight. This decision was based upon TWS's history of consistent satisfactory performance over the past 9 years in test planning, test execution, and meeting reliability and performance requirements.
- In FY17, the Navy issued an acquisition strategy for a series of incremental upgrades to develop an anti-ship capability. These upgrades modify the Block IV Tactical Tomahawk (TACTOM) into a Maritime Strike Tomahawk (MST). Consistent with mission changes brought about by plans to develop an anti-ship capability, the TWS was placed back on DOT&E oversight. The Navy intends to field MST as a Rapid Deployment Capability (RDC) with a Quick Reaction Assessment (QRA) test strategy with an Initial Operational Capability fielding in FY22. However, a QRA alone will not support fielding beyond an initial capability.
- To collect sufficient data for an adequate assessment of the MST capability, DOT&E identified the need for 16 test flights which could be accommodated by a combination of developmental and operational tests. Accomplishing this scope of live testing is reliant upon the Navy developing a tactical software in the-loop modeling and simulation test bed similar to the current Tomahawk modeling and simulation test bed for the land attack mission area.
- The Navy has yet to provide any plans to assess the functionality and lethality of the warhead against the MST target set.

System

- The Tomahawk Land Attack Missile is a long-range land attack cruise missile designed for launch from submarines and surface ships. Beginning in 2017, the Navy began planning the development of the anti-ship capability as part of the Block IV modernization program. To provide the anti-ship capability of the MST, a new seeker will be developed; however, the warhead for the MST mission will be the same as on the Block IV system.
- Currently, there are three fielded variants: Block III with a conventional unitary warhead, Block III with a conventional submunitions warhead, and Block IV with a conventional unitary warhead. Production of Tomahawk Block II and III missiles is complete. The Block IV Tomahawk is in production as the follow-on to the Block III conventional unitary warhead variant. These missiles are produced at lower cost and provide added capability, including the ability to communicate and be redirected to an alternate target during flight.
- The TWS also includes the Tomahawk Theater Mission Planning Center (TMPC) and the shipboard TTWCS. The TMPC and TTWCS provide for command and control, targeting, mission planning, distribution of Tomahawk tactical and strike data, and post launch control of Block IV missiles.

Mission

The Joint Force Commander employs naval units equipped with the TWS for long-range, precision strikes against land targets. Planned MST upgrades will allow the Joint Force Commander to employ the TWS in anti-ship missions.

Major Contractors

- Missile Element: Raytheon Missile Systems – Tucson, Arizona
- Weapon Control System Element: Lockheed Martin – Valley Forge, Pennsylvania
- Mission Planning Element:
  - Vencore, Inc. – San Jose, California (Mission Distribution System)
  - Tapestry Solutions – St. Louis, Missouri (Tomahawk Planning System)
  - BAE Systems – San Diego, California (Targeting Navigation Toolset)

Activity

- In 2013, DOT&E removed the TWS from oversight. This decision was based upon TWS history of consistent satisfactory performance over the past 9 years in test planning, test execution, and in meeting reliability and performance requirements. In FY17, DOT&E placed the TWS back on operational testing oversight because of the intended mission capability change initiated by the MST development.
- In October 2016, based on direction by the Deputy Secretary of Defense, the Navy approved an acquisition strategy for a series of incremental upgrades that modify the Block IV TACTOM into an MST. The Navy plans to introduce this capability in a subset of the TACTOM population (Block IV) as these missiles are inducted into the recertification line.
- In December 2016, operational test event OT-D-8, which commenced on February 22, 2016, completed. Testing was conducted in accordance with a DOT&E-approved test plan. Testing included cybersecurity events, a reliability/maintainability maintenance demonstration, non-firing strike group scenarios, modeling and simulation, and a live fire flight test. The Navy's Operational Test and Evaluation Force (OPTEVFOR) issued a classified operational test report on February 6, 2017. As the program was not under T&E oversight at the time, DOT&E did not oversee these test events.

Assessment

- The Navy plans to introduce the MST capability into the Block IV TACTOM missiles as the missiles go through their modernization process. The Navy does not intend to develop an MST Capability Development Document/Capability Production Document or any other type of requirements document to guide the developmental or operational test planning. Bypassing the Joint Capabilities Integration and Development System process, the Navy issued a Memorandum of Capability on January 19, 2017. At present, this document is the sole requirements document supporting development, production, and operational testing.
- The Navy intends to field MST as an RDC. The Navy's fielding decision will be informed by a limited initial operational test known as a QRA. Traditionally, RDCs conduct QRAs in order to inform a decision to expeditiously field an initial capability, but then plan and execute a full operational test program to support a full-fielding decision. The Navy's plan to conduct operational or live fire (lethality) testing to support a full-fielding decision/capability deployment is unclear. OPTEVFOR is developing an integrated evaluation framework to facilitate development of operational test plans and to identify resource needs. A subset of this overall operational test to support full deployment of the capability will frame the QRA. Consistent with direction for programs on oversight, the Tomahawk Test and Evaluation Master Plan (TEMP) will undergo revision to capture the post-RDC testing strategy and the resources required to execute should the decision be made to continue forward with a full fleet-wide system release.
- During initial MST T&E planning discussions, DOT&E provided the Navy with an operational test design that utilized, as an analogy, the existing validated requirements for the Offensive Anti-Surface Weapon (OASuW) program. While the OASuW material solution is different (Long Range Anti-Ship Missile (AGM-158C LRASM)), the basic mission was assumed to be similar enough to act as a basis to develop a test design. Subsequent to providing this design, the Navy released the MST Memorandum of Capability and its contents did not require alteration of DOT&E's test design. To collect sufficient data for an adequate assessment of the capability, the test design identified the need for 16 test flights (refined from the initial 36 test flight design) conducted as integrated developmental and operational testing. This reduced number of live flight tests assumes the Navy will develop a tactical software-in-the-loop modeling and simulation test bed to support the maritime strike mission that is similar to the current Tomahawk modeling and simulation test bed for the land attack mission area. Because of the very different environments and target characteristics, the current modeling and simulation test bed, optimized for the land attack mission, is not adequate for the maritime strike mission.
- The Navy is not planning to assess the lethality of the MST against its intended target set. Since ships are a new class of targets for the Tomahawk, the lethality against these targets must be demonstrated prior to fielding. The MST will also retain the land-attack role, therefore the Navy must also assess the lethality of the MST against the legacy land targets.

Recommendations

- Status of Previous Recommendations. The Navy has partially addressed previous recommendations.
- FY17 Recommendation.
  1. The Navy should plan to conduct, and budget appropriately for, full operational and live fire testing of the MST capability. This should include development of a tactical software-in-the-loop modeling and simulation test bed, and functionality and lethality testing of the warhead for the Memorandum of Capability reference target set as well as legacy land attack missions. This planning must be documented in an approved TEMP.

VH-92A Presidential Helicopter Replacement Program

Executive Summary
- The VH-92A program is progressing on schedule with excellent teamwork and open communication among all agencies involved.
- The Navy modified two Sikorsky S-92A aircraft to produce two VH-92A aircraft and the first aircraft has entered contractor testing with the second to follow in the fall of 2017.
- This effort includes the integration of the Mission Communications System (MCS) designed by Naval Air Systems Command (NAVAIR) at St. Inigoes, Maryland. MCS software development is progressing on schedule.
- The Navy intends to conduct integrated flight testing in mid-FY18. It will be followed by an operational assessment planned for December 2018 through January 2019 to support a Milestone C decision in 2QFY19. Planning for the operational assessment is progressing on schedule.
- VH-92A-unique fuel bladders passed drop testing in April 2017 after initial drop testing failures.
- The program has solved the challenges relative to connecting to the Crisis Management System and the Executive Airlift Command Network.
- Live fire testing is proceeding as scheduled.

System
- The VH-92A is a dual-piloted, twin-engine helicopter based on the Sikorsky S-92A. The Navy intends the VH-92A to maintain Federal Aviation Administration (FAA) airworthiness certification throughout its lifecycle.
- The VH-92A aircraft will replace the current Marine Corps fleet of VH-3D and VH-60N helicopters flown by Marine Helicopter Squadron One (HMX-1) to perform the presidential airlift mission.
- The Navy intends the VH-92A to be capable of operating worldwide in day, night, or adverse weather conditions. The VH-92A will be air-transportable to remote locations via a single Air Force C-17 cargo aircraft.
- The government-designed MCS will provide the ability to conduct simultaneous short- and long-range secure and non-secure voice and data communications. The Navy intends MCS to exchange situational awareness information with outside agencies, organizations, and supporting aircraft. The MCS hardware will be installed into the VH-92A at Sikorsky Aircraft in Stratford, Connecticut, and then software will be loaded and checked out by Lockheed Martin in Owego, New York.
- Final interior finishing and aircraft painting will be done at Owego to complete the VH-92A for deployment.
- Delivery of the first two Engineering Development Models (EDM-1 and EDM-2) is on schedule for 2018, followed by four System Development Test Article aircraft planned for 2019.

Mission
- HMX-1 equipped with the VH-92A aircraft will provide safe and timely transport of the President of the United States and other parties as directed by the White House Military Office.
- The VH-92A is required to operate from commercial airports, military airfields, Navy ships, and austere sites throughout the world.

Major Contractors
- Sikorsky Aircraft – Stratford, Connecticut (a Lockheed Martin Company subsidiary company since 2015)
- Lockheed Martin – Owego, New York

Activity
- Modifications to two S-92A aircraft are complete, and the aircraft are now in the VH-92A configuration. EDM 1 achieved its first flight at the Sikorsky facility in Stratford, Connecticut, on July 28, 2017. It has entered into contractor testing and has relocated to the Lockheed Martin facility at Owego, New York.
- EDM-2 is expected to achieve its first flight in November 2017 and it will then join EDM-1 for contractor testing at Owego. Sikorsky conducted flight test events close to the original program schedule.
- NAVAIR at St. Inigoes, Maryland, is continuing development of the MCS software. Systems integration laboratories, which

replicate the MCS for development, test, and training, are up and running and MCS software development is on schedule
- Sikorsky installed the MCS hardware as part of the VH-92A modifications and Lockheed Martin is installing early builds of the MCS software into the EDMs at Owego.
- The Navy is continuing to plan for the VH-92A operational assessment, which is forecast for December 2018 through January 2019. It includes HMX-1 aircrews, and 30 flight hours over 30 days utilizing two VH-92A aircraft. This assessment will exercise all Presidential airlift missions at actual mission sites with personnel participating from all agencies that support the White House. Scenarios are planned to include both VH-92A cabin configurations.
- After initial drop testing failures, the VH-92A-unique fuel bladders passed drop testing in April 2017.
- Live fire testing is proceeding as scheduled.

Assessment
- The program is progressing on schedule. Maintenance of FAA airworthiness certification is a key emphasis area.
- The Navy intends to conduct integrated developmental/operational testing for 150 flight hours at Naval Air Station Patuxent River, Maryland, beginning in mid-FY18 and will include loading a VH-92A onto a C-17 to simulate a long-distance deployment. Integrated testing will be followed by an operational assessment planned for December 2018 through January 2019 to support a Milestone C decision in 2QFY19.
- Preparing the operational assessment plan is on schedule. The Navy's Operational Test and Evaluation Force (OPTEVFOR)/HMX-1 will function as the Operational Test Agency and DOT&E will oversee testing. Timing of EDM-2 delivery in time for this operational assessment is a watch item.
- The program has solved previous challenges meeting the Net Ready Key Performance Parameter for the MCS relative to connection to the Crisis Management System and connection to the Executive Airlift Command Network.
- Preliminary review of the live fire test data collected to date is underway and proceeding well.

Recommendations
- Status of Previous Recommendations. The Navy should continue to address the FY16 recommendations.
  1. Complete plans for the operational assessment planned for December 2018 through January 2019.
  2. Continue planning efforts for HMX-1 transition to VH-92A.
- FY17 Recommendations. None.

Air Force Programs

Air Force Programs

AC-130J Ghostrider

Executive Summary

- The program completed Block 20 developmental testing in March 2017.
- The 18th Flight Test Squadron (18th FLTS), along with aircrews from the 1st Special Operations Group, Detachment 2, conducted an IOT&E of the Block 20 AC-130J from March 15 to July 20, 2017, to support a Full-Rate Production decision. The IOT&E included a Cooperative Vulnerability and Penetration Assessment (CVPA) in April 2017 and an Adversarial Assessment (AA) in June 2017.
- Although analysis is ongoing, preliminary data from the IOT&E indicate that the Block 20 AC-130J will support most elements of the Close Air Support and Air Interdiction missions, but some shortfalls remain:
  - The AC-130J's Gun Weapon System (GWS) fire control performed inconsistently when accounting for changing ballistic conditions. The 30 mm GWS also displayed problems maintaining a full rate of fire.
  - The complexity of system software, inadequate training and technical manuals, and the overall operating environment aboard the AC-130J diminishes usability.
- The Program Office has initiated efforts to correct the shortfalls identified during IOT&E.
- Block 30 commenced developmental testing in July 2017 and will include several new capabilities such as an integrated Combat System Officer (CSO) station, a special mission processor, and wing-mounted AGM-114 HELLFIRE missiles.
- The program declared Initial Operational Capability (IOC) on September 30, 2017.

System

- The AC-130J is a medium-sized, multi-engine, tactical aircraft with a variety of sensors and weapons for air-to-ground attack.
- The AC-130J is operated by nine aircrew members: two pilots, one CSO, one weapons system operator, and five special mission aviators (one sensor operator, one load master, and three gunners).
- U.S. Special Operations Command (USSOCOM) is developing AC-130J through the integration of modular components onto existing MC-130J aircraft. The AC-130J includes an open architecture to allow for follow-on development and future integration of block capabilities.
- Block 20 consists of the following modular components:
  - A dual-console Mission Operator Pallet (MOP) in the cargo bay controls all subsystems with remote displays and control panels on the flight deck.
  - An interim, limited-functionality, carry-on flight deck workstation for a CSO.
  - The weapon suite consists of an internal, pallet-mounted 30 mm side-firing chain gun and 105 mm cannon; wing-mounted GBU-39/B GPS-guided Small Diameter Bombs (SDBs) and GBU-39B/B Laser SDBs; and AGM-176 Griffin laser-guided missiles mounted internally and launched through the rear cargo door.
  - Two MX-20 electro-optical/infrared sensor/laser designator pods and multiple video, data, and communication links.
  - A side-mounted heads-up display (HUD) enhances pilot situational awareness in the cockpit.
- Block 30 future updates include:
  - A permanent CSO station on the flight deck.
  - A Special Mission Processor.
  - Wing-mounted AGM-114 HELLFIRE missiles.
- Block 40 will include a radio-frequency countermeasures (RFCM) system.
- The AC-130J retains all survivability enhancement features found on the MC-130J aircraft.
  - Susceptibility reduction features include the AN/ALR-56M radar warning receiver, the AN/AAR-47(V)2 Missile Warning System, the AN/ALE-47 countermeasure dispensing system, and the Large Aircraft Infrared Countermeasures system with the Next Generation Missile Warning System.
  - Vulnerability reduction features include fuel system protection (fuel tank foam to protect from ullage explosion), redundant flight-critical components, and armor to protect the crew and the oxygen supply.
- The AC-130J will replace legacy AC-130H/U aircraft.

Mission

The Joint Task Force or Combatant Commander will employ units equipped with the AC-130J to provide close air support and air interdiction using battlespace wide area surveillance, target geolocation, and precision munition application. Additionally, the AC-130J provides time-sensitive targeting, communications, and command and control capabilities.

Major Contractor
Lockheed Martin – Bethesda, Maryland

Activity

- The USSOCOM Acquisition Executive declared Milestone C for the AC-130J on October 5, 2016.
- The AC-130J Combined Test Force (CTF) of the 96th Operations Group completed the majority of Block 20 developmental testing in December 2016. The CTF conducted additional testing on the newly installed side-HUD in January and February, and verification of a deficiency correction to the SDB bomb rack in March 2017.
- The 18th FLTS, along with aircrews from the 1st Special Operations Group, Detachment 2, conducted an IOT&E of the Block 20 AC-130J from March 15 to July 20, 2017, in accordance with a DOT&E-approved test plan. Aircrew flew a total of 29 sorties and 130 flight hours from Hurlburt Field, Florida, and Marine Corps Base Kaneohe Bay, Hawaii. The IOT&E included a CVPA in April 2017 and an AA in June 2017.
- During IOT&E, the 18th FLTS completed 11 mission vignettes on specific capabilities; 10 full mission profile scenarios; 1 day of cold weather testing; and 2 phases of cybersecurity testing to fully characterize and evaluate the system. Testing expended 5,707 rounds of 30 mm and 105 mm ammunition and 26 precision-guided munitions.
- During IOT&E, the 780th Test Squadron, in coordination with DOT&E and the AC-130J CTF, conducted Phase 2 live fire testing to support the lethality evaluation of the AGM-176 Griffin missile against static ground targets and maneuvering boats, and the 105 mm gun against structures, personnel, technical vehicles, and lightly armored air defense vehicles.
- The program received the ninth aircraft in July 2017 to support declaring an IOC with six Block 20 aircraft. The twelfth MC-130J aircraft was inducted for modification to a Block 20 AC-130J in August 2017
- Production line cut-in of the Block 30 configuration is expected to begin with aircraft 14. The second and third aircraft, originally Block 10 configuration, were inducted for retrofitting to Block 30 to support developmental test and evaluation (DT&E) and the RFCM program.
- The U.S. Air Force Combat Effectiveness and Vulnerability Analysis Branch completed the Ballistic Vulnerability Analysis, Anti-Aircraft Artillery Susceptibility Analysis, Proximity Burst Analysis, and Occupant Casualty Analysis in 2QFY17.
- USSOCOM is developing the RFCM system for MC-130J and AC-130J under a separate Acquisition Category II program, with three AC-130J aircraft supporting trial-kit installation and testing beginning in 2QFY18. The RFCM program expects to conduct IOT&E in FY19 and will become part of the Block 40 AC-130J.

Assessment

- Analysis of IOT&E data was ongoing at the end of FY17. DOT&E expects to issue an IOT&E report in 1QFY18 to inform the 2QFY18 Full-Rate Production decision.
- A problem with the integration of the Bomb Rack Unit (BRU)-61/B was discovered late in DT&E and delayed the start of IOT&E by 2 weeks. A software conflict between the MOP and the BRU-61/B during multi-round salvos caused the BRU computer to lock up and inhibit release of SDBs. Regression testing verified the correction of the software error prior to IOT&E.
- Preliminary data indicate the Block 20 AC-130J will support most elements of the Close Air Support and Air Interdiction missions, but some notable shortfalls remain.
  - In live fire testing during IOT&E, the AC-130J successfully engaged operationally representative targets with its entire precision-guided munitions suite. Testing also included long-range engagements at the edge of the Launch-Acceptable Region that demonstrated the AC-130J's increased stand-off range.
  - Although the AC-130J aircrew were able to engage targets successfully with both guns throughout IOT&E, the GWS displayed performance inconsistencies.
    - Once calibrated, the Gun Fire Control System (GFCS) should compensate for changes in altitude, slant range, and ambient wind to enable accurate first rounds on target. However, changes in altitude or slant range would sometimes require a calibration update.
    - Operators are unable to independently update the GFCS wind calibration factor without changing the inherent gun-mount calibration factor, as they can on the same GWS on AC-130W.
    - The 30 mm GWS on the AC-130J experiences excessive "retriggers" in full rate of fire that reduce the utility of the firing mode, and which are not observed on the AC-130W. A retrigger occurs when the aim point of the gun is perturbed by recoil beyond a preset angular limit, called Tracking Inhibit; the gun will stop firing when it exceeds this limit so that it can re-center itself, and the operator must release and re-depress the trigger to resume fire.
  - Autonomous threat acquisition by aircraft defensive equipment is improving with each generation of aircraft in ways that may not be thoroughly demonstrated in operational test conditions; these capabilities may require follow-on tactics development by 18th FLTS.
  - Although Block 20 computational performance and stability improved over Block 10 operational utility evaluation (OUE) results, (preliminary data indicate fewer

system freezes or reboots), operator assessments of system usability did not improve over Block 10. Preliminary data show no statistically significant change in system usability survey scores from flight deck crew and MOP operators between Block 10 and Block 20; scores from special mission aviators, who now have the additional 105 mm gun to operate, decreased from Block 10.
    - System complexity, inadequate training and technical data, and multiple layers of logistics support contributed to poor system usability ratings. The multiple datalink systems require precise configuration by contract logistics support or aircrew before each mission. Although datalink availability improved over the Block 10 OUE, inconsistent procedures caused some datalinks to be unavailable on a few IOT&E sorties. Lack of datalink integration with primary MOP controls and displays increases operator workload to monitor them and degrades situational awareness.
  - Many of the deficiencies in the Block 10 aircraft that diminish usability remain a problem on the Block 20 aircraft. Light pollution from the added displays, which interferes with night-vision goggle operations by special mission aviators, has not improved. Although the cargo area floor has been leveled by the addition of floor panels to reduce trip hazards, the modifications now interfere with loading of 105 mm ammunition. The lack of a forward restraint in the 105 mm ammunition rack caused an excessive number of rounds to come loose from the brass in the gun breech.
- The CTF completed Phase 2 live fire lethality testing of the Griffin missile and 105 mm gun during Block 20 DT&E and IOT&E. Preliminary data analysis indicate:
  - The Griffin demonstrated mobility kills against stationary and moving trucks, as well as small boats, in both height-of-burst and point-detonate modes.
  - The PGU-46/B 30 mm round demonstrated limited effectiveness against personnel in the open on soft ground but is more effective against personnel on hard surfaces. For example, lethality to personnel above a "soft" plywood roof is lower than predicted because the round detonated below the roof's surface; manikins above a concrete roof incur more fragmentation damage than above a plywood roof.
  - The 105 mm round demonstrated expected lethality against personnel, trucks, and light armored vehicles.
- Preliminary results from the Vulnerability Analyses did not demonstrate any unexpected vulnerabilities, compared to legacy C-130 aircraft.
- The IOT&E phase included cybersecurity testing of the Block 20 AC-130J. Details will be described in the classified portion of the IOT&E report.
- Cold weather testing at McKinley Climatic Lab was halted due to concerns over cold-soaking short supply components likely to break at lower temperatures. The program still needs to address how it will deploy in cold conditions while maintaining full mission capability.

Recommendations

- Status of Previous Recommendations.
  1. The program closed all but two previous Category I – Urgent Deficiency Reports (DRs); one was downgraded. The program continues to work on a solution to the GPS interference DR.
  2. The program did not pursue fielding the PGU-13D/B 30 mm ammunition, so no additional lethality testing was necessary.
  3. The program has not yet provided a draft update to the Test and Evaluation Master Plan (TEMP) for the Full-Rate Production decision, but DOT&E continues to discuss the future test strategy with the test team.
- FY17 Recommendations. The Program Office should:
  1. Identify and implement upgraded GFCS software to correct accuracy and re-trigger anomalies prior to AC-130J deployment.
  2. Include a clear test strategy for future testing of the new capability increment baseline in the TEMP update for the Full-Rate Production decision. This should incorporate additional cybersecurity testing at the appropriate block of capability enhancement.
  3. Develop a plan to update and test tactics, techniques, and procedures for operational employment of the Block 20 AC-130J defensive systems suite.
  4. Work with 18th FLTS to complete the AC-130J cold climate evaluation.

AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM)

Executive Summary

- The Services completed operational test activities for the Air Intercept Missile (AIM)-120D System Improvement Program 1 (SIP-1) in November 2016; SIP-1 fielded in April 2017. SIP-1 is one of several software upgrade programs designed to enhance AIM-120D performance.
- The Services began operational test activities for the AIM-120C7 Advanced Medium-Range Air-to-Air Missile (AMRAAM) Advanced Electronic Protection Improvement Program (EPIP) in 2016, with testing continuing through mid-2018.
- The Air Force and Navy are in the final stages of test planning and scheduling to conduct cybersecurity testing of the AMRAAM missile, forecast to begin in summer 2018.

System

- AMRAAM is a radar-guided, air-to-air missile with capability in both the beyond visual-range and within visual-range arenas. A single aircraft can engage multiple targets with multiple missiles simultaneously when using AMRAAM.
- F-15C/D/E, F-16C/D, F/A-18C/D/E/F, EA-18G, F-35A/B, and F-22A aircraft are capable of employing the AMRAAM, and the missile is currently being tested/fielded for employment on the F-35C.
- The AMRAAM program develops and incorporates planned software upgrades. The AMRAAM Basic EPIP is a software upgrade to AIM-120C3-C7. An Advanced EPIP software upgrade began operational testing in FY16.
- The AIM-120D is the next variant in the AMRAAM family of missiles. The newest missile includes both hardware and software improvements over the AIM-120C3-C7. Four planned follow-on SIPs provide updates to the AIM-120D to enhance missile performance and resolve previous deficiencies.

Mission

- The Air Force and Navy, as well as several foreign military forces, employ various versions of the AIM-120 AMRAAM to conduct air-to-air combat missions.
- All U.S. fighter aircraft use the AMRAAM as the primary beyond visual-range air-to-air weapon.

Major Contractor

Raytheon Missile Systems – Tucson, Arizona

Activity

- The Air Force and Navy conducted all testing in accordance with DOT&E-approved test plans.

AIM-120D SIP

- The Services completed SIP-1 testing in November 2016. SIP-1 fielded in April 2017.
- SIP-2 operational test planning is in progress. Testing is scheduled to complete in 2019.

AIM-120C7 AEPIP

- Operational testing for the Advanced EPIP software upgrade to C7 missiles began in FY16 and is expected to complete in mid-FY18.

Cybersecurity

- The Air Force and Navy are in the final stages of test planning to conduct combined cybersecurity testing of the AMRAAM missile, forecast to begin in summer 2018.

Assessment

- AMRAAM continues to be operationally effective and suitable.
- The AIM-120D SIP-1 missile meets performance and reliability requirements.
- The AIM-120C3-7 Basic EPIP missile meets performance requirements.

Recommendations

- Status of Previous Recommendations. Test planning and execution are ongoing; the Air Force is addressing the previous FY15 recommendations to:
  1. Complete SIP-2 and Advanced EPIP operational testing to achieve the Services' desired mission effectiveness improvements for AMRAAM.

2. Complete cybersecurity testing of the AMRAAM missile in accordance with DOT&E cybersecurity testing policy.

- FY17 Recommendations. None.

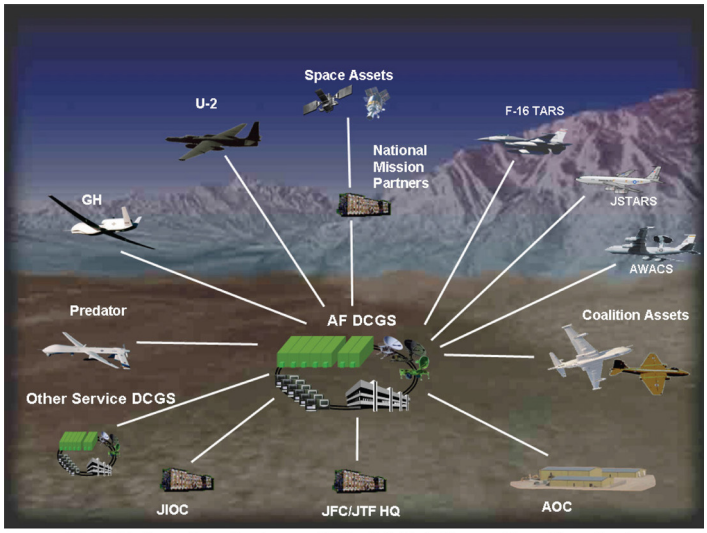
Air Force Distributed Common Ground System (AF DCGS)

Executive Summary

- The Air Force Distributed Common Ground System (AF DCGS) consists of eight Acquisition Category (ACAT) III programs. The Air Force has conducted OT&E for only three of those eight programs. Because the Air Force has not tested the entire integrated AF DCGS as a system, DOT&E cannot provide a comprehensive evaluation of AF DCGS operational effectiveness, operational suitability, and survivability.
- The operational tests for the three acquisition programs are:
  - The 605th Test and Evaluation Squadron (TES) conducted an Operational Utility Evaluation (OUE) for the Geospatial Intelligence (GEOINT) Workflow Enhancement (GWE) in August 2016. The OUE data indicate that GWE does not provide operational benefits to system operators.
  - The Air Force Operational Test and Evaluation Center (AFOTEC) conducted the System Release (SR) 3.0.1 OUE at Distributed Ground Station 2 (DGS-2) and the Distributed Mission System (DMS) site between January and February 2017. The SR 3.0.1 is intended to improve AF DCGS Signal Intelligence (SIGINT) capabilities. The test showed that the overall SIGINT performance is poor, and SR 3.0.1 did not significantly improve SIGINT performance. SR 3.0.1 is not operationally suitable, and it is not survivable against cyber threats.
  - The Air Force 605th TES completed the last phase of the four-phased Force Development Evaluation (FDE) on the GEOINT Baseline (GB) 4.1 in July 2017. GB 4.1 did not significantly improve the Air Force GEOINT capabilities.
- The Air Force began implementing an open architecture infrastructure for AF DCGS. The open architecture will phase out the legacy architectures that are no longer sustainable.

System

- AF DCGS, also referred to as the AN/GSQ-272 SENTINEL weapon system, is an intelligence enterprise system composed of 27 geographically separated, networked sites, including 5 core sites across the globe.
- AF DCGS provides hardware and software tools for planning and direction, processing and exploitation, analysis, and dissemination of intelligence, surveillance, and reconnaissance (ISR) information. The DCGS Integration Backbone provides the framework that allows sharing of ISR information with other military Services and intelligence agencies.
- The Air Force declared AF DCGS to be at Full Operational Capability in 2009 despite Air Force plans to continue system development.
- Currently, AF DCGS consists of eight ACAT III programs: Sensor Integration, GEOINT Transformation, GB 4.1, SIGINT Transformation, SR 3.0, Infrastructure Transformation, Multi Intelligence, and DCGS Reference Imagery Transition.



AOC - Air Operations Center
AWACS - Airborne Warning and Control System
GH - Global Hawk
HQ - Headquarters
JFC - Joint Forces Command
JIOC - Joint Intelligence Operations Center
JSTARS - Joint Surveillance Target Attack Radar System
JTF - Joint Task Force
TARS - Tactical/Theater Airborne Reconnaissance System

- To date, only three of the eight programs have undergone operational testing: GB 4.1, SR 3.0/3.0.1, and GWE.
  - GB 4.1 is a GEOINT upgrade that includes deficiency corrections and the capability to process and exploit feeds from updated sensors such as the Airborne Cueing and Exploitation System – Hyperspectral. The GB 4.1 update also allows continued interoperability with the sensors on the Global Hawk Block 40.
  - SR 3.0.1 is a SIGINT upgrade, which makes SIGINT data and services available to internal and external users, improves operations with the Airborne SIGINT Payload low-band sensor, and improves processing, exploitation, and dissemination for high-band sensors.
  - GWE is one of eight subsystems under the GEOINT Transformation program. GWE is intended to shorten the GEOINT workflow process.
- The Air Force is in the process of transitioning AF DCGS to an open architecture system via an agile acquisition strategy. This transition is expected to take several years. The open architecture is designed to enable the Air Force to field modular upgrades and updates on a standardized infrastructure.

Mission
- The Air Force uses AF DCGS to plan sensor information requests and to produce intelligence information from data collected by a variety of sensors on the U-2, RQ-4 Global Hawk, MQ-1 Predator, MQ-9 Reaper, MC-12, and other ISR platforms.
- The Air Force uses AF DCGS to connect to the multi-Service DCGS Integration Backbone, manage requests for sensors, process sensor data, exploit sensor data from multiple sources, and disseminate intelligence products.

Major Contractors
- Raytheon – Garland, Texas
- Lockheed Martin – Denver, Colorado
- L-3 Technologies – Greenville, Texas
- Leidos – Beavercreek, Ohio

Activity
- The 605th TES conducted a comparison test between GWE and the legacy workflow at DGS-Experimental (X) in March 2016 followed by an OUE at DGS-1 in August 2016. Both DGS-X and DGS-1 are located at Langley AFB, Virginia. The 605th TES conducted the GWE OUE in accordance with a DOT&E-approved test plan.
- AFOTEC conducted the SR 3.0.1 OUE at DGS-2 at Beale AFB, California, and DMS-Maryland in Fort Meade, Maryland, January through February 2017. DOT&E delegated test plan approval for this test to AFOTEC because it was not significantly different from the SR 3.0 OUE, which AFOTEC conducted in accordance with a DOT&E-approved test plan.
- The 605th TES conducted phase four of a four-phased FDE for GB 4.1 in July 2017 at DGS-3 at Osan Air Base, Republic of Korea, in accordance with a DOT&E-approved test plan.
- The Air Force is continuing the work on test and evaluation, systems engineering, and requirements documentation. These documents will reflect the system's transition to an open architecture infrastructure.

Assessment
- The Air Force has not conducted end-to-end AF DCGS testing that evaluates the system's ability to plan, process, and exploit multiple sources of intelligence (such as GEOINT, SIGINT, and other sources of intelligence such as web pages) and produce actionable intelligence by fusing this information.
- Neither GB 4.1 nor SR 3.0.1 significantly improved operational effectiveness. Neither GB 4.1 nor SR 3.0.1 are operationally suitable. The last phase of the GB 4.1 FDE did not produce the data to evaluate if the shortfalls noted from earlier phases regarding Full Motion Videos (FMV) have been resolved because the operational mission set at the test site during the FDE did not require FMV.
- The GWE showed potential to improve operations in a laboratory comparison test, but not during the OUE.
- AF DCGS is vulnerable to cyber adversaries. The Air Force delayed the cybersecurity Adversarial Assessment until the program can implement the new and improved firewall. The Air Force still has to resolve vulnerabilities found from previous Cooperative Vulnerability and Penetration Assessments.
- The Air Force did not provide a written description of cyber defense procedures for the system; therefore, DOT&E does not have sufficient information to recreate an operationally realistic cyber defense in operational tests.

Recommendations
- Status of Previous Recommendations. The Air Force addressed or made satisfactory progress toward implementing eight of the nine previous recommendations. The Air Force should still submit a Test and Evaluation Master Plan for DOT&E approval, which includes an accurate description of AF DCGS requirements, architecture, and interfaces sufficient to justify the test approach. The Program Office is making progress.
- FY17 Recommendations. The Air Force should:
  1. Conduct an AF DCGS system-level operational test that comprehensively evaluates the system's ability to help users process and exploit multiple sources of intelligence and produce actionable intelligence.
  2. Provide a written description of AF DCGS cyber defense process and procedures.

Air Operations Center – Weapon System (AOC-WS)

Executive Summary

- The Air Operations Center – Weapon System (AOC-WS) 10.1 is a system of systems that incorporates numerous software applications to conduct operational command and control (C2) of theater air, space, and cyber operations.
- In November and December 2016, the Air Force conducted an assessment of AOC-WS 10.1.13.3 to evaluate corrections to previously identified AOC-WS software discrepancies, upgrade AOC-WS management and mission application software, and advance the AOC-WS cybersecurity posture.
- In April and May 2017, the Air Force conducted an assessment of AOC-WS 10.1.14.E to evaluate improved encrypted access for mission software, upgrade monitoring and management capabilities of AOC systems, and advance the AOC-WS cybersecurity posture.
- Most of the contents of AOC-WS 10.1.13.3 and AOC-WS 10.1.14.E demonstrated the required capabilities for the AOC to execute the joint air tasking order cycle and conduct operational C2 of theater air operations.
  - Cybersecurity evaluations of both upgrades revealed vulnerabilities that pose risks to the AOC-WS contribution to mission.
  - To assure continued AOC Intelligence, Surveillance, and Reconnaissance Division (ISRD) contribution to the mission, the AOC-WS should maintain the Image Product Library (IPL) until Information Storage (iSToRE) can replicate all required legacy capabilities and correct known deficiencies.
  - Theater Battle Management Core Systems (TBMCS) testing identified incompatibility between TBMCS and the Air Support Operations Center. This was documented as a critical Category I deficiency.
- Despite the known cybersecurity vulnerabilities and the existing TBMCS Category I deficiency, Air Combat Command (ACC) elected to field both upgrades. The Air Force decided the operational gain of fielding TBMCS' new cryptographic-controlled access for all users and other operational capability gains in both upgrades outweighed the risk to mission.
- In April 2017, after the Senate Armed Services Committee denied the Air Force request for AOC-WS 10.2 program funding, the Air Force ceased contracted efforts on AOC-WS 10.2 development.
  - In October 2016, the Air Force submitted a Critical Change Report (CCR) after the program failed to meet Milestone C requirements and Full Deployment Decision within the 12-month program estimates for the second time.
  - The CCR was informed by poor capability performance during developmental testing.
- In August 2017, the Air Force canceled the AOC-WS 10.2 contract and is pursuing alternative approaches to achieve faster development, testing, and fielding of AOC-WS 10.2 requirements.

System

- The AOC-WS 10.1 (AN/USQ-163 Falconer) is a system of systems that incorporates numerous third-party software applications and commercial off-the-shelf products. Each third-party system integrated into the AOC-WS provides its own programmatic documentation.
- AOC-WS capabilities include C2 of joint theater air and missile defense; pre-planned, dynamic, and time-sensitive multi-domain target engagement operations; and intelligence, surveillance, and reconnaissance operations management.
- The AOC-WS consists of:
  - Commercial off-the-shelf voice, digital, and data communications hardware
  - AOC-WS software
  - Some software, including TBMCS – Force Level and the Master Air Attack Plan Toolkit (MAAPTK), is developed specifically for the AOC-WS to enable planning, monitoring, and directing the execution of air, space, and cyber operations
  - Other software applications, including Global Command and Control System – Joint (GCCS-J) and the Joint Automated Deep Operations Coordination System, are used by the AOC-WS to enable joint and interagency integration
  - Additional third-party systems that accept, process, correlate, and fuse C2 data from multiple sources and share them through multiple communications systems
- When required, the AOC-WS operates on several different local area networks (LANs), including the SECRET Internet Protocol Router Network, Joint Worldwide Intelligence Communications System, and a coalition LAN. The LANs connect the core operating system and primary applications to joint and coalition partners supporting the applicable areas of operation. Users can access web-based applications through the Defense Information Systems Network.

- The AOC-WS 10.2 requirements for a modernized, integrated, and automated approach to AOC operations remain valid. Following the cancellation of the AOC-WS 10.2 program, the Air Force remains committed to developing and fielding modernized AOC capabilities.
- C2 Air Operations Suite – C2 Information Services (C2AOS-C2IS) is a software developmental program to upgrade critical AOC-WS mission software. The Air Force intends to use the C2AOS-C2IS to enhance the ability of operators to perform AOC core tasks quickly and efficiently, as well as provide new planning and execution capabilities for integrated air and missile defense and net-enabled weapons.

Mission

The Commander, Air Force Forces or the Joint/Combined Forces Air Component Commander uses the AOC-WS to exercise C2 of joint (or combined) air forces, including planning, directing, and assessing air, space, and cyberspace operations; air defense; airspace control; and coordination of space and mission support not resident within theater.

Major Contractors

- AOC-WS 10.1 Production Center: Raytheon Intelligence, Information and Services – Dulles, Virginia
- AOC-WS 10.2 Modernization: Northrop Grumman – Newport News, Virginia

---

Activity

- In November and December 2016, the Air Force conducted an assessment of the AOC-WS 10.1.13.3, which included a Cooperative Vulnerability Inspection (CVI). The Operational Test Agency, 605th Test and Evaluation Squadron (TES), approved the test plan in accordance with delegated authority in DOT&E policy memo, "Guidelines for OT&E of Information and Business Systems," September 14, 2010. To support agile acquisition and fielding approaches, DOT&E delegates test plan approval based on an assessment of moderate or low overall risk to mission accomplishment of new software integration. AOC-WS 10.1.13.3 was assessed as moderate risk. The focus of this upgrade was to correct previously identified software discrepancies, upgrade AOC-WS management software, and advance the AOC-WS cybersecurity posture.
  - The AOC-WS software upgrades included GCCS-J, MAAPTK, and TBMCS – Force Level.
  - Additionally, this AOC WS upgrade added iSToRE software as a replacement for the AOC ISRD IPL software.
- In April and May 2017, the Air Force conducted an assessment of the AOC-WS 10.1.14.E, which included a CVI. AOC-WS 10.1.14.E new software integration was assessed as moderate risk to mission accomplishment. 605 TES approved the test plan in accordance with delegated authority from DOT&E. The focus of this upgrade was to advance the cybersecurity posture of AOC-WS; improve encrypted access for TBMCS and GCCS-J; upgrade AOC-WS software applications; and improve the capability to monitor and manage user computer-based access to AOC systems.
- In April 2017, after completion of the 2016 CCR, the Senate Armed Services Committee did not approve the Air Force budget request for AOC-WS 10.2. In August 2017, the Air Force ceased contracted efforts on AOC-WS 10.2 development and terminated the AOC-WS 10.2 contract. The Air Force stated that the current traditional acquisition strategy was not suited to take advantage of industry best practices for software development to quickly develop and field AOC-WS 10.2 requirements.
- In accordance with DOT&E recommendations, the Air Force is planning a comprehensive cybersecurity evaluation during the AOC-WS 10.1.15 upgrade planned for FY18.

Assessment

- During the November to December 2016 integrated developmental and operational test events, the Air Force adequately tested AOC-WS 10.1.13.3.
  - AOC-WS 10.1.13.3 demonstrated the required capabilities for the AOC to execute the joint air tasking order cycle and conduct operational C2 of theater air operations. While the Air Force identified some functional deficiencies during testing, these should not significantly affect the operational effectiveness and suitability of AOC-WS.
  - While iSToRE enhanced ISRD imagery management capabilities, it did not replace all the legacy functionality that currently exists in IPL.
  - A cybersecurity evaluation of AOC-WS 10.1.13.3 revealed vulnerabilities that pose risks to the AOC-WS mission.
  - In April 2017, despite the known cybersecurity vulnerabilities and some functional deficiencies, the AOC Configuration Review Board elected to field the AOC-WS 10.1.13.3 upgrade. The Air Force decided the gain in operational capability outweighed the possible risks to mission.
- During the April to May 2017 integrated developmental and operational test events, the Air Force adequately tested AOC-WS 10.1.14.E.
  - With one exception, AOC-WS 10.1.14.E demonstrated the required capabilities to support AOC execution of the joint air tasking order cycle and to conduct operational C2 of theater air operations.

- Previous TBMCS testing identified an incompatibility between TBMCS and the Air Support Operations Center. The interface incompatibility was documented as a critical Category I deficiency.
- A cybersecurity evaluation of AOC-WS 10.1.14.E revealed vulnerabilities that pose risks to the AOC-WS mission.
- In September 2017, despite the known cybersecurity vulnerabilities and existing Category I functional deficiency, ACC elected to accept the mission risk and field the AOC-WS 10.1.14E upgrade. The Air Force decided the operational gain of fielding TBMCS' new cryptographic controlled access for all users and other operational capability gains in AOC-WS 10.1.14.E outweighed the risk to the mission.

Recommendations

- Status of Previous Recommendations. The Air Force made progress on one FY15 recommendation by developing and testing software updates that close previously identified cybersecurity vulnerabilities. However, the Air Force faces the ongoing challenge of addressing emerging cybersecurity vulnerabilities identified in each AOC-WS upgrade, some of which are associated with third-party software not controlled by the AOC-WS Program Office. To address the FY15 recommendations, the Air Force needs to:
  1. Continue to improve AOC-WS dynamic cyber threat defense capabilities.
  2. Reassess the Help Desk Enabling Concept to support the installation and fielding of new capabilities at operational AOC locations.
- FY17 Recommendations. The Air Force should:
  1. Enable the AOC-WS to maintain IPL until iSToRE can replicate all required legacy capabilities and correct known deficiencies to assure continued ISRD contribution to mission.
  2. Collaborate with OSD to identify and implement any innovative operational test approaches to support the agile software development and fielding of future AOC-WS capabilities.
  3. Based on the cancellation of the AOC-WS 10.2 upgrade program, implement a solution to meet the long-standing requirement to collect and report reliability, availability, and maintainability data for the AOC-WS.

Battle Control System – Fixed (BCS-F)

Executive Summary
- In June 2017, the Air Force completed a Force Development Evaluation (FDE) on the Battle Control System – Fixed (BCS-F) Increment 3, Release 3.2.4 (R3.2.4) at all U.S. Air Defense Sectors (ADSs) and Regional Air Operations Centers (RAOCs).
- Planned BCS-F R3.2.4 capabilities included:
  - Corrections to known system management software deficiencies
  - An upgraded Radiant Mercury Guard information exchange security software and hardware
  - An upgraded cybersecurity intrusion detection system and firewall capabilities
  - Upgraded capabilities for managing information and data exchanges
  - An improved system cybersecurity posture
- While the Air Force identified some deficiencies, the ADSs and RAOCs equipped with BCS-F R3.2.4 were able to use operator workarounds to execute command and control and air battle management to support air sovereignty and air defense operations.
- As of August 2017, the Air Force transitioned to operational employment of BCS-F R3.2.4 at all ADSs and RAOCs.

System
- BCS-F is the tactical air surveillance and battle management command and control system for the continental U.S. and Canadian ADSs (Eastern ADS, Western ADS, Alaska RAOC, Canadian ADS) of the North American Aerospace Defense Command (NORAD) and U.S. Pacific Command (USPACOM) Hawaii RAOC.
- The system utilizes commercial off-the-shelf hardware within an open-architecture software configuration and operates within the NORAD and USPACOM air defense architecture.
- BCS-F integrates with the Federal Aviation Administration (FAA) via reception of FAA air surveillance radar and aircraft flight plan information.
- BCS-F R3.2.4 is a software and hardware sustainment upgrade of the BCS-F Increment 3. BCS-F R3.2.4 provides system management software upgrades, but does not add any new operational capabilities. The BCS-F R3.2.4 upgrade continues system sustainment improvements in preparation for integration with the new Wide Area Surveillance (WAS) sensor and an updated cybersecurity operational evaluation. BCS-F R3.2.4:
  - Replaced system cybersecurity intrusion detection and firewall hardware and software
  - Upgraded the Radiant Mercury Guard information exchange software and hardware
  - Upgraded system cybersecurity capabilities for managing information and data exchanges
  - Advanced the BCS-F cybersecurity posture

Mission
- The Commander, NORAD and Commander, USPACOM use BCS-F to execute command and control and air battle management to support air sovereignty and air defense missions for North American Homeland Defense and USPACOM air defense.
- Air defense operators employ BCS-F to conduct surveillance, identification, and control of U.S. sovereign airspace and control air defense assets, including fighters, to intercept and identify potential air threats to U.S. airspace.

Major Contractor
Raytheon Systems – Fullerton, California

Activity
- From April through June 2017, the 605th Test and Evaluation Squadron conducted an FDE on BCS-F R3.2.4 at all U.S. ADSs in accordance with the DOT&E-approved Test and Evaluation Master Plan and FDE test plan in April 2017.
- Prior to initiating the FDE on BCS-F R3.2.4, the Air Force elected to defer fielding of the intrusion detection capabilities.
- In September 2017, the Air Force initiated test and evaluation of the replacement intrusion detection system and firewall capabilities. This testing is ongoing and will not be completed until FY18.

- In addition to the Radiant Mercury Guard and ongoing intrusion detection system and firewall capabilities upgrade, the BCS-F Program Office has begun collaboration meetings to plan for a future BCS-F system cybersecurity assessment.

Assessment

- During the April to June 2017 dedicated operational test events at the ADSs and RAOCs, the Air Force adequately tested BCS-F R3.2.4.
  - Most of the contents of BCS-F R3.2.4 demonstrated the required capabilities for the NORAD ADSs and RAOCs, as well as the USPACOM Hawaii RAOC to execute command and control and air battle management to support air sovereignty and air defense operations.
    - While BCS-F R3.2.4 resolved numerous previously known deficiencies in battle management and mission support operations, it resulted in several new deficiencies. The most significant of these deficiencies adversely affected the integration of FAA-sourced flight plans.
    - The Air Force is planning for regression testing of a planned system update to resolve this deficiency.
  - During developmental testing, a cybersecurity vulnerability inspection of BCS-F R3.2.4 revealed vulnerabilities that could pose risks to homeland air sovereignty and air defense mission.
  - Due to delays in the development of the WAS sensor, the Air Force did not complete systems integration and operational testing of WAS with BCS-F.
- Although the Air Force did not collect sufficient operational test data to demonstrate the system availability and reliability with statistical confidence, BCS-F R3.2.4 is maintainable and reliable.
  - During 773.43 hours of testing, BCS-F R3.2.4 demonstrated a 99.97 percent operational availability, experiencing 14 minutes of system downtime.
  - Operating with BCS-F R3.2.4, the ADSs and RAOCs demonstrated a Mean Time Between Corrective Maintenance Actions (MTBCMA) of 9.2 hours.
  - The overall MTBCMA did not meet the operational requirement of 100 hours MTBCMA. The MTBCMA for Critical Field Repair Actions (2 failures) was 386.6 hours and the MTBCMA for Non-Critical Field Repair Actions (84 failures) was 9.4 hours.
- BCS-F R3.2.4 technical documentation and training for the system remains deficient.
  - Due to poorly developed system maintenance documentation, numerous discrepancies in system documentation were discovered during the FDE at each ADS and RAOC.
  - ADS and RAOC leaders are concerned the training provided during initial delivery of new capability is not at an appropriate level of detail, and not resourced to support immediate transition to unit operations and maintenance personnel. This is significant when considering ADS and RAOC commanders are engaged in continuous 24/7 real-world mission operations and are not resourced for development of new equipment and new system capability training for all unit personnel.
- The system survivability against cyber threats remains unknown. Changes in the system architecture have been implemented since BCS-F R3.2.2. While the Air Force has conducted periodic cybersecurity vulnerability inspections during developmental testing, BCS-F has not had a comprehensive cybersecurity assessment since 2012.
- To assess BCS-F system reliability and availability with the BCS-F R3.2.4 upgrades, each ADS and RAOC conducted a 2 to 3 week operations trial period at the end of the FDE.
  - After completion of the operations trial period, during which no additional system discrepancies were identified, ACC and each ADS and RAOC transitioned to operational employment of the BCS-F system with the BCS-F R3.2.4 upgrade.
  - The assessed deficiencies identified during the FDE, including the FAA flight plan integration deficiency, have acceptable operator workarounds that effectively mitigated any negative effects on mission due to operational employment of the system.

Recommendations

- Status of Previous Recommendations. The Air Force still needs to:
  1. Provide training instruction and resources on new capabilities in a format that minimizes the impact on personnel scheduling and availability while conducting a 24/7 real-world mission.
  2. Ensure accurate documentation of system upgrades and new capabilities to minimize the number of deficiencies identified during fielding and OT&E.
  3. Develop a method to monitor BCS-F life-cycle system operational availability and reliability in order to inform program life-cycle management and sustainment policies.
  4. Complete a system cybersecurity assessment to identify, prioritize, and correct cybersecurity deficiencies.
- FY17 Recommendations. None.

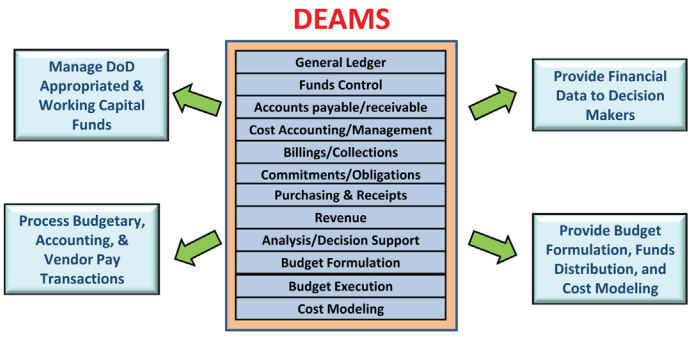
Defense Enterprise Accounting and Management System (DEAMS)

Executive Summary

- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted Operational User Evaluation (OUE) phase one testing from July 31 to August 18, 2017.
- The initial results from phase one of the OUE demonstrated significant operational effectiveness and suitability improvements from the Defense Enterprise Accounting and Management System (DEAMS) Increment 1 IOT&E. Following IOT&E, DOT&E assessed DEAMS Increment 1 as not operationally effective, not operationally suitable, and not survivable.
- DEAMS remains not survivable in a contested cyber environment, based on cybersecurity testing conducted during the OUE.

System

- DEAMS Increment 1 is a Major Automated Information System that uses commercial off-the-shelf enterprise resource planning software to provide accounting and management services.
- The DEAMS Increment 1 Program Management Office (PMO) is following an evolutionary acquisition strategy that adds additional capabilities and users incrementally. There are six scheduled releases. The Air Force anticipates over 15,000 users worldwide will use DEAMS by the end of the increment.
- DEAMS Increment 1 is intended to improve financial accountability by providing a single, standard, automated financial management system that is compliant with the Chief Financial Officers Act of 1990 and other mandates. DEAMS Increment 1 performs the following core accounting functions:
  - Core Financial System Management
  - General Ledger Management
  - Funds Management
  - Payment Management
  - Receivable Management
  - Cost Management
  - Reporting



- DEAMS interfaces with approximately 40 other systems that provide travel, payroll, disbursing, transportation, logistics, acquisition, and accounting support.
- DEAMS supports financial management requirements in the Federal Financial Management Improvement Act of 1996 and the DOD Business Enterprise Architecture.

Mission

Air Force financial managers and tenant organizations use DEAMS Increment 1 to do the following across the Air Force, U.S. Transportation Command, and other U.S. component commands:

- Compile and share accurate, up-to-the-minute financial management data and information
- Satisfy congressional and DOD requirements for auditing of funds, standardizing of financial ledgers, timely reporting, and reduction of costly rework

Major Contractors

- DSD Laboratories – Sudbury, Massachusetts
- Accenture Federal Services – Dayton, Ohio

Activity

- AFOTEC conducted phase one of the OUE from July 31 to August 18, 2017, in accordance with a DOT&E-approved plan. The Air Force plans to conduct phase two in the second and third quarters of FY18. OUE phase one testing collected day-to-day operations data at the following locations: Scott AFB, Illinois; MacDill AFB, Florida; Barksdale AFB, Louisiana; Nellis AFB, Nevada; Joint Base San Antonio-Randolph, Texas; Defense Finance and Accounting Service, Limestone, Maine.
- As part of the OUE, the Army Research Laboratory at White Sands Missile Range, New Mexico, supported the PMO in conducting a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) August 7-11, 2017, at Maxwell AFB – Gunter Annex, Alabama.

Assessment

- The initial results from phase one of the OUE demonstrated significant improvement from the DEAMS Increment 1

IOT&E (conducted in 2015) and the Verification of Fixes test (conducted in early 2016), during which DEAMS did not effectively perform several critical accounting and management tasks, four of which were Key Performance Parameters (KPPs). Some key effectiveness findings from the OUE test are:

- DEAMS provided an accurate balance of available funds to meet the KPP requirement. During the OUE, 97.5 percent of the balance queries were accurate, which is a significant improvement from the 62 percent demonstrated during the Verification of Fixes test.
- The PMO provided a new reporting tool to supplement the existing Discoverer reporting tool. Users found the new reporting tool to be useful. However, some users continue to rely on the Commanders' Resource Integration System and other legacy systems for reporting instead of using the DEAMS-provided reporting tools. Previous operational testing has found the Discoverer tool is not operationally suitable and has reached end of life.
- Transaction backlog continues to be a problem with DEAMS. During FY17, DEAMS posted over 99 percent of all transactions received from interface partners. Researching backlog transactions from interfacing systems is a manual process. The source data quality at the interfacing system may not be well controlled and can require the development of scripts to reprocess data.

- The DEAMS Program Office has made significant progress in the area of regression testing, which helps verify that enhancements or defect fixes to software do not adversely affect overall system performance. As of August 2017, regression scripts covered 22 of the 24 critical interfaces. In March 2016, regression scripts covered only four critical interfaces.
- At the start of the OUE in July 2017, the PMO reported 47 Severity 2 defects that adversely affect DEAMS. Severity 2 defects do not have a sustainable work around.
- DEAMS remains not survivable in a contested cyber environment. While the PMO has added cybersecurity to the deficiency management system for visibility and action, instituted dedicated cybersecurity patch releases on a quarterly basis, and reprioritized all cybersecurity findings for correction or risk acceptance, the CVPA showed that several high impact vulnerabilities continue to degrade DEAMS cybersecurity.

Recommendations

- Status of Previous Recommendations. The PMO did not completely satisfy the FY16 recommendations and should:
  1. Complete integration and testing of the Oracle Business Intelligence Enterprise Edition (OBIEE) reporting tool and demonstrate effectiveness through operational testing to allow the retirement of Discoverer and fielding of OBIEE.
  2. Complete mitigation of all cybersecurity vulnerabilities.
- FY17 Recommendations. The DEAMS Program Manager should:
  1. Continue efforts to reduce severity 2 defects in DEAMS.
  2. Continue efforts to reduce transaction backlog including the development of reusable scripts to fix transaction errors to ensure transaction ledgers are accurate and complete.

F-22A – Raptor Modernization

Executive Summary

- F-22A Increment 3.2B is a Major Defense Acquisition Program modernization effort intended to integrate AIM-120D and AIM-9X missile systems; an Enhanced Stores Management System (ESMS) for weapons integration and employment improvements; Intra-Flight Data Link (IFDL) improvements and electronic protection enhancements; improved emitter geolocation capability; and a Common Weapon Employment Zone for air-to-air missile employment.
- The Air Force identified ESMS deficiencies during Increment 3.2B developmental testing, completed in August 2017. Some of these were carried over into IOT&E, and the Air Force deferred corrective action to a future Operational Flight Program (OFP) effort.
- The Air Force Operational Test and Evaluation Center (AFOTEC) began Increment 3.2B IOT&E in September 2017 and will complete in April 2018. The Increment 3.2B Full-Rate Production decision is currently scheduled to occur in July 2018. F-22A Increment 3.2B IOT&E adequacy requires the ability to conduct mission-level, open-air flight testing against specific adversary air capabilities. As of the start of IOT&E, the Air Force was not able to provide the means to conduct open-air testing on the Nevada Test and Training Range (NTTR) using all of the appropriate air assets required by the IOT&E test plan.
- The NTTR Air-to-Air Range Infrastructure (AARI) instrumentation system provides an automated means for real-time battle shaping crucial to complex F-22A open-air operational flight testing through shooter-to-target accredited weapons fly-out simulations. As of September 2017, the Air Force had not demonstrated AARI readiness to support FY17-18 Increment 3.2B IOT&E and will not be able to accredit the system due to lack of end-to-end verification of all functions and detailed validation of weapons fly-out models.
- Without an accredited AARI system, the Air Force lacks the means of resolving operational mission-level measures for F-22A Increment 3.2B IOT&E in open-air flight testing, and places pending FY18 F-35 IOT&E open-air NTTR testing in jeopardy since a fully functional AARI is required for F-35 IOT&E.

System

- The F-22A is an air-superiority fighter that combines low observability to threat radars, sustained high speed, and integrated avionics sensors.
- Low observability reduces threat capability to engage F-22As with current adversary weapons.
- The aircraft maintains supersonic speeds without the use of an afterburner.
- Avionics that fuse information from the Active Electronically Scanned Array radar, other sensors, and datalinked information for the pilot enable employment of medium- and short-range air-to-air missiles, guns, and air-to-ground munitions.

- The Air Force intended the F-22A to be more reliable and easier to maintain than legacy fighter aircraft.
- F-22A air-to-air weapons are the AIM-120C/D radar-guided missile, the AIM-9M/X infrared-guided missile, and the M61A1 20 mm gun.
- F-22A air-to-ground precision strike capability consists of the 1,000-pound Joint Direct Attack Munition and the 250-pound Small Diameter Bomb Increment 1.
- The F-22A program delivers capability in increments. Incremental Enhanced Global Strike modernization efforts include the following current and near-term modernization efforts:
  - Increment 3.1 provided enhanced air-to-ground mission capability, to include geolocation of selected emitters, electronic attack, air-to-ground synthetic aperture radar mapping and designation of surface targets, and Small Diameter Bomb integration.
  - Increment 3.2A was a software-only upgrade providing improved electronic protection, Link 16 Receive, and combat identification capabilities. Increment 3.2A is a modernization effort within the scope of the F-22A Advanced Tactical Fighter baseline acquisition program of record and is currently fielded in operational F 22A units.
  - Update 5 combined an OFP upgrade providing software-driven radar enhancements, Ground Collision Avoidance System software, and the incorporation of limited AIM-9X capabilities. The Update 5 OFP is currently fielded in operational F-22A units.
  - Increment 3.2B is a separate Major Defense Acquisition Program modernization effort intended to integrate AIM-120D and AIM-9X missile systems; an ESMS for weapons integration and employment improvements;

IFDL and electronic protection enhancements; improved emitter geolocation capability; and integration of a Common Weapon Employment Zone for air-to-air missiles employed by the F-22A.
- Update 6 is a software-only OFP effort to update the aircraft KOV-20 cryptographic module with an F-22A cryptographic architecture change to accommodate multiple, simultaneous algorithms for Link 16 datalink interoperability and secure ultra-high frequency radio communications. Update 6 is also intended to incorporate deferred software corrections carried over from Increment 3.2B developmental testing. The Air Force intends to field Update 6 in CY19.
- F-22A Tactical Link 16 (TACLink) and Tactical Mandates (TACMAN) are separate pre-Milestone B hardware and software modernization programs intended to provide Link 16 transmit capability through the Multifunctional Information Distribution System/Joint Tactical Radio System and replace the legacy Mark XVII Mode 4 Identification Friend or Foe (IFF) system with the Mode 5 IFF system. The Air Force expects to field TACLink and TACMAN capabilities in FY21 and FY22, respectively.

Mission

Commanders will use units equipped with the F-22A to:
- Provide air superiority over friendly and non-permissive, contested enemy territory
- Defend friendly forces against fighter, bomber, or cruise missile attack
- Escort friendly air forces into enemy territory
- Provide air-to-ground capability for counter-air, strategic attack, counter-land, and enemy air defense suppression missions

Major Contractor

Lockheed Martin Aeronautics Company – Fort Worth, Texas

Activity
- The Air Force conducted Increment 3.2B testing in accordance with the DOT&E-approved Test and Evaluation Master Plan.
- The Air Force completed Increment 3.2B developmental testing in August 2017. Some of the deficiencies identified in developmental testing were carried over into IOT&E, and the Air Force deferred corrective action to a future OFP effort.
- AFOTEC began Increment 3.2B IOT&E in September 2017 and will complete in April 2018. The Increment 3.2B Full-Rate Production decision is currently scheduled to occur in July 2018.
- The NTTR AARI instrumentation system provides an automated means for real-time battle shaping crucial to complex F-22A open-air operational flight testing through shooter-to-target accredited weapons fly-out simulations. As of September 2017, the Air Force had not demonstrated AARI readiness to support FY17-18 Increment 3.2B IOT&E.

Assessment
- F-22A Increment 3.2B developmental testing experienced performance shortfalls across some of the enhancement capabilities that led to multiple unplanned OFP revisions. Accordingly, IOT&E did not begin until early September. ESMS functionality shortfalls identified in FY16-17 flight testing were not fully resolved. The Air Force deferred corrective action to future Update 6 OFP software modernization efforts.
- F-22A Increment 3.2B IOT&E adequacy requires the ability to conduct mission-level, open-air flight testing against specific adversary air capabilities in order to vet the full capabilities of the Increment 3.2B hardware and software enhancements. As of the start of IOT&E in September 2017, the Air Force was not able to provide the means to conduct open-air testing on the NTTR using all of the appropriate air assets required by the IOT&E plan. IOT&E open-air flight test execution will be inadequate unless the Air Force can provide the required assets for testing.
- NTTR AARI development was late to need for Increment 3.2B IOT&E, and as of September 2017 had not successfully completed network tests necessary for AARI utilization in IOT&E. AARI accreditation using current standards for test resource modeling and simulation is unlikely due to the lack of end-to-end verification of all functions and detailed validation of weapons fly-out models against valid reference sources such as live fire data and high-fidelity vendor models.
  - Without accreditation, AARI weapon fly-outs cannot be used to complete operational testing, and human intervention utilizing Range Training Officers (RTOs) will be required to accomplish missions.
  - Reliance on RTO interventions increases the risk of incorrect "kill" decisions due to estimates of weapons performance coupled with the dynamic nature of F-22A flight missions. This increases the likelihood that IOT&E missions may have to be reflown, creating the need for resources that would have been unnecessary with a working, accredited AARI system.
  - Without an accredited AARI system, it will be more difficult for the Air Force to resolve highly complex operational mission-level measures for F-22A Increment 3.2B IOT&E in open-air flight testing, and places pending FY18 F-35 IOT&E open-air NTTR testing in jeopardy since a fully functional AARI is required for F-35 IOT&E.

Recommendations

- Status of Previous Recommendations.
  1. The Air Force partially addressed FY16 recommendations regarding Increment 3.2B performance deficiencies and software anomalies, and deferred some corrective actions to future aircraft OFP efforts.
  2. In FY14, DOT&E recommended the Air Force resolve AARI sustainment, test readiness, and modernization shortfalls in order to support Increment 3.2B IOT&E test adequacy; however, the system did not demonstrate readiness for FY17 testing.
- FY17 Recommendations. The Air Force should:
  1. Provide the means to conduct F-22A operational testing against the adversary threat composition needed to fully vet F-22A and similar (i.e. F-35) capabilities in open-air flight testing on the NTTR.
  2. Resolve AARI sustainment, test readiness, and modernization shortfalls to support advanced aircraft open-air mission testing on the NTTR.

Global Positioning System (GPS) Enterprise

Executive Summary

- The Air Force conducted developmental test and evaluation (DT&E) for all three GPS enterprise segments (space, control, and user), but did not conduct operational testing in 2017. DT&E included GPS III Satellite Vehicle (SV) 02 acoustic and thermal testing, Next Generation Operational Control System (OCX) Launch Checkout System testing, and Military GPS User Equipment (MGUE) Increment 1 card testing.
- Schedule slips have caused operational testing delays for all GPS segments from dates listed in prior DOT&E Annual Reports.
- The Program Office has updated the Enterprise Test and Evaluation Master Plan (ETEMP) Revision B to reflect test strategy, schedule, and resource changes due to segment delays, acquisition strategy changes, and initiation of the Contingency Operations (COps) baseline. The ETEMP has been in coordination with the Services since November 2014.
- While progress has been made across the segments, significant GPS Enterprise operational risks remain:
  - OCX delays will limit adequate and timely operational testing for the full capabilities of GPS III satellites prior to extensive procurement and incorporation of the satellites into the operational constellation.
  - The Program Office has not planned for operational cybersecurity testing of the OCX Launch Checkout System (Block 0) baseline due to their concerns that cyber testing could place the non-redundant system (used for satellite launch and initialization) at risk. While Block 0 will not be used for operational employment of GPS III satellites, this ground control baseline will have command, control, and cyberspace access to future operational satellites.
  - While the program has a Lead Developmental Test Organization, it is a part of the Program Office instead of fully independent, which has resulted in a lack of insight to OCX developmental testing.
  - Due to the delays in the ground-based parts of the GPS Enterprise, there is ongoing risk that adequate OT&E of GPS III satellites will not be possible until as many as five satellites are on orbit, increasing the risk that testing will not discover deficiencies until it is too late to correct them.
  - GPS III lacks sufficient test resources for realistic operational testing, including on-orbit threats.
  - The GPS III Follow-On Production Acquisition Strategy Document, amended in 2017, lacks any description of integration, interdependencies, or risks between the GPS III Follow-On Production satellites and the ground control and user segments. Additionally, the Air Force has proposed a Milestone C decision in 2020, before any GPS III Follow-On Production satellites have been developed or tested. The continued lack of an enterprise strategy and integrated approach to program execution places the nation's GPS capability at significant risk.
  - The pathfinding value of the currently planned MGUE Lead Platform operational testing is limited since the Army and the Marines may not deploy their nominated Lead Platforms in the tested configurations.

AFSCN – Air Force Satellite Control Network
GPS IIR – Global Positioning System (GPS) Block II "Replenishment" Satellites
GPS IIR-M – GPS Block II "Replenishment – Modernized" Satellites
GPS IIF – GPS Block II "Follow-On" Satellites
GPS III – GPS Block III Satellites

System

- The GPS enterprise is an Air Force-managed, satellite-based radio navigation system of systems that provides military and civil users accurate position, velocity, and time within the multi-trillion cubic kilometer volume of near-Earth space, Earth atmosphere, and worldwide Earth surface areas.
- The current GPS enterprise consists of three operational segments:
  - Space Segment – The GPS spacecraft constellation consists of a minimum of 24 operational satellites in semi-synchronous orbit. The Air Force has successfully launched 70 GPS satellites and currently operates 31 healthy GPS satellites comprised of Block IIR (1997-2004), Block IIR-M (2005-2009), and Block IIF (2010-2016).
  - Control Segment – The GPS control segment consists of primary and backup GPS master control stations, satellite control antennas, a pre-launch satellite compatibility station, and geographically distributed operational monitoring stations. The GPS control segment includes the Operational Control System (OCS)/Architecture Evolution Plan, which supports operations of the current satellite constellation; the Launch/Early Orbit, Anomaly Resolution, and Disposal Operations (LADO) system;

Selective Availability/Anti-Spoof Module (SAASM) capabilities in U.S. and allied military GPS user equipment; and the SAASM Mission Planning System (SMPS).
  - User Segment – There are many versions of military GPS mission receivers fielded on a multitude of operational systems and combat platforms, including the Defense Advanced GPS Receivers and embedded Ground-Based GPS Receiver Application Modules (GB GRAM), numbering in the hundreds of thousands.
- In 2000, the DOD approved initiation of a GPS enterprise modernization effort to include upgrades to all three segments, along with new civil and military signals (M-code). In addition to replenishment of the satellite constellation, this modernization is intended to improve both military and civil signal integrity and service quality. Modernized GPS enterprise improvements include:
  - Space Segment – The Air Force intends for the GPS III satellites, an Acquisition Category (ACAT) 1D program, to be capable of transmitting a fourth civil signal and higher-powered M-code, as well as all legacy military and civil navigation signals of previous satellite blocks.
  - Control Segment – The Air Force plans to deliver OCX, an ACAT 1D program, in three blocks. OCX is intended to replace the current ground control segment and LADO, be backward compatible with Block IIR and later satellites, and interface with modified SMPS versions. OCX Block 0 is being developed to launch and initialize GPS III satellites, while OCX Block 1 is being developed to command and control GPS Block II and III satellites. OCX Block 2 is intended to provide full control of modernized civil and M-code signals and navigation warfare functions. OCX is intended to provide significant cybersecurity improvements over the current ground control system.
  - User Segment – MGUE Increment 1 is an ACAT ID program and Increment 2 is, currently, a pre-Major Defense Acquisition Program. MGUE Increment 1 includes the GB-GRAM-Modernized form factor for ground and low-dynamic platforms and the GRAM-Standard Electronic Module-E/Modernized for maritime and aviation applications. The MGUE Increment 2 Capability Development Document is in coordination.
- Due to delays in OCX Block I delivery, the Air Force initiated the COps program as a "bridge capability" to enable employment of GPS III satellites using legacy (pre-M-Code) signals for operational constellation sustainment until OCX Block 1 is available.
- In September 2017, the Air Force placed M-Code Early Use (MCEU) on contract. MCEU will deliver early operational use of core M-Code, with full M-Code functionality delivered in OCX Block 1.

Mission

Combatant Commanders of U.S. and allied military forces use GPS to provide accurate, position, navigation, and time information to operational users worldwide.

Major Contractors

- Space Segment
  - Block IIR/IIR-M/III satellites: Lockheed Martin Space Systems – Denver, Colorado
  - Block IIF satellites: Boeing, Network and Space Systems – El Segundo, California
- Control Segment
  - OCS: Lockheed Martin, Space Systems Division – Colorado Springs, Colorado
  - OCX: Raytheon Company, Intelligence, Information, and Services – Aurora, Colorado
  - COps and MCEU: Lockheed Martin, Space Systems Division – Colorado Springs, Colorado
- User Segment (MGUE Increment 1)
  - L-3 Technologies/Interstate Electronics Corporation – Anaheim, California
  - Raytheon Company, Space and Airborne Systems – El Segundo, California
  - Rockwell Collins – Cedar Rapids, Iowa

Activity

- Planning and preparation for operational testing of the space, ground, and user segments, beginning in 2019, is ongoing.
- The Air Force conducted DT&E for all three GPS enterprise segments (space, control, and user), but did not conduct operational testing in 2017. DT&E included GPS III SV02 acoustic and thermal testing, OCX Launch Checkout System testing, and MGUE Increment 1 card testing.
- Schedule slips in the development of all GPS segments have caused operational testing delays from dates listed in prior DOT&E Annual Reports.
- The Program Office has updated the ETEMP Revision B to reflect schedule and resource changes due to segment delays, acquisition strategy changes, and initiation of the COps baseline. The ETEMP has been in coordination with the Services since November 2014. The revision has been delayed by significant fluctuation in all enterprise segment delivery and availability schedules, OCX and MGUE acquisition strategies, initiation of COps, and Army concerns related to its Assured Precision Navigation and Timing program.

OCX

- The Air Force conducted an OCX Block 0 system acceptance in October 2017, but does not plan to declare OCX operational until Block 1 delivery.

- Following the 2016 Nunn-McCurdy review and recertification, the Air Force proposed OCX Block 1 and Block 2 delivery in April 2022 in an updated Milestone B Acquisition Program Baseline (APB). The Air Force expects the Milestone B and APB approval in late 2017.

COps

- The Air Force placed COps on contract in August 2017 and the Air Force Operational Test and Evaluation Center (AFOTEC) is planning operational testing in July 2019, concurrent with GPS III SV01 operational tests.

MCEU

- Following the September 2017 MCEU approval, the Air Force modified the contract to address M-Code "hot start" requirements for the GPS enterprise. Hot start is the capability of M-Code receivers to initialize legacy receivers with data derived from a modernized navigation signal.
- AFOTEC plans to conduct operational testing of MCEU in conjunction with MGUE operational testing in 2020.

GPS III and GPS III Follow-On Production

- The first of 10 GPS III satellites is in storage and planned for launch in May 2018.
- The Air Force amended the GPS III Follow-On Production Acquisition Strategy Document in 2017. The amendment addresses the second phase of the procurement strategy and outlines new capabilities for the next 22 GPS III satellites.

MGUE

- MGUE Increment 1 received Milestone B approval in January 2017.
- The Air Force conducted successful early developmental testing on the B-2 platform with a prototype MGUE card. Additionally, the Army's Program Executive Office for Ammunitions conducted field tests to assess the maturity of MGUE Increment 1 technology for precision-guided munitions.
- The Program Office is planning to conduct a developmental field test of MGUE card maturity in April 2018.
- The planned operational assessment of MGUE Increment 1 has slipped to 2019 due to delayed delivery of test receiver cards and software increments. As a result, MGUE Increment 1 IOT&E has slipped to 2020. This IOT&E will include data collection from separate MGUE Increment 1 OUEs on the four designated Service Lead Platforms.
- A Joint Service Working Group is developing courses of action to inform the MGUE Increment 2 acquisition strategy. The Air Force has been tasked to provide the strategy by March 2018.

Assessment

- The Air Force has improved the GPS enterprise schedule and addressed numerous schedule and performance risks; however, the articulation of program risks with stakeholders is incomplete, increasing the probability of unmitigated risks causing further program problems and delays.

OCX

- OCX delays will limit adequate and timely operational testing for the full capabilities of GPS III satellites prior to extensive procurement and incorporation of the GPS III satellites into the operational constellation.
- While the program has a Lead Developmental Test Organization, it is a part of the Program Office instead of fully independent, which has resulted in a lack of insight to OCX developmental testing.
- The Program Office has not planned for operational cybersecurity testing of the OCX Launch Checkout System (Block 0) baseline due to their concerns that cyber testing could place the non-redundant system at risk. While Block 0 will not be used for operational employment of GPS III satellites, this ground control baseline will have command, control, and cyberspace access to future operational satellites.
- Since the 2016 Nunn-McCurdy review, the Program Office has attempted to reduce future schedule risk by increasing manpower, improving system engineering and configuration management processes, and evolving its testing approach. However, it is not clear the Air Force has enough resources to conduct developmental testing on COps and OCX in parallel, which is required to keep both programs on the current schedule.

GPS III and GPS III Follow-On Production

- GPS III lacks sufficient test resources for realistic operational testing, including on-orbit threats.
- Due to the delays in the ground-based parts of the GPS Enterprise, there is ongoing risk that adequate OT&E of GPS III satellites will not be possible until as many as five satellites are on orbit, increasing the risk that testing will not discover deficiencies until it is too late to correct them.
- The Program Office is planning for the GPS III Follow-On Production Non-flight Satellite Testbed (GNST+) in the GPS III Follow-On Production program. However, GNST+ will not provide full capability for realistic threat testing. The program plans to conduct environmental testing at the component level; but, the program is not planning for test articles that would support characterization of man-made threats against the system.
- The GPS III Follow-On Production Acquisition Strategy Document, amended in 2017, lacks any description of integration, interdependencies, or associated risks between the GPS III Follow-On Production satellites and the ground control and user segments. Additionally, the Air Force has proposed a Milestone C decision in 2020, before any GPS III Follow-On Production satellites have been developed or tested. The continued lack of an enterprise strategy and integrated approach to program execution places the nation's GPS capability at significant risk.

MGUE

- The pathfinding value of the currently planned MGUE Lead Platform operational testing is limited, since the Army and the Marines may not deploy their nominated Lead Platforms in the tested configurations.
- MGUE OUE requires testing of a production-representative card in an operational configuration in an operationally

realistic environment to determine MGUE operational effectiveness, suitability, and mission capability.
- The need to include an MGUE "hot start" capability has driven new contracts for each of the three card vendors. This necessary change could adversely affect the card's power profiles (already of concern) and add to cost and schedule. An additional software change to the MGUE cards will be required to implement the subsequent enterprise hot start solution.
- The MGUE program continues to face challenges in transitioning card technology, to include new requirements and a lengthy security certification process for approving vendor changes to cards.

Recommendations

- Status of Previous Recommendations. The Air Force has partially addressed the recommendations from the 2011, 2014, and 2016 Annual Reports; however, the Air Force should still:
  1. Continue to plan for GPS enterprise end-to-end testing, including Lead Platform and non-Lead Platform integration, and DT&E and OT&E in realistic operational environments in time to support acquisition decisions.
  2. Ensure status; critical dependencies; and enterprise risks, impacts, and mitigation plans are well understood and promptly disseminated to all stakeholders.
  3. Maintain and disseminate accurate and timely schedule information for all segments, ensuring the schedules reflect segment interdependencies, current government estimates, and caveats for assumptions.
  4. Prioritize and commit resources to ensure successful execution of the COps program, including active and independent monitoring of the COps development progress.
  5. Plan for an adequate MGUE Increment 1 operational assessment encompassing integration and DT&E on at least one Lead Platform per form factor to inform these acquisition decisions.
  6. Plan for and conduct comprehensive risk reduction integration testing with all platforms, munitions, and interfaces expected to integrate with MGUE Increment 1.
  7. Conduct an assessment to determine the degree to which designated Lead Platforms for MGUE Increment 1 cover the range of operational factors and integration challenges for the complete portfolio of supported DOD platforms.
  8. Integrate and test each MGUE Increment 1 vendor solution on applicable Lead Platforms as soon as those vendor solutions are available. The Air Force does not plan to ensure each available MGUE Increment 1 vendor solution for a given form factor is integrated with all Lead Platforms for that respective form factor to support adequate MGUE IOT&E.
- FY17 Recommendations.
  1. The Air Force should plan to demonstrate GPS III satellite capability against on-orbit threats with operationally representative test articles, including a full-scale GPS test resource (or "iron bird") for realistic operational testing of on-orbit threats.
  2. The Program Office should plan for operational cybersecurity testing of OCX Block 0 to ensure a comprehensive cyber assessment of the ground control system that will access GPS III satellites on-orbit prior to their operational employment.
  3. The Air Force should develop an integrated, enterprise strategy for GPS III Follow-On Production and clearly articulate satellite, ground, and user segment interdependencies and risks.

Joint Space Operations Center (JSpOC) Mission System (JMS)

Executive Summary

- The Air Force has not conducted any OT&E for Joint Space Operations Center (JSpOC) Mission System (JMS) Increment 2, but executed significant development and developmental testing for JMS Increment 2, Service Packs (SP) 9 and 11 in 2017.
- The SP9 developmental testing campaign was extended to address system stability, operator training, and development of operational procedures. Despite improved performance during SP9 developmental testing, there are a number of remaining critical deficiencies that are expected to change the scope of the SP9 operational delivery and testing. DOT&E expects operational testing for SP9 to begin no earlier than February 2018.
- The Air Force is finalizing a revision to the JMS Test and Evaluation Master Plan (TEMP) to reflect program schedule and content changes, including OT&E for SP11, necessitated by the addition of functional capabilities.
- While some interoperability testing has occurred, delays in the JMS Increment 2 delivery increase the risk of late discovery of integration deficiencies between JMS and Space Fence Increment 1.

System

- JMS is a net-centric, service-oriented architecture of hardware, software, data, and network connectivity that is intended to process, integrate, store, and allow for the compilation, exploitation, sharing, and visualization of Space Situational Awareness (SSA) sensor data and analysis to support command and control tasking and battle-management decisions for space forces.
- The Air Force has installed operational JMS hardware strings and infrastructure at Vandenberg AFB, California. The U.S. Strategic Command will fund and install a backup site at Naval Support Facility Dahlgren, Virginia. Additional non-operational instances and partial instances of JMS are installed for development and developmental testing purposes at a multitude of other sites, including Vandenberg AFB, California, and Space and Naval Warfare Systems Center Pacific at the Point Loma Annex of Naval Support Center San Diego, California.
- JMS net-centric enterprise services, including data visualization, mission applications, and functional queries, are accessible to worldwide users running JMS client software on non-JMS workstations connected through the SECRET Internet Protocol Router Network (SIPRNET) and the Joint Worldwide Intelligence Communication System (JWICS).
- JMS is intended to replace legacy Space Defense Operations Center (SPADOC) and space specific portions of the Astrodynamic Work Station (ASW).

- The Air Force is developing JMS in two increments.
  - Increment 1 delivered an initial service-oriented architecture infrastructure and user tools, including a client workstation-accessible User Defined Operational Picture that allows access to and analysis of data from legacy systems, integrated collaboration/messaging/data sharing tools, and space order of battle processing.
  - Increment 2 is being developed to deliver mission functionality in three SPs.
    - SP7 delivered updates and additions to Increment 1-delivered hardware and software infrastructure, including servers, space surveillance network (SSN) communications services connectivity, system security and message processing capabilities, and limited space surveillance data processing and visualization tools. The Air Force did not operationally test SP7 because it did not replace legacy SPADOC and ASW systems and was not used for mission critical functions.
    - SP9 is intended to update and expand JMS hardware and software to perform functions currently performed by SPADOC and ASW, with improved accuracy, efficiency, and responsiveness. Those functions include administration and maintenance of the space catalog, orbit determination for resident space objects (RSOs), assessment of conjunctions (collision risk) between RSOs, and high-accuracy tasking of sensors for orbital safety, threat modeling, and operational decisions.
    - SP11 is intended to complete Increment 2 functionality on the Secret and Top Secret enclaves. It should also include the ability to ingest and integrate more highly classified data, support routine Space Object Identification tasking, and support processing for critical events such as RSO Closely Spaced Operations, breakups, re-entries and de-orbits, launch processing, and

processing of uncorrelated tracks. SP11 is also intended to encompass test, training, and exercise capabilities and availability and reliability improvements, which had been planned for delivery in the descoped SP13.

Mission

The Commander, Joint Functional Component Command for Space uses JMS to enable the coordination, planning, synchronization, and execution of continuous, integrated space operations in support of national and Combatant Commander objectives.

Major Contractors

- Government prime contractor:
  - Air Force Space and Missile Systems Center – Los Angeles AFB, California
- System Integrator, Increments 1 and 2:
  - Space and Naval Warfare Systems Command (SPAWAR) – San Diego, California
- Increment 1 sub-contractors:
  - Polaris Alpha – Colorado Springs, Colorado
  - The Design Knowledge Company – Fairborn, Ohio
- Increment 2 sub-contractors:
  - Analytical Graphics Incorporated – Exton, Pennsylvania
  - Artificial Intelligence Solutions – Lanham, Maryland
  - Omitron – Beltsville, Maryland

Activity

- The Air Force did not conduct OT&E for JMS Increment 2 in 2017, but did complete significant development and developmental testing for JMS Increment 2, SP9 and SP11, including:
  - Two additional phases of functional developmental testing for SP9
  - Three JMS Astro/catalog Verification and Evaluation against Legacy Instantiations (JAVELIN) tests, which focused on the JMS SP9 capability to maintain the space object catalog in comparison to the legacy system
  - Five SP11 integration tests
- The program manager wisely extended SP9 developmental testing to improve system stability, operator training, and to develop operational procedures. Despite the extension of developmental testing, the Air Force proposed a reduction in the operational scope of SP9 due to remaining deficiencies and operational user concerns.
- The Air Force Operational Test and Evaluation Center (AFOTEC) is planning an Operational Utility Evaluation (OUE) of JMS SP9 following an Integrated Test and Evaluation (IT&E) period; however, the scope of the OUE may be reduced due to the proposed operational changes to SP9.
- The Air Force is finalizing development of a revision to the JMS TEMP, to reflect program schedule and content changes, including the addition of OT&E for SP11, necessitated by the addition of functional capabilities.
- The Air Force validated a modeling and simulation tool to support the evaluation of system capacity under high-user loading.

Assessment

- Despite improved performance during SP9 DT&E, there are a number of remaining critical deficiencies that are expected to change the scope and timing of SP9 operational testing. Additionally, the Program Office is reassessing the Increment 2 schedule following the delay of IT&E. DOT&E expects operational testing for SP9 to begin no earlier than February 2018.
- Due to SP9 development problems, resource constraints related to SP9 and SP11 concurrency, and an unrealistic schedule, DOT&E expects SP11 to be delayed. While some interoperability testing has occurred, delays in the JMS Increment 2 delivery increase the risk of late discovery of integration deficiencies between JMS and Space Fence Increment 1.
- The Program Office and AFOTEC have placed significant focus on cybersecurity assessment and hardening; however, additional work remains to enable defenders to monitor JMS in order to provide an adequate cyber defense.
- The Air Force deferred, to an undefined increment, validated JMS CDD requirements, which were planned for delivery in SP13 and not included in SP11. This undefined increment may become the program of record being planned to equip the new National Space Defense Center.

Recommendations

- Status of Previous Recommendations. The program has implemented several changes to address FY16 recommendations, however the Air Force still needs to:
  1. Develop an acquisition strategy for post-Increment 2 capabilities and the National Space Defense Center program of record.
  2. Provide cyber defenders, system administrators, and operators with the ability to detect cyber attacks and mitigate their operational impacts.
  3. Conduct independent, non-cooperative, threat representative penetration testing to assess protect, detect, react, and restore components of cybersecurity for Increment 2. This testing is planned for SP9 and SP11.
  4. Conduct JMS-Space Fence interoperability testing. While partial JMS SP11 and Space Fence interoperability testing occurred at the SPAWAR development system, this testing

did not encompass sufficient system configurations for adequate interoperability testing.

5. Develop and validate modeling and simulation tools to support evaluation of JMS high accuracy catalog size and accuracy. This is planned for delivery in SP11.

- FY17 Recommendation.
  1. In addition to prioritizing Space Fence requirements in SP11, the Program Office needs to develop courses of action with the Space Fence Program Office to achieve operationally representative integration testing between both systems during OT&E.

KC-46A

Executive Summary

- The KC-46 program completed all planned flight test events necessary for the Federal Aviation Administration (FAA) Aircraft Amended Type Certificate of the Boeing 767-2C aircraft in July 2017. A few remaining flights are expected to satisfy FAA requirements during the final review process. The program is continuing to accomplish FAA Supplemental Type Certificate test events to complete FAA certification of the KC-46A aircraft.
- Flight testing to certify the aerial refueling (AR) system and the first eight aircraft for receiver operations with the KC-46A began in October 2017.
- Electromagnetic pulse (EMP) testing was not accomplished in accordance with the DOT&E-approved Test and Evaluation Master Plan (TEMP) and the LFT&E Strategy. While testing indicated the KC-46A flight-critical systems and boom refueling systems are likely survivable to the 6 decibel (dB) contractual requirement, the Program Office approved verification plan did not demonstrate the residual KC-46A mission systems capability during such an event.
- IOT&E is likely to start in January 2019 or later. Schedule analysis identified two key milestones affecting IOT&E start: (1) completion of AR certification of the initial group of three receivers before the beginning of operational aircrew training and (2) certification of all 18 receivers planned to participate in operational test by the mid-point of IOT&E.
- Analysis of boom AR testing to date showed a significant number of instances where the boom nozzle contacted the receiver aircraft outside the refueling receptacle and in many of those instances, the Aerial Refueling Operators (AROs) were unaware those contacts had occurred. Boom nozzle contact outside the receptacle can damage antennae or other nearby structures, but is especially problematic for low-observable receiver aircraft by damaging radar-absorbing coatings. A potential contributing factor for both the number of contacts outside the receptacle and undetected contacts is the reduced visual acuity of the AROs using the remote vision system. Boeing and the Air Force teams are conducting root cause analysis, reviewing the historical data, and will be collecting additional data during upcoming tests.

System

- The KC-46A AR aircraft is the first increment of replacement tankers (179) for the Air Force's fleet of more than 400 KC-135 tankers.
- The KC-46A design uses a modified Boeing 767-200ER commercial airframe with numerous military and technological upgrades, such as the fly-by-wire refueling boom, the remote ARO's station, 787 cockpit, additional fuel tanks in the body, and defensive systems.

- The KC-46A will provide both a boom and probe-drogue refueling capabilities. The KC-46A is equipped with an AR receptacle so that it can also receive fuel from other tankers, including legacy aircraft.
- The KC-46A is designed to have significant palletized cargo and aeromedical capacities; chemical, biological, radiological, and nuclear survivability; and the ability to host communications gateway payloads.
- Survivability enhancement features are incorporated into the KC-46A design.
  - Susceptibility is reduced with an Aircraft Survivability Equipment suite consisting of Large Aircraft Infrared Countermeasures (LAIRCM), a modified version of the ALR-69A Radar Warning Receiver (RWR), and a Tactical Situational Awareness System. The suite is intended to correlate threat information from pre-flight planning, the RWR, and other on- and off-board sources and to prompt the crew with an automatic re-routing suggestion in the event of an unexpected threat.
  - Vulnerability is reduced by adding a fuel tank inerting system and integral armor to provide some protection to the crew and critical systems.

Mission

Commanders will use units equipped with the KC-46A to perform AR to accomplish six primary missions to include nuclear operations support, global strike support, air bridge support, aircraft deployment, theater support, and special operations support. Secondary missions will include airlift, aeromedical evacuation, emergency AR, air sampling, and support of combat search and rescue.

Major Contractor

The Boeing Company, Commercial Aircraft in conjunction with Defense, Space & Security – Seattle, Washington

Activity

- The KC-46 program completed all planned flight test events necessary for the FAA Aircraft Amended Type Certificate of the Boeing 767-2C aircraft in July 2017. A few remaining flights are expected to satisfy FAA requirements during the final review process. The program is continuing to accomplish FAA Supplemental Type Certificate test events to complete FAA certification of the KC-46A aircraft.
- The program is now accomplishing testing using the production-representative version of last year's redesigned prototype boom.
- Flight testing to certify the AR system and the first eight aircraft for receiver operations with the KC-46A began in October 2017.
- The KC-46A deployed to Fairbanks, Alaska, for cold weather testing in January 2017 and then to Yuma, Arizona, for hot weather testing in August 2017. The program had planned to accomplish additional cold weather testing in the McKinley Climactic Laboratory at Eglin AFB, Florida, in September 2017 but decided not to accomplish testing at that venue due to the threat of hurricanes. The program is planning on accomplishing those additional tests in December 2017 in Alaska.
- Boeing completed Block 20 LAIRCM flight testing at Moses Lake, Washington, in 2017 to confirm installed system performance.
- The Navy conducted EMP testing at Naval Air Station, Patuxent River, Maryland, in July 2017 on behalf of Boeing. Testing was not accomplished in accordance with the DOT&E-approved TEMP and the LFT&E Strategy. Testing demonstrated KC-46A flight critical capabilities were still available after exposure to a 6 dB pulse; however, testing did not fully demonstrate AR capabilities as required. The program uninstalled or deactivated multiple mission critical systems prior to testing and, therefore, their EMP tolerance was not tested on an aircraft in a mission-representative configuration. Additionally, the testing did not demonstrate the function of the AR boom and the wing AR pods following an EMP event to show the KC-46A can perform the required missions.
- The Air Force plans to complete two nuclear threat-focused assessments for the KC-46A in FY18: (1) assess the ability to launch and fly a safe distance from a simulated nuclear attack to a KC-46A staging base, and (2) assess the KC-46A's inherent nuclear hardness to blast, radiation, flash, thermal, and EMP effects. Requirements resulting from proprietary data agreements have hindered the start of these activities.
- The Program Office coordinated with Boeing for access to a production-representative KC-46A for a Cybersecurity Vulnerability Assessment (the second cybersecurity vulnerability assessment during developmental testing) in May 2017. The program will use the classified results to inform continued software updates and cybersecurity testing during operational tests.

Assessment

- IOT&E is likely to start in January 2019 or later. Schedule analysis identified two key milestones affecting IOT&E start: (1) completion of AR certification of the initial group of three receiver aircraft before the beginning of operational aircrew training and (2) certification of all 18 receiver aircraft planned to participate in operational test by the mid-point of IOT&E. DOT&E concurs with the initial program plan requiring these 18 receiver aircraft as necessary to support an adequate IOT&E of a new Air Force tanker.
- Analysis of boom AR testing to date showed a significant number of instances where the boom nozzle contacted the receiver aircraft outside the refueling receptacle and in many of those instances, the AROs were unaware those contacts had occurred. Boom nozzle contact outside the receptacle can damage antennae or other nearby structures, but is especially problematic for low-observable receiver aircraft by damaging radar-absorbing coatings. A potential contributing factor for both the number of contacts outside the receptacle and undetected contacts is the reduced visual acuity of the AROs using the remote vision system. Boeing and the Air Force teams are conducting root cause analysis, reviewing the historical data, and will be collecting additional data during upcoming tests. Without an appropriate solution, this problem will have adverse operational mission effects on low-observable aircraft at a minimum.
- EMP testing was not adequate to assess whether the KC-46A is mission capable to the contractually required 6 dB design margin based upon Military Standard (MIL-STD) 464. The program powered down or removed critical mission systems that were not required to meet the threshold Key Performance Parameter requirement including radios, satellite communications, weather radar, RWR, LAIRCM system, and the wing AR pods for this test. The program pre-deployed the refueling boom with hydraulics deactivated for the EMP test and therefore the capability to deliver fuel during or immediately following the EMP event was not tested. No test was performed with all flight and mission systems on, which is required to provide a representative load to the system under EMP conditions.
- The KC-46A EMP design margin was based on MIL-STD 464 and the threat defined in MIL-STD 2169. After the fixed-price contract was awarded, the DOD instituted a new MIL-STD 3023 that requires tanker aircraft supporting the nuclear deterrent mission to meet a 20 dB EMP design margin versus the contractually required 6 dB EMP design margin. Unless additional tests are resourced, the Air Force or U.S. Strategic Command will not know if the KC-46A meets the 20 dB EMP hardening requirement in MIL-STD 3023.
- Boeing and the Air Force still need to complete several tests that assess areas that significantly influence the aircraft's survivability. These include flight testing of the On-Board Inert Gas Generation System and thermal testing of the nuclear flash curtains.

- LAIRCM testing provided hit point distribution data to inform the vulnerability assessment and to verify that LAIRCM performance on the KC-46A has not been degraded from previously demonstrated performance on other aircraft. The evaluation included both system configurations (Block 20 with ultraviolet missile warning system and Block 30 with two-color infrared missile warning system).

Recommendations

- Status of Previous Recommendations. The Air Force has addressed all FY12 through FY14 recommendations. The Air Force still needs to address the following FY15 and FY16 recommendations:
  1. Ensure all AR receiver aircraft are certified for use by operational aircrew early enough in IOT&E to permit sufficient operational testing.
  2. In conjunction with U.S. Strategic Command, determine whether its personnel can conduct the nuclear deterrence and strike missions with a KC-46A only having 6 dB EMP shielding as per the contract. If additional EMP shielding is deemed necessary, the Air Force should conduct testing as part of FOT&E to determine the actual KC-46A EMP design margin.
  3. Develop an executable schedule that is based on program demonstrated-to-date fly and re-fly rates.
- FY17 Recommendation.
  1. The Air Force should re-test the KC-46A in an operationally representative condition to determine the actual EMP design margin. Demonstrate the function of the AR boom and the wing AR pods following an EMP test to show the KC-46A can perform the required missions.

Massive Ordnance Penetrator (MOP)

Executive Summary

- In December 2016, the Air Force successfully completed one GBU-57 Massive Ordnance Penetrator (MOP) drop from a B-2 aircraft, followed by another weapon drop in January 2017, also from a B-2 aircraft; both on representative targets.
- In May 2017, the Air Force successfully completed a three-weapon drop from B-2 aircraft on a representative target.
- Collectively, the three GBU-57 MOP tests, conducted at the White Sands Missile Range (WSMR), New Mexico, demonstrated effectiveness of the Enhanced Threat Response (ETR)-IV weapon modifications.
- DOT&E published a classified Early Fielding Report summarizing the ETR-IV test results in November 2017.

System

- MOP is a large, GPS-guided, penetrating weapon with the ability to attack deeply-buried and hardened bunkers and tunnels. The warhead case is made from a special high-performance steel alloy and its design allows for a large explosive payload while maintaining the integrity of the penetrator case during impact.
- The B-2 Spirit is the only aircraft in the Air Force programmed to employ MOP.
- The GBU-57 warhead is more powerful than its predecessors, the BLU-109 and GBU-28.
- MOP was developed from an Air Force-led, Quick Reaction Capability and is a SECDEF special interest effort under DOT&E oversight. MOP transitioned to an Air Force program of record in August 2017.

Mission

Combatant Commanders use the B-2 equipped with MOP to conduct pre-planned, day or night attacks against defended point targets vulnerable to blast and fragmentation effects and requiring significant penetration, such as hardened and deeply buried facilities.

Major Contractor

The Boeing Company, Defense, Space & Security – St. Louis, Missouri

Activity

- In December 2016, the Air Force conducted one live weapon drop on a representative target at WSMR to evaluate weapon functionality with the ETR-IV modifications. An Air Force B-2 aircraft flew the mission.
- In January 2017, the Air Force conducted an additional single-weapon test, also on a representative target at WSMR, to evaluate weapon effectiveness. An Air Force B-2 aircraft flew the mission.
- In May 2017, the Air Force conducted a three-weapon test on a representative target at WSMR to evaluate ETR-IV modifications and to test weapon effectiveness. Three Air Force B-2 aircraft each flew one sortie to complete the mission.
- These events completed the ETR-IV test.
- DOT&E submitted a classified Early Fielding Report in November 2017 detailing the results of ETR-IV.
- The Air Force conducted all testing in accordance with the DOT&E-approved Quick Reaction Capability test plan.

Assessment

- The ETR-IV testing successfully demonstrated weapon effectiveness of the current weapon configuration when paired with proper tactics, techniques, and procedures (TTPs). A partial failure on the second ETR-IV test event identified a failure mode that appears to occur under specific circumstances with improper TTPs.
- No further ETR testing is currently planned.

Recommendations

- Status of Previous Recommendations. There were no previous recommendations for this program.
- FY17 Recommendations.
  1. The Air Force should identify the root cause of the partial failure of the second ETR-IV test event in January 2017.
  2. The Defense Threat Reduction Agency should continue to improve the fidelity of the modeling and simulation tools intended to be used for MOP weaponeering.

Miniature Air Launched Decoy (MALD) and MALD–Jammer (MALD-J)

Executive Summary

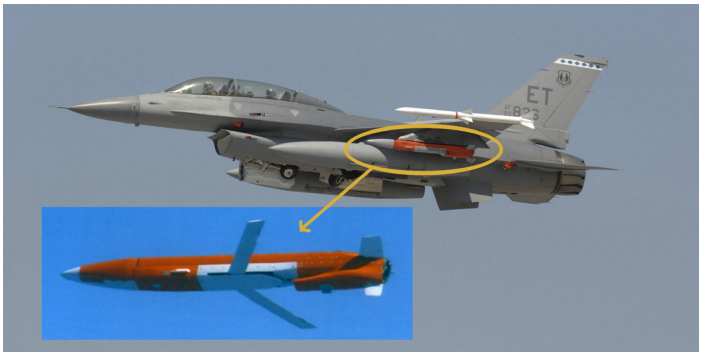
- The Air Force Operational Test and Evaluation Center (AFOTEC) completed an FOT&E for the Miniature Air Launched Decoy – Jammer (MALD-J) to address deficiencies discovered in the IOT&E period.
- MALD-J is operationally effective and suitable.
- DOT&E removed MALD-J from the oversight list on June 21, 2017.

System

- MALD is a low-cost, expendable, air-launched vehicle that replicates the flight of manned aircraft.
- MALD-J adds an electronic attack jammer to the MALD with the capability to jam Early Warning/Acquisition/Ground Control Intercept radars while retaining the capabilities of the MALD.
- The F-16 C/D and B-52H are the lead aircraft to employ MALD and MALD-J.

Mission

Combatant Commanders will employ units equipped with MALD or MALD-J to improve battlespace access for airborne strike forces by deceiving, distracting, or saturating enemy air-defense systems.



- MALD is designed to support an airborne strike force to achieve mission success by deceiving enemy radars and air-defense systems to treat MALD as a viable target.
- MALD-J is designed to support an airborne strike force to achieve mission success by jamming enemy radars and air-defense systems by degrading/denying detection of friendly aircraft or munitions.

Major Contractor

Raytheon Missile Systems – Tucson, Arizona

Activity

- AFOTEC conducted testing of MALD-J (and MALD) in accordance with a DOT&E-approved test plan.
- In January 2016, AFOTEC completed ground testing of the GPS Aided Inertial Navigation System (GAINS) obsolescence upgrade (known as GAINS II) to the MALD-J at the National Radar Cross Section Test Facility, New Mexico.
- In October 2016, the Air Force's 28th Test and Evaluation Squadron completed a Force Development Evaluation at White Sands Missile Range, New Mexico. The evaluation characterized GPS-degraded navigation and assessed the performance of the GAINS II upgrade. Six MALD-Js flew without incident.
- In January 2017, the Digital Integrated Air Defense System (DIADS) simulation facility at Edwards AFB, California, supported mission-level testing by modeling GPS-denied navigation performance in a many-on-many threat laydown scenario.
- DOT&E removed MALD-J from the oversight list on June 21, 2017.

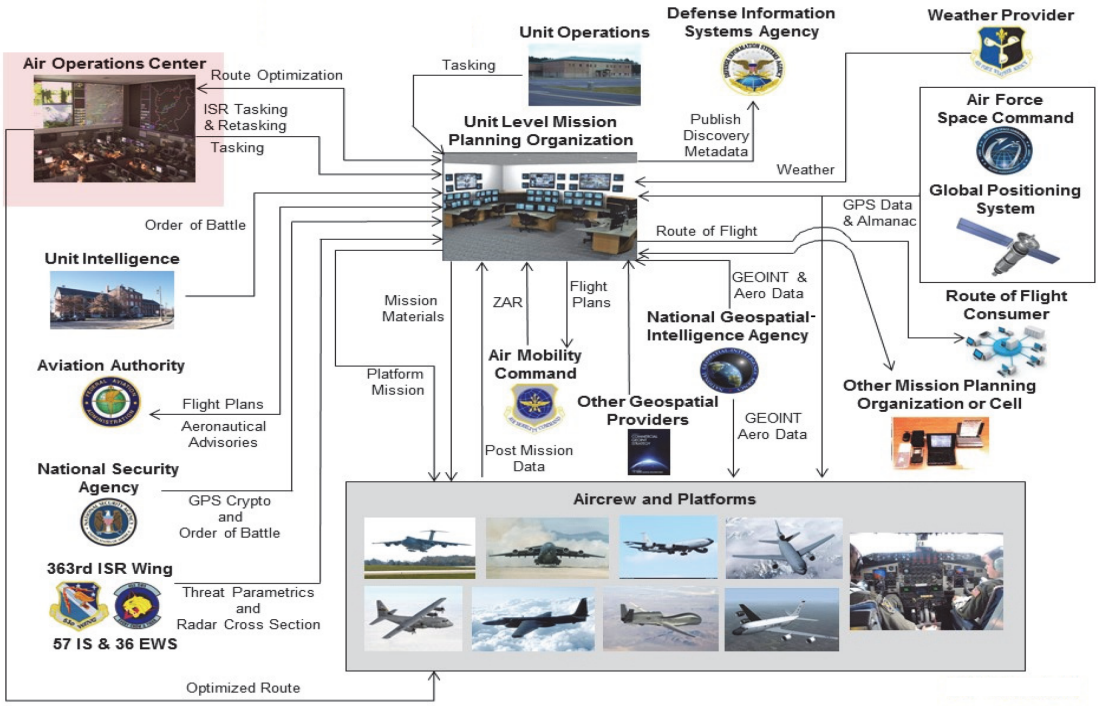
Assessment

- MALD-J is effective, suitable, and mission capable in a GPS-denied environment.
- Results from ground and open-air testing indicate GAINS II provides improved navigational performance in a GPS-contested environment
- Results from mission-level testing showed MALD-J provides the desired effect on Integrated Air Defense systems (IADS) and that navigation performance in a GPS-denied environment resulted in minimal operational impact to support mission tasking.

Recommendations

- Status of Previous Recommendations. The Air Force satisfactorily addressed all of the FY16 recommendations with GAINS II software corrections in a GPS-denied environment and incorporated a many-on-many mission-level simulation in DIADS.
- FY17 Recommendations. None.

Mission Planning Systems (MPS) / Joint Mission Planning System – Air Force (JMPS-AF)



Aero - Aeronautical
EWS - Electronic Warfare Squadron
GEOINT - Geospatial Intelligence
IS - Intelligence Squadron
ISR - Intelligence, Surveillance, and Reconnaissance
ZAR - Zone Availability Report

Executive Summary

- The Air Force completed developmental testing of the Air Force Mission Planning System Increment 5 (MPS Inc 5) C-17 and Mobility Air Force Automated Flight Planning Service (MAFPS) modules and certified these ready for IOT&E in FY17.
- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted the C-17 Joint Mission Planning System (JMPS) IOT&E in 4QFY17. DOT&E issued an operational test report in December 2017 in support of the Air Force full deployment decision.
- AFOTEC began MAFPS IOT&E in August 2017 and plans to complete this testing in November 2017. Upon completion DOT&E will issue an operational test report on the effectiveness and suitability of MAFPS.
- The classified MAFPS functions were ready for test during the IOT&E period. However, its enclave-dependent environment and the interfaces required to implement the SECRET Internet Protocol Router (SIPR) concept of operations were not ready. Therefore, additional post-IOT&E operational test and evaluation will be required to assess MAFPS classified capabilities.

System

- The Air Force MPS Inc 5 is a software-only acquisition category III program consisting of common mission planning software modules for unit-level aircraft platform mission planning and centralized Mobility Air Forces Air Operations Center global mobility planning and dispatching.
- MPS Inc 5 migrates Air Force airlift (C-5), tanker (KC-135, KC-10), airdrop (C-17, C-130), and combat search and rescue (HH-60 and HC/MC-130) legacy mission planning platforms to the JMPS.
  - JMPS is a standard desktop configuration solution for Air Force aircraft mission planning consisting of a package of common and platform-unique mission planning applications.
  - Aircraft platform-specific Mission Planning Environments (MPEs) are sets of developed applications built from a Framework, common components, and unique planning components.
  - The Framework is the basis of the MPE. Software developers add common components (e.g., weather, electronic warfare planner, etc.) and federated applications that support multiple users to the framework. Developers

then add a unique planning component for the specific aircraft type (e.g., C-17) to complete the MPE.
  - An MPE can operate as an unclassified system or a classified system.
- MPS Inc 5 MAFPS replaces the legacy Air Force Air Mobility Command (AMC) 618th Air Operations Center (AOC)-Tanker Airlift Control Center Advanced Computer Flight Plan (ACFP) mission planning system.
  - MAFPS software supports AOC-level mission planning for Mobility Air Forces global strategic airlift, aerial refueling, and tactical airlift missions.
  - The MAFPS command and control enclave consists of a server suite; AOC, global flight planning, and administration clients; and mobility enterprise information services providing connections to external sources of information required to plan global air mobility missions.
  - MAFPS is a data-driven mission planning system that integrates aircraft performance data, weather, airspace restrictions, Digital Aeronautical Flight Information File data, global routing considerations, and international boundaries enabling global air mobility planning.
  - MAFPS is designed to automate global mobility planning processes and data integration not available with the legacy ACFP mission planning system. MAFPS is further designed to provide a means for mission planners to optimize route planning with respect to flight mission time and fuel considerations.

Mission
- AMC MAFPS force-level global mobility planning occurs worldwide at AOCs. For example, U.S. Transportation Command planners use MAFPS in the AOC environment then pass products to units for execution.
- At the aircraft unit level, individual aircrews or mission planning cells use MPS Inc 5 JMPS to plan flight missions across the full spectrum of air missions ranging from peacetime training missions to complex combat missions.

Major Contractors
- DCS Corporation – Alexandria, Virginia
- BAE Systems – San Diego, California
- TYBRIN Corporation – Fort Walton Beach, Florida

Activity
- AFOTEC conducted MPS Inc 5 testing in accordance with the DOT&E-approved TEMP and the DOT&E-approved C-17 JMPS and MAFPS IOT&E plans.
- The Air Force completed MPS Inc 5 C-17 and MAFPS developmental testing in FY17 and certified the systems ready for IOT&E.
- AFOTEC conducted the C-17 MPS Inc 5 JMPS IOT&E from July through September 2017.
  - The planned cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) did not occur due to availability of the supporting test organization. Results of previous developmental test and evaluation cybersecurity cooperative vulnerability assessments informed the cybersecurity Adversarial Assessment in place of the planned IOT&E CVPA.
  - AFOTEC was not able to load and manipulate mission planning products in the C-17 simulator at Charleston AFB, South Carolina, pending completion of a Cyber Impact Evaluation by the C-17 Program Office.
  - IOT&E test data analysis was ongoing at the end of FY17.
- AFOTEC began MAFPS IOT&E in August 2017, and plans to complete testing in November 2017.
  - The classified MAFPS functions were ready for test during the IOT&E period. However, its enclave-dependent environment and the interfaces required to implement the SIPR concept of operations were not ready. Post-IOT&E, formal FOT&E will be required to evaluate these capabilities.

Assessment
- As of the end of FY17, DOT&E analysis of MPS Inc 5 IOT&E data and results was ongoing. DOT&E issued its operational test report in December 2017 to support the Air Force planned full deployment decision.
- Depending on results of the MPS Inc 5 C-17 JMPS IOT&E cybersecurity Adversarial Assessment, a post-IOT&E operational CVPA may be required to identify shortfalls not found during developmental testing assessments.
- MAFPS classified capabilities will require formal FOT&E once these systems are ready for operation.

Recommendations
- Status of Previous Recommendations. There are no previous recommendations.
- FY17 Recommendation.
  1. The Air Force should plan on conducting formal FOT&E of MAFPS classified capabilities as soon as system readiness allows in FY18.

MQ-9 Reaper Armed Unmanned Aircraft System (UAS)

Executive Summary

- The Air Force fielded the Block 5 Remotely Piloted Aircraft (RPA) and Block 30 Ground Control System (GCS) in May 2017 and began conducting combat Block 5 RPA/ Block 30 GCS combat operations in June 2017. Results of the FY16 Air Force Operational Test and Evaluation Center (AFOTEC) FOT&E of the MQ-9 Block 5 RPA and Block 30 GCS demonstrated that the system was not operationally capable of conducting wide area searches to hunt fixed or moving targets with the Lynx Synthetic Aperture Radar (SAR) system. Furthermore, FOT&E results showed that the MQ-9 Unmanned Aircraft System (UAS) was not operationally effective in the hunter mission role. FOT&E results also established that the Block 5 RPA and Block 30 GCS were not operationally suitable, and the Block 5 RPA was subject to overheating problems in operationally relevant environments.
- In May 2017, the Air Force 53rd Wing began a Force Development Evaluation (FDE) of the MQ-9 system to test software and hardware changes intended to correct some of the deficiencies from the FY16 FOT&E. The FDE is ongoing, and to date has demonstrated that the Air Force addressed the overheating problems observed during the FY16 FOT&E, but did not resolve the radar system deficiencies encountered during the test. Additional preliminary observations indicate the following:
  - An improved aircraft Generator Control Unit (GCU) and expansion of the Payload Control Computer (PCC) thermal operating limits have alleviated Block 5 RPA overheating problems encountered in FY16 FOT&E.
  - Block 30 GCS radar control human-machine interface (HMI) improvements enabled aircrews to perform simple SAR tasks such as spot image and moving target indicator (MTI) radar scan operations; however, the Lynx SAR continues to be difficult to configure in the GCS, remains unreliable, and has not demonstrated the ability to perform operationally relevant wide-area search functions.
- The Air Force continues planning to upgrade the MQ-9 GCS to the Block 50 configuration beginning in FY21. Block 50 GCS development and fielding is a major acquisition effort projected to cost approximately $1 Billion. The Air Force intends for the Block 50 GCS to incorporate an ergonomically optimized cockpit, new HMI, multi-level security, improved cautions and warnings interface, and separated flight and payload systems. The Air Force has not completed a new Test and Evaluation Master Plan (TEMP) to support the Block 50 GCS test and evaluation activities.

System

- The MQ-9 Reaper UAS is a remotely piloted and armed aircraft system that uses optical, infrared, and radar sensors to locate, identify, target, and attack ground targets.

  - The MQ-9 RPA is a medium-sized aircraft that has an operating ceiling up to 50,000 feet, an internal sensor payload of 800 pounds, an external payload of 3,000 pounds, and an endurance of approximately 14 hours.
  - Aircraft sensors include the Multi-spectral Targeting System (MTS)-B electro-optical and infrared targeting sensor and the Lynx SAR system.
  - The GCS commands the MQ-9 RPA for launch, recovery, and mission control of sensors and weapons. RPA launch and recovery operations use C-band line-of-sight datalinks, and RPA mission control uses Ku-band satellite links.
- MQ-9 RPAs carry AGM-114 HELLFIRE II anti-armor precision laser-guided missiles, GBU-38 Joint Direct Attack Munition (JDAM) 500-pound bombs, and GBU-12 500-pound, laser-guided bombs.
- The Air Force is using an evolutionary acquisition approach for meeting Increment One Capability Production Document requirements, with Block 1 and Block 5 RPAs and Block 15 and Block 30 GCSs.
- The Air Force is currently fielding the Block 5 RPA and the Block 30 GCS.
- The Air Force designed the Block 5 RPA to incorporate improved main landing gear, an upgraded electrical system with more power, an additional ARC-210 radio, encrypted datalinks, a redesigned avionics bay and digital electronic engine control system, the BRU-71 bomb rack, high-definition video, and upgraded software to allow the two-person aircrew to operate all onboard sensors and systems.
- The Air Force designed the Block 30 GCS to incorporate upgraded flight control displays and avionics, secure digital datalinks, Integrated Sensor Control System, Continuous Look Attack Management for Predator, Control of Lynx and Analysis Workstation software, and high-definition multifunction displays.

Mission
- Combatant Commanders use units equipped with the MQ-9 to conduct armed reconnaissance and pre-planned strikes. When provided wide-area search cues from off-board sources, units equipped with MQ-9s can execute cued searches to find, fix, track, target, engage, and assess critical emerging targets (both moving and stationary).
- MQ-9 units can also conduct aerial intelligence gathering, reconnaissance, surveillance, and target acquisition for other airborne platforms.

Major Contractor
General Atomics Aeronautical Systems Inc. – San Diego, California

---

Activity
- The Air Force conducted MQ-9 testing in accordance with the DOT&E-approved TEMP.
- The Air Force fielded the Block 5 RPA and Block 30 GCS on May 15, 2017, and began conducting Block 5 RPA/Block 30 GCS combat operations in June 2017.
- The Air Force will complete delivery of the MQ-9 program of record fleet under low-rate initial production.
- In May 2017, the Air Force 53rd Wing began an FDE of the MQ-9 UAS at Creech Air Force Base, Nevada, to assess Operational Flight Program (OFP) software version 904.6.4 and hardware changes intended to correct deficiencies and address some of the FY16 FOT&E shortfalls. As of the end of FY17, the FDE is ongoing. Key hardware and software changes incorporated the following:
  - Improved GCU. The GCU controls the engine operating speed at which the generator will begin supplying electrical power to the RPA. The Air Force redesigned the GCU to enable RPA GCU electrical power during ground operations at lower power settings to conserve aircraft battery life prior to take-off.
  - Increased PCC temperature limits. During the FY16 FOT&E, the PCC often reached its yellow caution temperature limit before take-off, contributing to ground aborts. The Air Force reevaluated the yellow caution temperature limit and determined that it could be raised from 85 degrees Celsius to 96 degrees Celsius with no deleterious effects to the PCC.
  - Improved Lynx SAR GCS HMI. The Air Force developed a simpler interface to partially replace the complicated SAR HMI flown during the FY16 FOT&E. The new interface reduces the modes available to spot images and MTIs and uses graphical cues to indicate the spot resolutions, MTI target sizes, and speeds available. The previous legacy system interface is still available for executing other complex SAR modes.
  - MTS-B hardware and software changes. MTS-B hardware now includes both the legacy AN/DAS-1 and new AN/DAS-4 hardware. The AN/DAS-4, which the Air Force intends to field in FY18, is an upgraded version of the entire MTS B system that incorporates additional high-definition video modes, target location accuracy enhancements, automatic boresight alignment, and a laser designator tracker. New MTS-B software, compatible with both hardware versions, includes split screen modes to enable simultaneous viewing of targets in different modes.
  - Video-Oriented Transceiver for Exchange of Information (VORTEX). VORTEX provides encrypted MTS B video and metadata to MQ-9-supported ground units equipped with Remotely Operated Video Enhanced Receiver (ROVER) hardware kits.
- The Air Force continues planning to upgrade the GCSs to the Block 50 configuration starting in FY21. The Block 50 GCS development and fielding is a major acquisition effort projected to cost approximately $1 Billion. The Block 50 GCS is expected to incorporate an ergonomically optimized cockpit, new HMI, multi-level security, improved cautions and warnings interface, and separated flight and payload systems.
- General Atomics delivered the last of 195 Block 1 RPAs to the Air Force in 2015, and then transitioned the production line to Block 5 RPAs. As of July 2017, General Atomics had delivered 52 of 155 planned Block 5 RPAs. Total Air Force MQ-9 deliveries as of July 2017 include 247 of 350 planned MQ-9s (Block 1 and Block 5 combined). General Atomics plans to deliver the final Block 5 RPA in FY21.

Assessment
- Results of the FY16 AFOTEC FOT&E of the MQ-9 Block 5 RPA and Block 30 GCS demonstrated that the system was not operationally capable of conducting wide-area searches to hunt fixed or moving targets with the Lynx SAR system. Furthermore, FOT&E results showed that the MQ-9 UAS was not operationally effective in the hunter mission role. FOT&E results also established that the Block 5 RPA and Block 30 GCS were not operationally suitable, and the Block 5 RPA was subject to overheating problems in operationally relevant environments.
- The 2017 FDE is ongoing, and to date has demonstrated that the Air Force addressed the overheating problems observed during the FY16 FOT&E, but did not resolve the radar system deficiencies encountered during the test. Additional preliminary observations indicate the following:

- An improved aircraft GCU and expansion of the PCC thermal operating limits have alleviated Block 5 RPA overheating problems encountered in the FY16 FOT&E.
- The improved GCU appears to be functioning correctly. Battery depletion problems on the ground encountered during testing in the FY16 FOT&E have not been observed in the FY17 FDE, and pilots have not had to monitor battery status as closely as the FOT&E testers had to resulting in lower pilot workloads during ground operations.
- The PCC temperature limit increase allows more time for ground operations without encountering overheating, which contributed to reduced pilot workload.
- Block 30 GCS radar control HMI improvements enabled aircrews to perform simple SAR tasks such as spot image and MTI radar scan operations; however, the Lynx SAR continues to be difficult to configure in the GCS, remains unreliable, and has not demonstrated the ability to perform operationally relevant wide-area search functions.
- The new MTS-B AN/DAS-4 sensor and software appear to provide useful capabilities that function as designed. The split screen mode aided target location. Automatic boresight alignment capability eliminated the requirement to have a local target board and associated infrastructure to perform airborne manual boresights for the video camera and laser designator.
- Combat Search and Rescue scenarios demonstrated that the MQ-9 aircrews could establish radio communications with a downed pilot, secure the area around the downed pilot from enemy forces by taking SAR spot images, and monitor the area with SAR MTI.
- The MQ-9 transmitted unencrypted and encrypted MTS-B video and metadata to ground units equipped with ROVER; however, transmission reliability from VORTEX to ROVER was not consistently reliable.
- Unencrypted and encrypted radio communications were demonstrated; however, communication on some frequencies was poor. HAVEQUICK radio communication does not work well.
- The MQ-9 UAS maintenance construct requires Air Force personnel to maintain both the RPA and GCS. Air Force maintainers cannot consistently maintain the Block 30 GCS without assistance from contractor personnel.

- The Air Force currently plans to complete the MQ-9 Increment One system with the Block 50 GCS and a future system OFP. The AFOTEC IOT&E of the Block 50 GCS and future capabilities is scheduled to occur in FY22 or later. A new TEMP is required to document the test strategy and resources necessary to evaluate the Block 50 GCS; incorporation of new program of record content; and testing of Lynx SAR wide-area search capabilities that could not be performed during the FY16 FOT&E.

Recommendations

- Status of Previous Recommendations. The Air Force made some progress toward, but did not fully satisfy the FY16 recommendations to correct shortfalls identified during the FY16 FOT&E.
- FY17 Recommendations. The Air Force should:
  1. Correct the shortfalls identified in the FY16 FOT&E and FY17 FDE, including problems with the SAR, and confirm preliminary findings that hot weather thermal management shortfalls have been successfully mitigated.
  2. Conduct sufficient testing during Block 50 IOT&E to determine the ability of the MQ-9 system to execute an all-weather operational hunter mission role using the SAR.
  3. Develop and submit a new TEMP for DOT&E approval, documenting the incorporation of new program of record content (e.g., the Block 50 GCS) and the test and evaluation strategy and resources required to mature and test these capabilities and systems.

RQ-4B Global Hawk High-Altitude Long-Endurance Unmanned Aerial System (UAS)

Executive Summary

- DOT&E approved the Air Force Capstone Test and Evaluation Master Plan (TEMP) in June 2016, which provides an overarching test approach for the system architecture and capability upgrades included in the new program baseline and future modernization programs. DOT&E anticipates that the program will develop TEMP annexes according to the requirements and schedule documented in the approved Capstone TEMP.
- The Air Force is currently planning to conduct RQ-4B Block 30/Airborne Signals Intelligence Payload (ASIP) FOT&E in either FY18 or FY19 depending on ASIP Increment 1 development progression and availability of RQ-4B Block 30 developmental test assets. This test will include a re-evaluation of the RQ-4B Block 30 Signals Intelligence (SIGINT) mission capabilities with the ASIP sensor, as well as an assessment of previously identified ground station, air vehicle, communication system, interoperability, and cybersecurity shortfalls.
- The MS-177 sensor radiated high levels of electromagnetic interference (EMI) during Northrup Grumman developmental testing in an anechoic chamber. This high-level EMI can interfere with the ASIP system, producing false signal detection reports. The program is in the process of investigating this problem to determine an acceptable solution.
- There is a significant delay when the RQ-4B platform is transferring MS-177 sensor images to the Distributed Ground Station (DGS) installations using the legacy system link. Although the RQ-4B is a strategic platform, these delays do not allow the operator to determine when to reacquire an image or allow the exploitation of imagery in near real-time to support warfighter intelligence needs.
- Testing of the new weather radar showed three deficiencies all associated with the Keyboard-Video-Monitor switch: (1) the switch location adversely effects pilot operations because switch usage requires the pilot to leave his position to access the switch; (2) the switch button logic does not allow the ground system to display the weather radar information while allowing the pilot to also manipulate SECRET Internet Protocol Router Network (SIPRNET) functions; and (3) when the switch needs to be power-cycled to regain functionality, it requires a minimum of 10 minutes to allow maintenance personnel to remove a panel and disconnect then reconnect power to the switch thus adversely interrupting the intelligence collection process. The program is in the process of addressing all three of these deficiencies with full implementation of a new switch planned to occur by the end of December 2017.

- In July 2016, DOT&E published the classified RQ-4B Global Hawk Block 40 IOT&E report based on test results from the RQ-4B Block 40/Multi-Platform Radar Technology Improvement Program (MP-RTIP) IOT&E conducted from September 2015 through January 2016. DOT&E discontinued oversight of the RQ-4B Block 40 program in September 2016 since the IOT&E had completed and the Air Force did not plan to implement any major capability enhancements to the platform.

System

- The RQ-4B Global Hawk is a remotely piloted, high-altitude, long-endurance airborne intelligence, surveillance, and reconnaissance (ISR) system that includes the Global Hawk unmanned air vehicle, various intelligence and communications relay mission payloads, and supporting command and control ground stations.
- The RQ-4B Global Hawk Block 30 system is equipped with a multi-intelligence payload that includes both the Enhanced Integrated Sensor Suite imagery intelligence payload and ASIP SIGINT sensor. The Air Force is in the process of retrofitting two Block 30 aircraft with the Multi-Spectral (MS)-177 sensor to provide high resolution MS imaging capability with accurate and automatic geolocation capabilities at high stand-off ranges.
- All RQ-4B systems use line-of-sight and beyond line-of-sight communication systems to provide air vehicle command and control and to transfer collected intelligence data to ground stations for exploitation and dissemination.

- The Air Force Distributed Common Ground System (AF DCGS) supports ISR collection, processing, exploitation, analysis, and dissemination for the Block 30 Global Hawk system. The AF DCGS employs global communications architecture to connect multiple intelligence platforms and sensors to numerous DGS installations where intelligence analysts produce and disseminate intelligence products.
- The Air Force has taken delivery of all 21 RQ-4B Block 30 air vehicles along with 9 Mission Control and 10 Launch and Recovery ground stations. Each Launch and Recovery ground station controls one air vehicle. The Air Force does not intend on procuring any additional Mission Control or Launch and Recovery ground stations.

Mission

- Commanders use RQ-4B Global Hawk reconnaissance units to provide high-altitude, long-endurance intelligence collection capabilities to support theater operations. Units equipped with RQ-4B Global Hawk use line-of-sight and beyond line-of-sight satellite datalinks to control the Global Hawk system and transmit collected intelligence data.
- Operators collect imagery and SIGINT data to support ground units and to identify intelligence-essential elements of information for theater commanders.
- Ground-based intelligence analysts exploit collected imagery, ground-moving targets, and SIGINT to provide intelligence products that support theater operations.
- Forward-based personnel can receive imagery intelligence directly from Global Hawk.

Major Contractor

Northrop Grumman Aerospace Systems, Strike and Surveillance Systems Division – San Diego, California

---

Activity

- The Air Force is currently planning to conduct FOT&E in FY18 or FY19 depending on ASIP Increment 1 development progression and availability of RQ-4B Block 30 developmental test assets. This test will include a complete re-evaluation of the RQ-4B Block 30 SIGINT mission capabilities with the ASIP sensor, as well as an assessment of previously identified ground station, air vehicle, communication system, interoperability, and cybersecurity shortfalls.
- DOT&E approved the Air Force Capstone TEMP in June 2016, which provides an overarching test approach for the system architecture and capability upgrades included in the new program baseline and future modernization programs. DOT&E anticipates that the program will develop TEMP annexes according to the requirements and schedule documented in the approved Capstone TEMP.
- The Air Force is currently developing a comprehensive program test strategy and TEMP to correct previously identified RQ-4B Block 30 capability shortfalls and test a series of modernization upgrades. This strategy will identify the next set of RQ-4B Block 30 FOT&E events planned for FY18. Events include re-evaluation of previously identified ASIP/SIGINT mission capability shortfalls, interoperability deficiencies, MS-177 sensor integration, weather radar integration, mission planning upgrades, and other system modernization changes.
- The 53 Test and Evaluation Group, Detachment 2 conducted a Force Development Evaluation under an Air Combat Command-approved test plan from July through August 2017 to support fielding of the new weather radar system installed on the RQ-4B platform.

Assessment

- Since the RQ-4B Block 30 combined with ASIP IOT&E in 2011, the Air Force has corrected most RQ-4B air vehicle reliability and availability problems and implemented many of previously planned system improvements. However, because of programmatic difficulties resulting from the previous DOD decision to retire the RQ-4B fleet, the Air Force has not yet conducted a comprehensive FOT&E to verify correction of all major IOT&E deficiencies.
- In July 2016, DOT&E published the classified RQ-4B Global Hawk Block 40 IOT&E report based on test results from the RQ-4B Block 40 MP-RTIP IOT&E conducted from September 2015 through January 2016. DOT&E discontinued oversight of the RQ-4B Block 40 program in September 2016 since the IOT&E had completed and the Air Force did not plan to implement any major capability enhancements to the platform.
- The MS-177 radiated high levels of EMI during Northrup Grumman developmental testing in an anechoic chamber. This high-level EMI can interfere with the ASIP system, producing false signal detection reports. The program is in the process of investigating this problem to determine an acceptable solution.
- There is a significant delay when the RQ-4B platform is transferring MS-177 sensor images to the DGS installations using the legacy system link. Although the RQ-4B is a strategic platform, these delays do not allow the operator to determine when to reacquire an image or allow the exploitation of imagery in near real-time to support warfighter intelligence needs.
- The Force Development Evaluation testing for the new weather radar showed three deficiencies all associated

with the Keyboard-Video-Monitor switch: (1) the switch location adversely effects pilot operations because switch usage requires the pilot to leave his position to access the switch; (2) the switch button logic does not allow the ground system to display the weather radar information while allowing the pilot to also manipulate SIPRNET functions; and (3) when the switch needs to be power-cycled to regain functionality, it requires a minimum of 10 minutes to allow maintenance personnel to remove a panel and disconnect then reconnect power to the switch thus adversely interrupting the intelligence collection process. The program is in the process of addressing all three of these deficiencies with full implementation of a new switch planned to occur by the end of December 2017.

Recommendations

- Status of Previous Recommendations. The Air Force has made progress toward addressing FY16 recommendations. The Air Force has begun to develop RQ-4B Capstone TEMP annexes to guide developmental and operational testing of these systems, articulate a plan to complete the FOT&E for the RQ-4B Block 30 SIGINT mission using the ASIP sensor, and address cybersecurity deficiencies observed during the RQ-4B Block 40/MP-RTIP IOT&E. The Air Force still needs to develop AF DCGS training, procedures, tools, communication, and management enhancements to allow exploitation of RQ-4B Global Hawk Block 40 GMTI data in near-real time.
- FY17 Recommendations. The Air Force should:
  1. Complete development of RQ-4B program Capstone TEMP annexes to guide execution of the RQ-4B Global Hawk Block 30 FOT&E and to define operational test requirements for future Block 30 system upgrades.
  2. Develop a plan to complete the FOT&E for the RQ-4B Block 30 SIGINT mission using the ASIP sensor.
  3. Conduct adequate flight tests to characterize the MS-177/ASIP EMI problem to determine an acceptable solution for Air Combat Command.
  4. Address the image transfer latency problem from the MS-177 to the DGS when using the legacy system link.

Small Diameter Bomb (SDB) II

Executive Summary

- The Small Diameter Bomb (SDB) II developmental and live fire testing is ongoing. The Air Force began Government Confidence Testing (GCT) in October 2016. The Air Force awarded the Low-Rate Initial Production Lot 3 contract for 250 weapons in January 2017.
- The SDB II is progressing in the Normal Attack (NA) mode, the primary employment method for the SDB II. The Air Force successfully demonstrated Coordinate Attack (CA) in 2017 and is progressing toward demonstrating Laser Illuminated Attack (LIA) in 2017 prior to entering IOT&E.
- The program implemented corrective actions and fixes for all failure modes discovered in developmental test. The program discovered five anomalies in GCT, identified and implemented a fix for one, and continues working solutions to address the remaining four.
- The Air Force is scheduled to begin IOT&E in 3QFY18 with an adequately resourced test program.

System

- The SDB II is a 250-pound, air-launched, precision-glide weapon that uses deployable wings to achieve standoff range. F-15E aircraft employ SDB IIs from the BRU-61/A four-weapon carriage assembly.
- The Air Force directed design of the SDB II to provide the capabilities deferred from SDB I. It includes a weapon datalink allowing for post-launch tracking and control of the weapon, as well as a multi-mode seeker to provide the ability to strike mobile targets in adverse weather.
- The SDB II combines Millimeter-Wave radar, imaging infrared, and laser-guidance sensors in a terminal seeker, in addition to a GPS and an Inertial Navigation System to achieve precise guidance accuracy in adverse weather.
- It incorporates a multi-function warhead (blast, fragmentation, and shaped charge jet) designed to defeat armored and non-armored targets. The weapon can be set to initiate on impact, at a preset height above the intended target, or in a delayed mode.

- The Air Force intends the SDB II to provide reduced collateral damage while achieving kills across a broad range of target sets by precise accuracy, small warhead design, and focused warhead effects.
- There are three principal attack modes: NA, LIA, and CA. The SDB II can be used against moving or stationary targets using its NA (radar/infrared sensors) or LIA modes, and fixed targets with its CA mode.
- The SDB II provides increased weapons load per aircraft compared to legacy air-to-ground munitions used against offensive counter-air, strategic attack, interdiction, and close air support targets in adverse weather.

Mission

- Combatant Commanders will use units equipped with the SDB II to attack stationary and moving ground targets in degraded weather conditions at standoff ranges.
- An SDB II-equipped unit or Joint Terminal Attack Controller (JTAC) will engage targets in dynamic situations and use a weapon datalink network to provide in-flight target updates, in-flight retargeting, weapon in-flight tracking, and, if required, weapon abort.

Major Contractor

Raytheon Missile Systems – Tucson, Arizona

Activity

- As of 2017, the Air Force has completed 19 NA, 3 CA, 4 LIA Guided Test Vehicle (GTV) and 13 Live Fire (LF) tests against moving and stationary targets as part of contractor-led developmental testing. The Air Force conducted 7 GTV and 6 LF tests with ultrahigh frequency updates; 12 GTV and 7 LF test shots were conducted with Link 16 updates. NA is the primary employment method for the SDB II.
- The Program Office completed 17 rounds of seeker Captive Flight Tests, resulting in over 2,260 target runs in a wide variety of terrain and environmental conditions. These tests provided terabytes of seeker performance data and logged over 483 hours of seeker operation without a single failure.
- The program has augmented and refined the Integrated Flight System (IFS) model by incorporating the results of over 2,260 Captive Flight Test runs as well as weapon flight tests. Raytheon released its IFS model verification and validation report in July 2017, and the Air Force Operational Test and

Evaluation Center expects to give initial accreditation prior to the start of operational testing.
- The Program Office completed over 2,000 hours of ground reliability testing and over 1,000 hours of in-flight reliability testing. The in-flight portion of captive carry reliability testing is ongoing.
- The program redesigned the Air Turbine Alternator (ATA), which provides power to the SDB II fuze, to address a deficiency identified during a captive flight test failure. Regression testing is nearing completion. At least 10 weapons incorporating the new ATA will be available and employed during IOT&E.
- The program began a 28-shot NA mode GCT program in October 2016, which is testing the weapon in more operationally realistic environments with more operationally representative hardware and software. GCT has completed 18 shots resulting in 14 successes, 3 failures, and 1 shot with anomalies still officially under review.
- The Air Force awarded the Low-Rate Initial Production Lot 3 contract on January 31, 2017, for 250 weapons.
- The Air Force conducted all testing in accordance with the DOT&E-approved Test and Evaluation Master Plan.

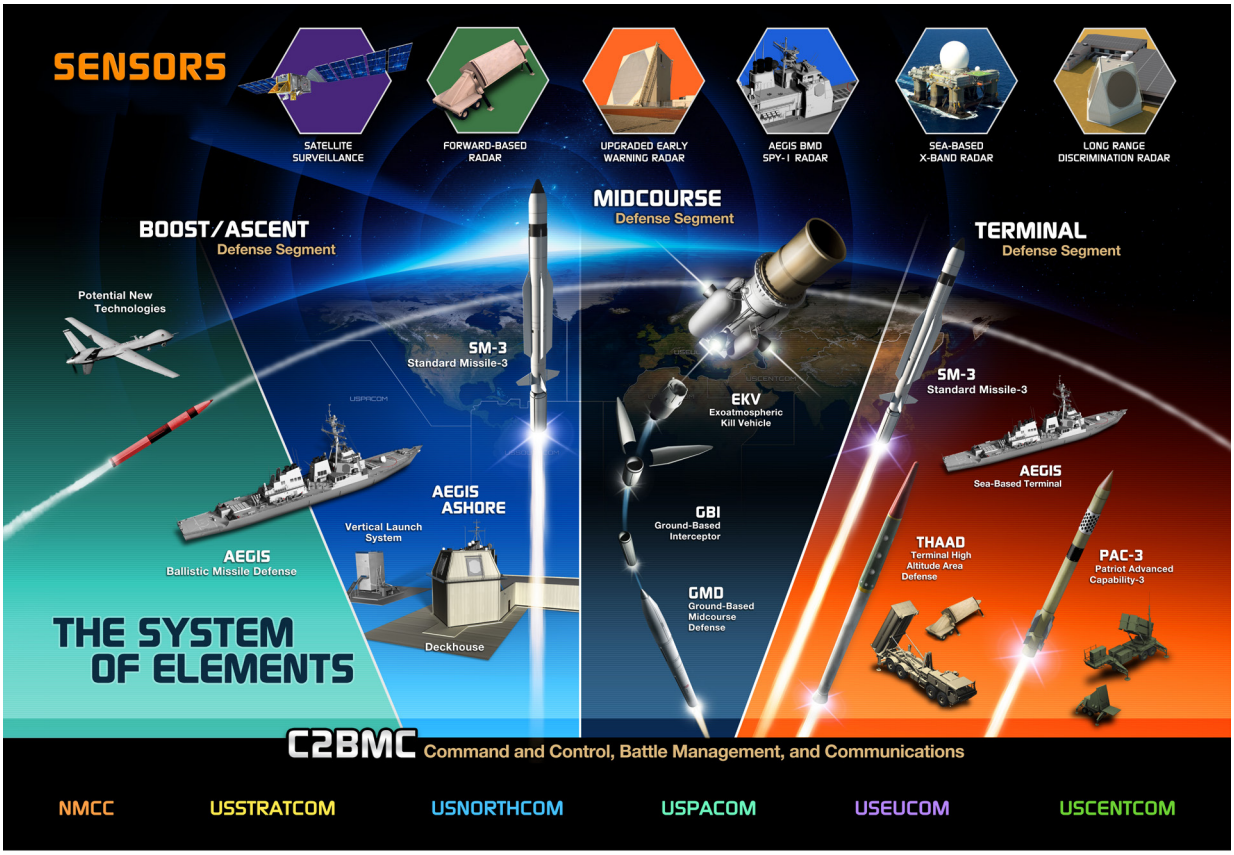
Assessment
- In the NA mode, the primary employment method for the weapon, the SDB II successfully engaged both moving and stationary targets, including proper classification of target type (wheeled versus tracked) on 19 of 22 GTV flight tests (including GCT); 3 events had failures. The program has implemented corrective actions and fixes for all failure modes discovered in test.
- The Air Force has completed 18 flight tests during GCT, which included instances of GPS degradation/denial, several JTAC-controlled weapons, simple denial and deception measures, in-flight retargeting, maneuvering and stop/start motion by targets, and higher clutter environments, including more decoy or confuser targets to stress the classification feature of the weapon. The Air Force has not yet accomplished successful employment against maritime targets, nor a ripple release (dropping multiple bombs in rapid succession) in GCT, both of which are planned to be completed prior to IOT&E.
- In the CA and LIA modes, the program adequately addressed the two failure types found in the CA mode, as demonstrated in test. The program conducted a successful test of a new software version in the LIA mode with another test scheduled before IOT&E to validate the fix.
- A total of 57 SDB IIs have been employed during testing to date. Forty weapons have been successful in terms of Free Flight Reliability, with 13 failures and 1 more under review because of anomalous performance. The resulting reliability level is between 0.75-0.76, depending on the resolution of the outstanding anomalies. This is below the 0.80 level to be achieved by the end of IOT&E; the rate of discovering new failure modes has been steady, implying the weapon is not yet fully mature. In addition, the program has thoroughly implemented corrective actions and fixes for all failure modes discovered in test and there have been no failures of components or software for which a fix has been implemented. Further testing in GCT and the Captive Carry Reliability Test program will be performed in an attempt to increase confidence in weapon reliability.
- The Program Office is preparing for IOT&E with an adequately resourced test program and no major unresolved programmatic testing problems. IOT&E is scheduled to begin in 3QFY18.
- One of the live fire test events (LF-10) detonated but failed to guide to the target. LF-10 was the first LF mission using LIA. The previous test using LIA (LIA-2) also missed its moving target. The failure investigation revealed the laser guidance algorithm to be inadequate against moving targets. The modification of the algorithm is ongoing. LIA-2 has been repeated and LF-10 will be repeated prior to IOT&E.
- The Air Force discovered five anomalies during GCT to date. These include: a software coding error that has been fixed and tested; a maritime target problem; and three anomalies related to employment against static targets, which are being addressed in a final weapon software version that will be tested prior to IOT&E.
- The SDB II continues to perform well against moving targets in the NA mode, but has difficulty in some conditions against static targets. A combination of software improvements and modified employment procedures to be implemented prior to IOT&E are expected to improve performance against static targets.
- Continued comparisons of the IFS model pre- and post-flight predictions indicate the model is adequate for the kinematics flown in flight test to date. Raytheon Missile Systems continues to develop and update the IFS model, which will be essential to the assessment of the results of live fire and operational testing. IFS, in combination with lethality and free flight reliability data, will produce single shot kill probability values needed to assess end-to-end weapon effectiveness against a range of operationally relevant targets.

Recommendations
- Status of Previous Recommendations. The Air Force completed all previous recommendations.
- FY17 Recommendations. The Air Force should:
  1. Continue to refine and coordinate the GCT test matrix to maximize confidence in readiness for IOT&E.
  2. Ensure that weapon software is finalized and adequately tested prior to the commencement of IOT&E.

Ballistic Missile Defense Systems

Ballistic Missile Defense Systems

Ballistic Missile Defense System (BMDS)



NMCC - National Military Comand Center
USCENTCOM - U.S. Central Command
USEUCOM - U.S. European Command
USNORTHCOM - U.S. Northern Command
USPACOM - U.S. Pacific Command
USSTRATCOM - U.S. Strategic Command

Executive Summary

- The Ground-based Midcourse Defense (GMD) element demonstrated the capability to defend the U.S. Homeland from a small number of intermediate-range ballistic missile (IRBM) or intercontinental ballistic missile (ICBM) threats with simple countermeasures when the Homeland Defense Ballistic Missile Defense System (BMDS) employs its full sensors/command and control architecture. This assessment is upgraded from FY16.
- The Regional/Theater BMDS demonstrated a limited capability to defend the U.S. Pacific Command (USPACOM), U.S. European Command (USEUCOM), and U.S. Central Command (USCENTCOM) areas of responsibility for small numbers of medium-range ballistic missile and IRBM threats (1,000 to 4,000 km), and a fair capability for short-range ballistic missile threats (less than 1,000 km range). This assessment is unchanged from FY16.
- The Missile Defense Agency (MDA) FY17 cybersecurity assessment activity represents progress and an initial commitment to operational cybersecurity assessment across multiple BMDS elements. The Army Research Laboratory Survivability/Lethality Analysis Directorate conducted cybersecurity assessments on parts of GMD; Command and Control, Battle Management, and Communications (C2BMC); BMDS Overhead Persistent Infrared Architecture (BOA); AN/TPY-2 Forward-Based Mode (FBM) radar; and Sea-Based X-band (SBX) radar. The Cybersecurity Vulnerability and Penetration Assessments (CVPAs) identified cybersecurity vulnerabilities; however, additional, less restrictive testing is required to inform cybersecurity vulnerability mitigation efforts, improve net defense, and characterize BMDS capability in a cyber-contested environment.
- The MDA conducted Flight Test, Ground-Based Interceptor-15 (FTG-15), intercepting an ICBM class target for the first time. FTG-15 was also the first intercept using the Capability Enhancement-II (CE-II) Block 1 exo-atmospheric kill vehicle (EKV) and the first demonstration of the three-stage Configuration 2 booster. The Homeland Defense BMDS performed nominally.
- The MDA conducted nine element-level flight tests and one Navy fleet exercise. No Theater/Regional BMDS-level intercept flight tests took place in FY17.

- The MDA conducted Ground Test, Integrated-07a (GTI-07a) and Ground Test, Distributed (GTD-07a), using strategic and theater/regional scenarios from the U.S. Northern Command (USNORTHCOM) and USPACOM areas of responsibility.
- Since FY10, DOT&E has assessed and reported annually that the lack of independent accreditation of modeling and simulation for performance assessment has limited DOT&E use of these data for quantitative evaluations. This assessment remains unchanged for FY17, although the MDA has made progress in defining high-priority accreditation gaps and allocating resources to address them. The MDA should increase the development priority and ensure adequate funding for the BMDS simulation-based performance assessment capability. This capability should include modeling and simulation verification, validation, and accreditation, as well as the ability to produce high-fidelity and statistically significant BMDS-level performance assessments.
- The MDA conducted numerous wargames and exercises designed to enhance Combatant Command ballistic missile defense (BMD) readiness and increase Service member confidence in the deployed elements of the BMDS.

System

The BMDS is a federated and geographically distributed system of systems that relies on element interoperability and warfighter integration for operational capability and efficient use of guided missile/interceptor inventory. The BMDS includes five elements: four autonomous combat systems and one sensor/command and control architecture.

- Autonomous combat systems – GMD, Aegis BMD/Aegis Ashore Missile Defense System (AAMDS), Terminal High-Altitude Area Defense (THAAD), and Patriot
- Sensor/command and control architecture
  - Sensors – COBRA DANE radar, Upgraded Early Warning Radars (UEWRs), SBX radar, AN/TPY-2 (FBM) radar, Aegis AN/SPY-1 radar aboard an Aegis BMD ship, and the Space Based Infrared System (SBIRS)
  - Command and control – C2BMC, including BOA

Mission

- USNORTHCOM, USPACOM, USEUCOM, and USCENTCOM employ the assets of the BMDS to defend the United States, deployed forces, and allies against ballistic missile threats of all ranges.
- The U.S. Strategic Command synchronizes operational-level global missile defense planning and operations support for the DOD.

Major Contractors

- The Boeing Company
  - GMD Integration: Huntsville, Alabama
- Lockheed Martin Corporation
  - Aegis BMD, AAMDS, and AN/SPY-1 radar: Moorestown, New Jersey
  - C2BMC: Huntsville, Alabama, and Colorado Springs, Colorado
  - SBIRS: Sunnyvale, California
  - THAAD Weapon System and Patriot Advanced Capability-3 Interceptors: Dallas, Texas
  - THAAD Interceptors: Troy, Alabama
- Northrop Grumman Corporation
  - GMD Fire Control and Communications: Huntsville, Alabama
  - BOA: Boulder, Colorado; Colorado Springs, Colorado; and Azusa, California
- Orbital ATK
  - GMD Booster Vehicles: Chandler, Arizona
- Raytheon Company
  - GMD EKV and Standard Missile-3/6 Interceptors: Tucson, Arizona
  - Patriot Weapon System including Guidance Enhanced Missile-Tactical interceptors, AN/TPY-2 radar, COBRA DANE radar, SBX radar, and UEWRs: Tewksbury, Massachusetts

---

Activity

- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan (IMTP).
- One developmental homeland defense intercept flight test, FTG-15, occurred in FY17. The MDA conducted FTG-15 in May 2017, intercepting an ICBM-class target for the first time using the GMD system, the AN/TPY-2 (FBM) radar, the C2BMC system, the SBX radar, and the SBIRS. FTG-15 was also the first intercept using the CE II Block 1 EKV and the first demonstration of the three-stage Configuration 2 booster.
- The MDA conducted nine element-level fight tests (five Aegis BMD tests, two THAAD tests, and two Patriot tests) and one Navy fleet exercise. No theater/regional BMDS-level intercept flight tests took place in FY17; the MDA had planned such a test with Aegis BMD and Patriot, however the Navy redirected the Aegis ship to support real-world operations.
- The MDA conducted GTI-07a in June 2017, assessing the BMDS Capability Increment 4 functionality improvements using strategic and theater/regional scenarios from USNORTHCOM's and USPACOM's areas of responsibility.
- The MDA conducted GTD-07a in September and October 2017. It complimented and executed many of the same scenarios as GTI-07a, but in a distributed test environment. GTD ground tests use live operational networks, whereas GTI ground tests use laboratory-based networks.
- The MDA conducted numerous wargames and exercises designed to enhance Combatant Command BMD readiness

and increase Service member confidence in the deployed elements of the BMDS.
- The MDA conducted cooperative cybersecurity assessments of parts of the following BMDS assets:
  - A limited CVPA of the FTG-15 GMD flight test architecture in June 2017.
  - A CVPA of USNORTHCOM's C2BMC S8.2-1.1, the C2BMC portion of the Cheyenne Mountain Management Node, the C2BMC Distributed Training System, and BOA 5.1 in July 2017.
  - An additional limited cooperative cybersecurity test on USNORTHCOM's C2BMC S8.2-1.1, BOA 5.1, and the AN/TPY-2 (FBM) radar CX2.1.1 configured with the Superdome computer processor in September 2017. The MDA used the event to verify corrective actions for some of the deficiencies identified during the C2BMC S8.2-1 and BOA 5.1 platform CVPA in July 2017.
  - A limited CVPA of the X-band radar (XBR) component of the SBX sensor in October 2017.

Assessment
- GMD has demonstrated capability to defend the U.S. Homeland from a small number of IRBM or ICBM threats with simple countermeasures when the Homeland Defense BMDS employs its full sensors/command and control architecture.
- The Regional/Theater BMDS demonstrated a limited capability to defend the USPACOM, USEUCOM, and USCENTCOM areas of responsibility for small numbers of medium-range ballistic missile and IRBM threats (1,000 to 4,000 km), and a fair capability for short-range ballistic missile threats (less than 1,000 km range). The Theater/Regional BMDS assessment remains unchanged since no Theater/Regional BMDS-level intercept flight tests took place in FY17. This also means that there were no flight test opportunities for BMDS-level integrated training for warfighters.
- The MDA made progress toward characterizing the cybersecurity posture of fielded and soon-to-be fielded BMDS Increment 4 capabilities. Additional CVPAs and Adversarial Assessments (AAs) are required to support a comprehensive cybersecurity assessment of BMDS network and system cybersecurity.
  - All CVPAs and cybersecurity assessments in FY17 identified cybersecurity vulnerabilities; however, critical limitations affecting test adequacy resulted from constrained test boundaries; insufficient time to plan, coordinate activity, and resolve technical issues prior to test events; and in the case of AN/TPY-2(FBM) radar, limited asset availability resulting from real-world operational needs in USPACOM.
  - The MDA has not yet conducted any AAs on any operational systems in the BMDS architecture, which are necessary to support a cybersecurity survivability assessment.
- During FTG-15, the Homeland Defense BMDS performed without fault. The three-stage Configuration 2 GBI booster flew as designed and delivered the EKV to the proper geographic position with the desired velocity. The CE-II Block 1 EKV intercepted and negated the ICBM-representative reentry vehicle. Guidance systems throughout the engagement functioned nominally.
- During FY17 ground testing, the MDA exercised new capabilities and assessed BMDS interoperability using hardware-in-the-loop simulation and operational assets communicating over operational networks (GTI-07a and GTD-07a, respectively). Test data informed enhanced homeland defense and theater/regional functionality development for BMDS Capability Increment 4, which is defined as:
  - BOA data integrated into the BMDS and providing X-band cues.
  - BMD planning, SBIRS interface change, and communications enhancements.
  - Performance improvements and GBI reliability upgrade.
  - Implementation of updated cybersecurity protections.
- In FY10, DOT&E reported, "the MDA began execution of its revamped IMTP to collect the data needed to accredit the models and simulations used for assessing performance and effectiveness of the BMDS." Through FY16, DOT&E has assessed and reported annually that the lack of independent accreditation of modeling and simulation for performance assessment have limited DOT&E use of these data for quantitative evaluations. This assessment remains for FY17, although this year the MDA and the BMDS Operational Test Agency jointly identified and are developing plans to resolve the major limitations that have been prohibiting accreditation of the models. Accreditation across the elements and the BMDS framework is still several years away.

Recommendations
- Status of Previous Recommendations. The MDA has addressed all but eight previous BMDS recommendations, three of which are classified and therefore not listed here.
  1. All Services should develop and implement integrated BMDS-level training in formal warfighter certification plans.
  2. Discrimination and debris mitigation techniques warrant further development by MDA.
  3. The MDA should publish a comprehensive BMDS cybersecurity description document that delineates the strategy at the BMDS-level as well as at the element-level for effective cybersecurity, achievable milestones for implementing the strategy, and stakeholder roles and responsibilities at all cybersecurity tiers.
  4. The MDA should conduct comprehensive cybersecurity assessments and electronic warfare testing across all BMDS elements.
  5. The MDA should increase the development priority and associated funding for the BMDS simulation-based

performance assessment capability including modeling and simulation verification, validation, and accreditation, and the ability to produce high-fidelity and statistically-significant BMDS-level performance assessments.

- FY17 Recommendations. The MDA should:
  1. Fund each of the individual elements/model developers to address the major modeling and simulation limitations that are preventing independent accreditation.
  2. Conduct more rigorous operational assessment of BMDS assets via operational CVPAs and AAs to inform cybersecurity vulnerability mitigation efforts, improve net defense, and characterize BMDS capability in a cyber-contested environment. The MDA should leverage opportunities to conduct AAs on operational assets in FY18 in cooperation with ongoing Persistent Cyber Operations and the DOT&E Cybersecurity Assessment Program.
  3. Develop a comprehensive cybersecurity test and evaluation strategy for each BMDS element and implement these strategies through the IMTP. The strategy for each element should include:
     - Plans to conduct independent cybersecurity assessments of existing operational BMDS assets to inform the Department's understanding of the current BMDS cybersecurity posture and operational environment.
     - Cybersecurity test activities earlier in the development cycle to inform system design and software configuration changes.
     - Rigorous operational cybersecurity T&E to support fielding of new capabilities in order to properly inform operational risk assessments; mitigate critical cybersecurity vulnerabilities; improve network defense; and ultimately make BMDS systems and networks more secure against cyber adversaries.
     - Consistent cybersecurity assessment approach, commitment, and accesses to critical BMDS assets across the elements.
  4. In planning cybersecurity events, include sufficient time for the Program Office, the BMDS Operational Test Agency, and DOT&E to obtain needed resources for each event. Late execution of test planning and test plan delivery leaves insufficient time to resolve key issues (e.g., inadequate detail in the test conduct, data management, analysis, and evaluation plans).
  5. Leverage and coordinate with ongoing cybersecurity assessment efforts to conduct operational cybersecurity assessments (CVPAs and AAs) in order to maximize efficiency and reduce duplication of activity across the DOD. These efforts include the DOT&E Cybersecurity Assessment Program, the USD(AT&L) cyber assessment efforts in support of section 1647 of the FY16 National Defense Authorization Act, and the Department's ongoing Persistent Cyber Operations.

Sensors / Command and Control Architecture

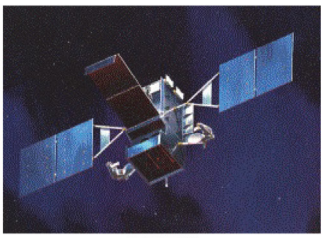

Aegis AN/SPY-1 Radar


AN/TPY-2


Cobra Dane


C2BMC


UEWR


SBIRS


Sea-Based X-band Radar

C2BMC - Command and Control, Battle Management and Communications
SBIRS - Space-Based Infrared System
UEWR - Upgraded Early Warning Radars

Executive Summary

- The Missile Defense Agency (MDA) continued to mature the Ballistic Missile Defense System (BMDS) sensors/command and control architecture. The MDA:
  - Used the sensors and/or the command and control architecture in nine tests and supported four additional Air Force intercontinental ballistic missile (ICBM) reliability and sustainment flight tests.
  - Completed the Critical Design Review for the Long-Range Discrimination Radar.
  - Initiated the defense of Hawaii radar program.
  - Completed the Sensor Analysis of Alternatives and presented the findings to the Missile Defense Executive Board.
- The Army Research Laboratory Survivability/Lethality Directorate (ARL/SLAD) conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) of the Command and Control, Battle Management, and Communications (C2BMC) system and the BMDS Overhead Persistent Infrared Architecture (BOA), as well as a limited CVPA (no penetration testing) on the AN/TPY-2 (Forward-Based Mode (FBM)) radar to identify cybersecurity vulnerabilities; verify fixes for some vulnerabilities; and collect data on a new tool intended to improve C2BMC network defense. The MDA has not yet conducted Adversarial Assessments (AAs) on any sensors or command and control assets in the BMDS architecture, which are necessary to support a cybersecurity survivability assessment.
- The MDA and the Army continue working to achieve Full Materiel Release of the AN/TPY-2 (FBM) radar. Of the 33 total materiel release conditions, 9 have been closed and the remaining 24 are expected to be closed in the next 2 years.
- AN/TPY-2 (FBM) radar operator training and Interactive Electronic Technical Manuals (IETMs) continue to be deficient.
- The MDA began ground testing C2BMC Spiral 8.2 (S8.2), which implements a redundant unified client that replaces two independent clients implemented in C2BMC S6.4.

System

- The BMDS sensors are systems that provide real-time ballistic missile threat data to the BMDS. The Services use the data to counter ballistic missile attacks. The Army, Navy, Air Force, and the MDA operate the sensor systems.
  - The COBRA DANE radar is a fixed site, single-face, L-band phased array radar operated by the Air Force and located at Eareckson Air Station (Shemya Island), Alaska.
  - The Upgraded Early Warning Radars (UEWRs) are fixed site, multiple-face, ultrahigh frequency radars, operated by the Air Force and located at Beale AFB, California, and Thule Air Base, Greenland (two radar faces each location).

A third radar is operated by the Royal Air Force (RAF) with Air Force liaisons on site at RAF Fylingdales, United Kingdom (three radar faces). The MDA and Air Force Space Command are also upgrading the Early Warning Radars in Clear Air Force Station, Alaska, and Cape Cod Air Force Station, Massachusetts (projected fielding for both is FY18).
  - The Sea-Based X-band (SBX) radar is a mobile, phased array radar operated by the MDA and located aboard a twin-hulled, semi-submersible, self-propelled, ocean-going platform.
  - The AN/TPY-2 (FBM) radar is a transportable, single-face, X-band phased array radar commanded and tasked by the C2BMC, and located at sites in Japan, Israel, Turkey, and the U.S. Central Command (USCENTCOM) area of responsibility.
  - The Space Based Infrared System (SBIRS) is a satellite constellation of infrared sensors operated by the Air Force with an external interface to the BMDS located at Buckley AFB, Colorado.
  - The list of BMDS sensors also includes the Aegis AN/SPY-1 radar. See the Aegis Ballistic Missile Defense (BMD) article (page 291) for reporting on this sensor.
- The C2BMC system is a Combatant Command interface to the BMDS and the integrating element within the BMDS. More than 70 C2BMC workstations are fielded at U.S. Strategic Command, U.S. Northern Command (USNORTHCOM), U.S. European Command (USEUCOM), U.S. Pacific Command (USPACOM), and USCENTCOM; numerous Army Air and Missile Defense Commands; Air and Space Operations Centers; Maritime Operation Centers; and other supporting warfighter organizations.
  - The current C2BMC provides Combatant Commands and other senior national leaders with situational awareness of BMDS status, system coverage, and ballistic missile tracks by displaying selective BMDS data for strategic/national missile defense and for theater/regional missile defense. The C2BMC does this by utilizing multiple message formats and diverse terrestrial and satellite communications paths.
  - The C2BMC also provides a consolidated upper echelon BMD mission plan at the Combatant Command and component level. BMDS elements (Aegis BMD, Ground-based Midcourse Defense (GMD), Patriot, and Terminal High-Altitude Area Defense (THAAD)) use their own command and control battle management systems and mission-planning tools for stand-alone engagements.
  - The current C2BMC S6.4 suite provides command and control for the AN/TPY-2 (FBM) radar as well as track reporting to support weapon system cueing and engagement operations.
  - BOA is a system within the C2BMC enterprise that receives raw infrared sensor information on boosting and midcourse ballistic objects and feeds that track data to C2BMC (S8.2-1 and beyond) for use in cueing BMDS sensors and weapon systems, and for situational awareness.
  - Using the BMDS Communications Network, the C2BMC forwards AN/TPY-2 (FBM) and AN/SPY-1 tracks to GMD. C2BMC uses the Tactical Digital Information Link-Joint message formats to send C2BMC system track data to Aegis BMD, THAAD, Patriot, and coalition systems for sensor cueing and engagement support.

Mission
- Combatant Commands intend to integrate the BMDS sensors and C2BMC with other BMDS elements to intercept ballistic missile threats that target the United States and U.S. allies.
  - Combatant Commands use the BMDS sensors to detect, track, and classify/discriminate ballistic missile threats.
  - Combatant Commands use C2BMC for deliberate and dynamic planning; situational awareness; track management; AN/TPY-2 (FBM) sensor management and control; engagement support and monitoring, data exchange between C2BMC and BMDS elements; and network management.

Major Contractors
- COBRA DANE Radar: Raytheon Company, Intelligence, Information, and Services – Dulles, Virginia
- UEWRs: Raytheon Company (Prime), Integrated Defense Systems – Tewksbury, Massachusetts; Harris Corporation/Exelis (Sustainment) – Colorado Springs, Colorado
- SBX and AN/TPY-2 (FBM) Radars: Raytheon Company, Integrated Defense Systems – Tewksbury, Massachusetts
- SBIRS: Lockheed Martin Corporation, Space Systems – Sunnyvale, California
- C2BMC: Lockheed Martin Corporation, Rotary and Mission Systems – Huntsville, Alabama, and Colorado Springs, Colorado
- BOA: Northrop Grumman Corporation – Boulder, Colorado; Colorado Springs, Colorado; and Azusa, California

---

Activity
- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- The MDA used the sensors and/or the command and control architecture in six tests and five targets-of-opportunity data collections. The MDA conducted:
  - Two BMDS-level ground tests. The MDA conducted Ground Test, Integrated-07a (GTI-07a) in June 2017, assessing the BMDS Capability Increment 4 functionality improvements using strategic and theater/regional scenarios from USNORTHCOM's and USPACOM's

areas of responsibility. The MDA conducted Ground Test, Distributed-07a (GTD-07a) in September and October 2017. It complemented and included many of the same scenarios as GTI-07a, but in a distributed test environment. GTD ground tests use live operational networks, whereas GTI ground tests use laboratory-based networks.
  - One GMD flight test. The MDA conducted Flight Test, Ground-Based Interceptor-15 (FTG-15) in May 2017, intercepting an ICBM-class target for the first time. FTG-15 was also the first intercept using the Capability Enhancement-II Block 1 exo-atmospheric kill vehicle and the first demonstration of the three-stage Configuration 2 booster.
  - One Navy fleet exercise. In September and October 2017, the multi-event Formidable Shield-17 (FS-17) Navy fleet exercise was conducted. The firing (or simulated firing) ships prosecuted remote engagements using data from NATO maritime assets, transmitted by C2BMC through a NATO communications gateway.
  - Two THAAD flight tests. The MDA conducted Flight Test, THAAD-18 (FTT-18) in July 2017. It was the first THAAD intercept of an intermediate-range ballistic missile target. The MDA conducted Flight Experiment, THAAD-01 (FET-01) in July 2017 to examine the THAAD element response to target dynamics. During both of these tests, the MDA used C2BMC S8.2-1 and BOA 5.1 for the first time.
  - Radars from the sensor architecture collected data from five ballistic missile targets-of-opportunity during 2016.
- ARL/SLAD, in support of the MDA, conducted three cybersecurity events:
  - In July 2017, ARL/SLAD evaluated USNORTHCOM's C2BMC S8.2-1.1, the C2BMC portion of the Cheyenne Mountain Management Node, the C2BMC Distributed Training System, and BOA 5.1 in a CVPA.
  - In September 2017, ARL/SLAD conducted additional limited cooperative cybersecurity assessments on USNORTHCOM's C2BMC S8.2-1.1, BOA 5.1, and the AN/TPY-2 (FBM) radar CX2.1.1 configured with the Superdome computer processor. The C2BMC Program Office used this event to collect data on a prototype net defense tool that it intends to integrate into the C2BMC baseline.
  - In October 2017, ARL/SLAD conducted a limited CVPA of the X-band radar (XBR) portion of the SBX.
- The Air Force conducted four ICBM reliability and sustainment flight tests using the MDA sensors and/or the command and control architecture. The Air Force conducted Glory Trip-221 (GT 221; February 2017), GT-220 (April 2017), GT-222 (May 2017), and GT-223 (August 2017) tests of the Minuteman III ICBM. For these four tests, the MDA provided the Space Tracking Surveillance System (GT 221), Enterprise Sensors Lab (GT 220 – GT 223), Mount Wilson Aerospace Facility for Integrated Optical Test (GT 220 – GT 223), Discrimination Sensor Technology (GT 221), Overhead Sensors (GT 220 – GT 223), and SBIRS (GT 221).
- The MDA completed the Sensor Analysis of Alternatives and presented the findings to the Missile Defense Executive Board in October 2016.
- The MDA initiated the defense of Hawaii radar program. Over FY17, initial analytical studies were completed and site surveys conducted.
- The MDA completed the Critical Design Review for the Long-Range Discrimination Radar in September 2017.
- The MDA integrated and accredited for developmental test C2BMC's Overhead Persistent Infrared (OPIR) simulation tools, Future OPIR External Simulation (FOXSIM) and On-Line Generic Adaptive Simulator (OLGASIM), to provide modeling and simulation representation of future sensor inputs to BOA 5.1. The BMDS Operational Test Agency team accredited the models for operational assessment.

Assessment

- During FTG-15, the GMD element performed nominally. The C2BMC S6.4-3.0 element forwarded SBIRS and AN/TPY-2 (FBM) CX-2.1 radar data to GMD Fire Control (GFC). GFC cued the SBX 3.3.1 radar. Based on correct SBX discrimination data, the GFC commanded a Mode 2 engagement. The Capability Enhancement-II Block 1 exo-atmospheric kill vehicle intercepted and negated the ICBM-representative reentry vehicle.
- ARL/SLAD's FY17 cybersecurity assessments of C2BMC, BOA, AN/TPY-2(FBM) radar, and XBR were the MDA's initial attempt at independent operational cybersecurity assessment to identify vulnerabilities on these systems. Real-world operational needs and lack of adherence to the test plans limited CVPA data collection during the September 2017 cybersecurity event.
- The cybersecurity assessments conducted in FY17 identified cybersecurity vulnerabilities; however, additional less restrictive testing (e.g., minimize "blacklisting;" full CVPA and AA team access to all systems and sub-systems that may introduce vulnerabilities to the BMDS architecture) is required to inform cybersecurity efforts, improve net defense, and characterize BMDS capability in a cyber-contested environment. This testing should include CVPAs and AAs that address previous CVPA limitations, other instantiations of C2BMC and AN/TPY-2, and other non-MDA sensors that are critical to BMDS capability (i.e., UEWRs and COBRA DANE).
- The MDA and the Army continue working to achieve Full Materiel Release of the AN/TPY-2 (FBM) radar. Of the 25 Initial Materiel Release conditions for software version CX-1.2.3_18, which includes 2 that the Army transferred from the CX-1.3.7 materiel release, the Army closed 5 prior to FY17 and an additional 4 in FY17. Further, the Army has drafted eight additional materiel release conditions for software version CX-2.1.0. The Army expects to close all remaining open materiel release conditions by 2019.
- The Army continues to transition AN/TPY-2 (FBM) radar operations and maintenance from contractor logistics support

to organic soldier operations and maintenance. Soldiers are now responsible for activities at two of the five deployed radars. Operator training and IETMs continue to be deficient.
- During FY17 ground testing, the MDA exercised new capabilities and assessed BMDS interoperability using hardware-in-the-loop simulation and operational assets communicating over operational networks (GTI-07a and GTD-07a, respectively). Test data informed enhanced homeland defense and theater/regional functionality development for BMDS Capability Increment 4 defined as:
  - BOA data integrated into the BMDS and providing X-band cues.
  - Ballistic missile defense planning, SBIRS interface change, and communications enhancements.
  - Performance improvements and Ground-Based Interceptor reliability upgrade.
  - Implement updated cybersecurity protections.
- During FTT-18 and FET-01, BOA 5.1 acquired and tracked the target, and transmitted the data to C2BMC S8.2-1 per the architecture design. C2BMC S8.2-1 demonstrated nominal situational awareness and track processing.
- During ballistic missile targets-of-opportunity in 2016, radars from the sensor architecture acquired, tracked, and reported track data to the GFC component. Truth data were also collected and the MDA's post-event data analysis confirmed that the overall system performed as designed.
- The MDA successfully conducted BMDS-associated operations on the Minuteman III target in all four FY17 Glory Trips. The MDA uses Glory Trips to reduce risk for future BMDS tests, exercise developmental capabilities, collect data for algorithm development and analysis, and to collect data for Critical Engagement Conditions and Empirical Measurement Events for model anchoring.
- The MDA demonstrated C2BMC S6.4 threat assessment, threat evaluation, sensor resource management, sensor track data processing, track reporting, target selection, sensor/weapon access determination, and engagement monitoring during flight tests, as well as during real-world ballistic missile targets-of-opportunity events. This software version does not enable automatic engagement coordination among different BMDS elements (e.g. THAAD and Aegis BMD).
- The MDA began ground testing of C2BMC S8.2, which will ultimately implement automatic engagement coordination, which the MDA currently plans for 2023. The MDA implemented a redundant unified client within C2BMC S8.2 that replaced the Global Engagement Manager and Combatant Command suites implemented in C2BMC S6.4. The MDA is also implementing geographic C2BMC redundancy. The MDA plans to field C2BMC S8.2 to USNORTHCOM and USPACOM in FY18 followed by fielding to USEUCOM and USCENTCOM in FY19.

Recommendations
- Status of Previous Recommendations. The MDA has addressed previous sensors/command and control recommendations with three exceptions, two of which are classified. The MDA should:
  1. In conjunction with the Army, update the AN/TPY-2 (FBM) radar IETMs and improve radar operator training.
- FY17 Recommendations. The MDA should:
  1. Demonstrate C2BMC S8.2 internal failover capability (e.g., unified client string A to string B) and external geographic failover capability (e.g., USNORTHCOM to USPACOM) to assess C2BMC S8.2's ability to continue operations during an active engagement period.
  2. Develop a comprehensive operational cybersecurity test and evaluation strategy for each BMDS sensor and the C2BMC. This strategy should be included in the Integrated Master Test Plan and reflect the following:
     - Planned CVPAs of SBX and the AN/TPY-2 (FBM) radar configured with the x86 computer processor in FY18.
     - Planned AAs of the SBX; AN/TPY-2 (FBM) radar configured with the x86 computer processor; AN/TPY-2 (FBM) radar configured with the Superdome computer processor; C2BMC S6.4, C2BMC S8.2, and BOA in operational environments.
     - Coordination with the U.S. Air Force to conduct operational cybersecurity testing of the UEWRs and COBRA DANE radar.
     - Sufficient time to plan cybersecurity events, to ensure required resources are available to support adequate test conduct and enable timely resolution of key issues (e.g., sufficient detail in the test conduct, data management, analysis, and evaluation plans).
  3. Leverage and coordinate with ongoing cybersecurity assessment efforts to conduct operational cybersecurity assessments (CVPAs and AAs) of critical BMDS assets, in order to maximize efficiency and reduce duplication of activity across the DOD. These efforts include the DOT&E Cybersecurity Assessment Program, the Department's ongoing Persistent Cyber Operations, and the USD(AT&L) cybersecurity assessment efforts required by section 1647 of the National Defense Authorization Act for FY16.

Ground-Based Midcourse Defense (GMD)

Executive Summary

- The Ground-based Midcourse Defense (GMD) element has demonstrated capability to defend the U.S. Homeland from a small number of intermediate-range ballistic missile (IRBM) or intercontinental ballistic missile (ICBM) threats with simple countermeasures when the Homeland Defense Ballistic Missile Defense System (BMDS) employs its full sensors/command and control architecture.
- The Missile Defense Agency (MDA) intercepted an ICBM-class target for the first time during Flight Test, Ground-Based Interceptor-15 (FTG-15). FTG-15 was also the first intercept using the Capability Enhancement-II (CE-II) Block 1 Exo-atmospheric Kill Vehicle (EKV) and the first demonstration of the three-stage Configuration 2 booster. The GMD element performed nominally.
- The Army Research Laboratory Survivability/Lethality Analysis Directorate (ARL/SLAD) conducted a limited Cooperative Vulnerability and Penetration Assessment (CVPA) to assess the cybersecurity of the FTG-15 GMD test architecture. Although testing identified some cyber vulnerabilities, the minimal test scope and the test conduct restrictions prevented an assessment of the overall cybersecurity posture of GMD assets. The MDA has not conducted Adversarial Assessments (AAs) on any GMD systems in the BMDS architecture, which are necessary to support a cybersecurity survivability assessment.
- Quantitative evaluation of GMD operational effectiveness (including system performance, reliability, and lethality) requires extensive ground testing with independently accredited modeling and simulation (M&S), which the MDA has not yet conducted.
- The MDA:
  - Fielded updated GMD Fire Control (GFC) and EKV software.
  - Refurbished Missile Field 1 at Fort Greely, Alaska.
  - Completed the Redesigned Kill Vehicle (RKV) Preliminary Design Review.
  - Emplaced five CE-II Block 1 EKVs with three-stage Configuration 2 boosters, and plans to emplace three more by the end of 2017.
- The MDA conducted Ground Test Integrated-07a (GTI-07a) and Ground Test Distributed (GTD-07a), using strategic and theater/regional scenarios from the U.S. Northern Command (USNORTHCOM) and U.S. Pacific Command (USPACOM) areas of responsibility.

System

- GMD counters IRBM and ICBM threats to the U.S. Homeland. GMD consists of:
  - Ground-Based Interceptors (GBIs) at Fort Greely, Alaska, and Vandenberg AFB, California.

  - GMD ground system, including GFC nodes at Schriever AFB, Colorado, and Fort Greely, Alaska; Command Launch Equipment at Vandenberg AFB, California, and Fort Greely, Alaska; and In-Flight Interceptor Communication System Data Terminals at Vandenberg AFB, California; Fort Greely, Alaska; Eareckson Air Station, Alaska; and Fort Drum, New York.
  - GMD secure data and voice communications system, including long-haul communications using the Defense Satellite Communication System, commercial satellite communications, and fiber-optic cable (both terrestrial and submarine).
  - External interfaces that connect to Aegis Ballistic Missile Defense ships; North American Aerospace Defense/USNORTHCOM Command Center; Command and Control, Battle Management, and Communications system at Schriever AFB, Colorado, and Joint Base Pearl Harbor-Hickman, Hawaii; Space Based Infrared System at Buckley AFB, Colorado; and AN/TPY-2 Forward-Based Mode radars at Japan Air Self Defense Force bases in Shariki and Kyoga-Misaki, Japan.

Mission

Military operators from the U.S. Army Space and Missile Defense Command/Army Forces Strategic Command (the Army component to U.S. Strategic Command) will use the GMD system to defend the U.S. Homeland against IRBM and ICBM attacks using the GBI to defeat threat missiles during the midcourse segment of flight.

Major Contractors
- GMD Prime: The Boeing Company, Network and Space Systems – Huntsville, Alabama
- Boost Vehicle: Orbital ATK, Missile Defense Systems – Chandler, Arizona
- Kill Vehicle: Raytheon Company, Missile Systems – Tucson, Arizona
- Fire Control and Communications: Northrop Grumman Corporation, Information Systems – Huntsville, Alabama

---

Activity
- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- The MDA fielded GFC 6B3.1 software in January 2017 to mitigate obsolescence and to enhance cybersecurity.
- The MDA fielded CE-II EKV software version 10 to the operational baseline in March 2017.
- The MDA completed the RKV Preliminary Design Review in March 2017.
- The MDA conducted FTG-15 in May 2017, intercepting an ICBM-class target for the first time. FTG-15 was also the first intercept using the CE-II Block 1 EKV and the first demonstration of the three-stage Configuration 2 booster.
- The MDA conducted GTI-07a in June 2017, assessing the BMDS Capability Increment 4 functionality improvements using strategic and theater/regional scenarios from the USNORTHCOM and USPACOM areas of responsibility.
- ARL/SLAD, in support of the MDA, conducted a limited CVPA of the GMD FTG-15 test architecture in June 2017.
- The MDA completed the refurbishment of Missile Field 1 at Fort Greely, Alaska, in September 2017.
- The MDA conducted GTD-07a in September and October 2017. It executed many of the same scenarios as GTI-07a, but in a distributed test environment. GTD ground tests use live operational networks, whereas GTI ground tests use laboratory-based networks.
- As of the end of FY17, the MDA has emplaced five CE-II Block 1 EKVs with three-stage Configuration 2 boosters with plans to emplace three more by the end of calendar year 2017.
- The MDA conducted minimal RKV lethality activities in FY17 due to a $55 Million mid-year congressional budget reduction to the RKV program. The MDA reduced the RKV lethality effort by $8.15 Million (94 percent). Test planning and design efforts for light gas gun and/or sled tests were suspended.

Assessment
- GMD has demonstrated capability to defend the U.S. Homeland from a small number of IRBM or ICBM threats with simple countermeasures when the Homeland Defense BMDS employs its full sensors/command and control architecture.
- During FTG-15, the GMD element performed without fault. The three-stage Configuration 2 GBI booster flew as designed and delivered the EKV to the proper geographic position with the desired velocity. The CE-II Block 1 EKV intercepted and negated the ICBM-representative reentry vehicle. Guidance systems throughout the engagement functioned nominally.
- The limited CVPA conducted by ARL/SLAD was a notable first attempt at an independent cybersecurity assessment. Though the assessment identified vulnerabilities, the test was insufficient to inform a cybersecurity evaluation for the operational GMD system. The MDA restricted the assessment to only portions of the GMD architecture associated with FTG-15 located at the Missile Defense Integration and Operations Center at Schriever AFB, Colorado, and Vandenberg AFB, California. The assessment did not include the entire operational environment.
  - The tested components were intentionally isolated from four GMD sites, nine supporting sensors, and the GBI silos and boosters/EKVs.
  - ARL/SLAD could not complete the outsider assessment in accordance with the CVPA test plan due to Temporary Design Departure (TDD) requirements.
  - Within the FTG-15 architecture, the MDA "blacklisted" (i.e., denied access to) critical parts of GMD networks and systems at all locations, limiting an end-to-end assessment. DOT&E and ARL/SLAD were unaware of the blacklist until the start of testing. To mitigate this problem in other FY17 CVPAs, the MDA began to include blacklists as part of the test plans.
  - The MDA did not provide ARL/SLAD and DOT&E sufficient system and network documentation to adequately plan and prepare for the assessment.
- The MDA has not yet conducted a cybersecurity AA of GMD.
- During FY17 ground testing, the MDA exercised new capabilities and assessed BMDS interoperability using hardware-in-the-loop simulation in GTI-07a and operational assets communicating over operational networks in GTD-07a. Test data informed enhanced homeland defense and theater/regional functionality development for BMDS Capability Increment 4, which is defined as:
  - BMDS Overhead Persistent Infrared Architecture data integrated into the BMDS and providing X-band cues.
  - Ballistic missile defense planning, Space Based Infrared System interface change, and communications enhancements.
  - Performance improvements and GBI reliability upgrade.
  - Implementation of updated cybersecurity protections.
- While the MDA made some progress during FY17, quantitative evaluation of GMD operational effectiveness requires extensive ground testing with independently accredited M&S, which the MDA has yet to perform. Due to the lack of required data, the MDA lacks independently

accredited M&S to support an assessment of GMD performance, reliability, and lethality.

Recommendations

- Status of Previous Recommendations. The MDA has addressed previous GMD recommendations with the exception of three recommendations, one of which is classified. The MDA should:
  1. Increase emphasis on GMD survivability testing, including cybersecurity. The MDA should plan tests, demonstrations, and exercises to acquire additional survivability data and include them in the BMDS Integrated Master Test Plan.
  2. Accelerate efforts to accredit M&S for performance assessment supporting GMD OT&E, including RKV and countermeasure performance.
- FY17 Recommendation. The MDA should:
  1. Provide adequate funding for and accelerate development of a lethality T&E strategy for the RKV against updated threats and engagement conditions to support performance assessments and M&S tool accreditation.
  2. Develop a comprehensive operational cybersecurity test and evaluation strategy for GMD assets in the BMDS architecture. This strategy should be included in the Integrated Master Test Plan and reflect the following:
     - Planned CVPAs and AAs of existing operational GMD assets and of new increment capabilities, in order to properly inform operational risk assessments; mitigate critical cybersecurity vulnerabilities; improve network defense; and make BMDS systems and networks more secure against cyber adversaries.
     - Elimination of previous practices of port isolation, blacklisting, and restricting assessments for CVPAs and AAs of GMD assets. Discontinuing these practices will enable an adequate evaluation of GMD cybersecurity posture.
     - Sufficient time to plan cybersecurity events, to ensure required resources are available to support adequate test conduct and enable timely resolution of key issues (e.g., inadequate detail in the test conduct, data management, analysis, and evaluation plans).
  3. Leverage and coordinate with ongoing cybersecurity assessment efforts to conduct operational cybersecurity assessments (CVPAs and AAs) in order to maximize efficiency and reduce duplication of activity across the DOD. These efforts include the DOT&E Cybersecurity Assessment Program, the Department's ongoing Persistent Cyber Operations, and the USD(AT&L) cybersecurity assessment efforts required by section 1647 of the National Defense Authorization Act for FY16.

Aegis Ballistic Missile Defense (Aegis BMD)

Executive Summary

- The Missile Defense Agency (MDA) conducted five Aegis Ballistic Missile Defense (BMD) intercept flight tests in FY/CY17. Aegis BMD successfully engaged four of the five ballistic missile targets in those tests. During one of these tests, Aegis BMD successfully engaged a complex ballistic missile for the first time. Such missiles pose a challenge in discriminating the target reentry vehicle from other objects. In another test, Aegis BMD intercepted a simple ballistic missile target with a Standard Missile-3 (SM-3) Block IIA missile for the first time.
- Aegis BMD participated in six non-intercept flight test events in FY/CY17 with simulated Standard Missile variants engaging live targets and a live SM-6 Dual I missile engaging a simulated target.
- Aegis BMD provided hardware-in-the-loop (HWIL) representations for two Ballistic Missile Defense System (BMDS) ground tests that provided information on Aegis BMD interoperability and functionality in various regional/theater and strategic scenarios.
- The MDA delivered high-fidelity digital modeling and simulation (M&S) runs-for-the-record results in FY17 to support assessments of Aegis Ashore (Baseline 9.B1) and Aegis Baseline 9.C1 Sea-Based Terminal (SBT) performance for select scenarios.
- DOT&E has lower confidence in SM-3 missile reliability due to recent in-flight failures, coupled with MDA shortfalls in simulating the in-flight environment in its SM-3 ground test program, addressing failures and anomalies identified during flight testing, and implementing a rigorous configuration management and control process for SM-3 production.

System

- Aegis BMD is a sea- and land-based missile defense system that employs the multi-mission shipboard Aegis Weapon System, with improved radar and new missile capabilities to engage ballistic missile threats. The Aegis BMD includes:
  - Computer program modifications to all Aegis Weapon System elements, including the AN/SPY-1 radar, to support multiple BMDS mission capabilities including long-range surveillance and track, engagement support surveillance and track, and organic engagement with the SM-3, SM-6, or modified SM-2 Block IV missile variants against ballistic missiles of all ranges
  - A modified Aegis Vertical Launching System, which stores and fires SM-3 Block IA, Block IB, and Block IIA guided missiles, modified SM-2 Block IV guided missiles, and SM-6 Dual I guided missiles
  - SM-3 Block IA, Block IB, and Block IIA guided missiles that use maneuverable kinetic warheads to accomplish midcourse engagements of short-range ballistic missiles (SRBMs), medium-range ballistic missiles (MRBMs), and intermediate-range ballistic missiles (IRBMs)
  - Modified SM-2 Block IV guided missiles that provide SBT capability against SRBMs and MRBMs
  - SM-6 Dual I guided missiles that provide SBT capability against SRBMs and MRBMs in their terminal phase of flight, anti-ship cruise missiles, and all types of aircraft

Aegis Cruiser

Aegis Ashore and Vertical Launch System

- Aegis BMD ships and Aegis Ashore are designed to conduct missile defense operations, send/receive cues to/from other BMDS sensors through tactical datalinks, and conduct engagements using remote track data from BMDS sensors. Aegis BMD ships also are designed to conduct autonomous missile defense operations.
- Aegis Ashore (Baseline 9.B1) is a land-based version of Aegis BMD, with an AN/SPY-1 radar and Vertical Launching System to enable engagements against MRBMs and IRBMs with SM-3 guided missiles. The first Aegis Ashore site in Romania is the land-based component of the second phase of the European Phased-Adaptive Approach (EPAA) for the defense of Europe.
- The Aegis BMD weapon system configurations currently deployed or under development are summarized below.

WEAPON SYSTEM	AEGIS BASELINE (BL) NOMENCLATURE	PLATFORM	MISSILES
Aegis BMD 5.1	BL 9.C2	Guided-Missile Destroyers (DDGs)	SM-3 Blocks IA, IB, and IIA; SM-6 Dual I and Dual II
	BL 9.B2	Aegis Ashore	SM-3 Blocks IA, IB, and IIA
Aegis BMD 5.0 (Capability Upgrade)	BL 9.C1	DDGs	SM-3 Blocks IA and IB; SM-6 Dual I and Dual II; and SM-2 Block IV
	BL 9.B1	Aegis Ashore	SM-3 Blocks IA and IB
Aegis BMD 4.1	Not Applicable	DDGs and Guided-Missile Cruisers (CGs)	SM-3 Blocks IA and IB; SM-6 Dual I
Aegis BMD 4.0.3			SM-3 Blocks IA and IB
Aegis BMD 3.6.3			SM-3 Blocks IA and IB; SM-2 Block IV

Mission

The Navy can accomplish three missile defense-related missions using Aegis BMD:

- Defend deployed forces and allies from short- to intermediate-range theater ballistic missile threats
- Provide forward-deployed radar capabilities to enhance defense against ballistic missile threats of all ranges by sending cues or target track data to other BMDS elements
- Provide ballistic missile threat data to the Command and Control, Battle Management, and Communications (C2BMC) system for dissemination to Combatant Commanders' headquarters to ensure situational awareness

Major Contractors

- Aegis BMD Weapon System: Lockheed Martin Corporation, Rotary and Mission Systems – Moorestown, New Jersey
- AN/SPY-1 Radar: Lockheed Martin Corporation, Rotary and Mission Systems – Moorestown, New Jersey
- SM-3, SM-2 Block IV, and SM-6 Missiles: Raytheon Company, Missile Systems – Tucson, Arizona

---

Activity

- The MDA conducted all FY/CY17 testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- The MDA conducted five Aegis BMD intercept flight tests in FY/CY17. Overall, Aegis BMD successfully engaged four of the five ballistic missile targets in those tests:
  - In December 2016 during Flight Test Standard Missile-27 (FTM-27) Event 1, an Aegis Baseline 9.C1 destroyer engaged a complex MRBM target with a salvo of two SM-6 Dual I missiles. FTM-27 Event 1 was the first demonstration of Aegis BMD SBT capability against complex ballistic missile targets.
  - In February 2017 during SM-3 Block IIA Cooperative Development Project Flight Test Standard Missile-01 (SFTM-01), an Aegis Baseline 9.C2 destroyer intercepted a simple-separating MRBM target with an SM-3 Block IIA missile. This was the first intercept with the SM-3 Block IIA missile, which the United States and Japan are developing cooperatively to defeat MRBMs and IRBMs.
  - In June 2017 during SFTM-02, an Aegis Baseline 9.C2 destroyer attempted to intercept an MRBM target with an SM-3 Block IIA missile. The destroyer detected, tracked, and engaged the target with an SM-3 Block IIA missile, although SFTM-02 did not achieve the planned intercept. Aegis Ashore received track data from the Aegis Baseline 9.C2 destroyer and conducted the first successful simulated engagement on the MRBM remote track.
  - In August 2017 during FTM-27 Event 2, an Aegis Baseline 9.C1 destroyer engaged a complex MRBM target with a salvo of two SM-6 Dual I missiles. The test, which was a follow-on from FTM-27 Event 1, further demonstrated aspects of the Baseline 9.C1 SBT engagement capability.
  - In October 2017 during the fourth event of the multi-event Formidable Shield-17 (FS-17) Navy fleet exercise, an Aegis BMD 4.0.3 destroyer engaged and intercepted an MRBM target with a production-representative SM-3 Block IB Threat Update (TU) missile. As part of the scenario, some of the participating NATO naval assets intercepted three anti-air warfare (AAW) targets as part of a complex multinational integrated air and missile defense (IAMD) exercise that validated the NATO Smart Defense concept. This event satisfied one of the requirements for

a Full-Rate Production decision for the SM-3 Block IB missile.

- Aegis BMD participated in six non-intercept flight test events in FY/CY17 with simulated Standard Missile variants engaging live targets and a live SM-6 Dual I missile engaging a simulated target:
  - In March 2017 during FTX-30, an Aegis Baseline 9.C2 ship operating in IAMD mode conducted a simulated SM-3 Block IIA engagement of a live simple-separating SRBM target and SM-2 missile engagements against multiple subsonic and supersonic anti-ship cruise missiles.
  - In July 2017 during FTX-32, Aegis Ashore, configured with Baseline 9.B2, detected, tracked, and engaged a complex MRBM target with associated objects with a simulated SM-3 Block IIA missile. Aegis Ashore also reported track data via Link 16 to an Aegis BMD laboratory conducting a simulated engagement on the remote track.
  - In September 2017 during FTX-31, an Aegis Baseline 9.C1 ship and Aegis Ashore detected and tracked a complex-separating SRBM target with associated objects. The ship conducted a simulated engagement against the SRBM and two AAW targets. Aegis Ashore, configured with Baseline 9.B2, reported these track data via Link 16 to an Aegis BMD laboratory, which conducted a simulated engage on remote engagement against the SRBM remote track using a simulated SM-3 Block IIA missile.
  - In September and October 2017 during Events 1 and 2 of FS-17, Aegis BMD 4.0.3 and Aegis Baseline 9.C1 destroyers conducted simulated engagements of ballistic missile targets using remote data. NATO maritime assets transmitted the remote track data through C2BMC and a NATO communications gateway. In each event, NATO maritime assets, not participating as BMD assets, fired simulated or live missiles and engaged four AAW targets.
  - In October 2017 during Standard Missile Controlled Test Vehicle-03 (SM CTV-03), an Aegis BMD 4.1 destroyer detected, tracked, and engaged a simulated ballistic missile target with a live SM-6 Dual I missile. The missile firing supports certification of the Aegis BMD 4.1 upgrade to include hosting the SBT capability into Aegis BMD 4.0.
- Aegis BMD provided HWIL representations for two BMDS ground tests that provided information on Aegis BMD interoperability and functionality in various regional/theater and strategic scenarios:
  - Ground Test Integrated-07a (GTI-07a) in June 2017 explored defense of U.S. Pacific Command and homeland defense scenarios in a HWIL environment. Aegis Baseline 9.C1 and Aegis BMD 4.1, 4.0.3, and 3.6.3 participated in the test as firing assets or long-range surveillance and tracking support ships.
  - Ground Test Distributed-07a (GTD-07a) in September and October 2017 examined BMDS defense capabilities and interoperability in U.S. Pacific Command and homeland defense scenarios using operational assets and communications in a distributed environment. Aegis Baselines 9.C1 and 9.C2 and Aegis BMD versions 4.1, 4.0.3, and 3.6.3 participated as firing assets and long-range surveillance and tracking units.
- The MDA delivered high-fidelity digital M&S runs-for-the-record results in FY17 to support assessments of Aegis Ashore and Aegis Baseline 9.C1 SBT performance for select scenarios. The Navy Commander, Operational Test and Evaluation Force (COMOPTEVFOR) accredited the SBT M&S run set for performance in May 2017. COMOPTEVFOR's accreditation of the Aegis Ashore M&S run set is still in progress.

Assessment

- With one exception, the MDA completed its planned flight testing with the SM-3 Block IB TU missile as documented in the Integrated Master Test Plan. The lone exception is FTM-24, a planned engagement against a complex MRBM target that the MDA delayed until FY20. The legacy SM-3 Block IB missile (i.e., without the TU) completed its flight testing in November 2014.
- DOT&E has lower confidence in SM-3 missile reliability due to recent in-flight failures, coupled with MDA shortfalls in simulating the in-flight environment in its SM-3 ground test program, addressing failures and anomalies identified during flight testing; and implementing a rigorous configuration management and control process for SM-3 production.
- The MDA missile ground test program may not adequately simulate the in-flight environment:
  - Contractors introduced a software design flaw into the SM-3 Block IB that was not present in the SM-3 Block IA. The MDA did not discover this flaw during ground testing, but instead discovered this flaw during a failed SM CTV-01 launch in 2016 and subsequent investigation after the EPAA Phase 2 capability declaration.
  - During the course of routine production testing, Raytheon discovered a rare condition that could cause the SM-3 Block IB Kinetic Warhead Guidance Unit Guidance Unit to fail. The MDA halted deliveries of SM-3 Block IB missiles for approximately 5 months while it identified a root cause. The MDA corrected the problem with Block IB software build 6.404, released in August 2016.
  - The SM-3 Block IB electromagnetic interference test and subsequent ground tests have not been compliant with Military Standard 461F, did not evaluate the self-compatibility of SM-3 Block IB electrical and software systems, and did not reflect in-flight electrical grounding, including electrical isolation and grounding shifts due to stage separations.
- The MDA did not thoroughly address, prior to flight testing, the software flaws that were present during recent flight testing:
  - The MDA did not correct the software design flaw that led to the SM CTV-01 failure before conducting the test. The MDA did not correct this problem before retesting the SM-3 during SM CTV-01a, but rather employed patches in a non-tactical software build to conduct the test.

  - Another software design flaw that caused kinetic warhead guidance units to be unresponsive was observed during contractor acceptance testing, but was not addressed prior to conducting five subsequent flight tests. Although the flaw did not adversely affect the flight tests, it represented an unmitigated risk to SM-3 reliability. The root cause of this flaw appears to be the MDA configuration and control process for SM-3, discussed below.
- The SM-3 program may need to improve configuration management and control:
  - The software design flaw that caused the failed SM CTV-01 launch was associated with a change to the software boot-up processes and not related to capability upgrades. The MDA's continuing efforts to improve the SM-3 Block IB could introduce other unintended consequences.
  - The MDA discovered the software design flaw associated with kinetic warhead guidance units (also discussed above) when it observed a performance difference in one of the circuit cards in 2016. This performance difference resulted from an approved manufacturing tooling change made in 2011. The MDA did not evaluate the potential for software performance problems caused by the tooling change until it conducted the SM CTV-01 failure investigation 5 years later.
  - The MDA did not discover an unapproved manufacturing process change in 2014 associated with wiring harnesses until one failed a hardware inspection over a year later. Failures associated with this change had the potential to prevent stage separation during SM-3 Block IB missile operational use.
- Results from flight testing, high-fidelity M&S, and HWIL and distributed ground testing demonstrate that Aegis BMD 4.0 and Baseline 9.1 firing assets can engage and intercept non-separating, simple-separating, and complex-separating ballistic missiles in the midcourse phase with SM-3 Block IB and Block IB TU guided missiles. However, flight testing and M&S are not yet sufficient to assess the full range of expected threat types, ground ranges, and raid sizes.
- The SM-3 Block IIA guided missile has flown in two developmental intercept flight tests, the first achieving a successful intercept. The second attempt, during SFTM-02, was unsuccessful because a sailor onboard the firing ship inadvertently pushed a button that caused the Aegis Weapon System to break engagement and initiate a message commanding the SM-3 Block IIA missile to destruct, destroying the missile in flight. DOT&E attributes this flight test failure to a design deficiency that allows an operator to break a ballistic missile engagement with the push of a button, without having to confirm the action. After conducting a Failure Review Board (FRB), the MDA provided a number of recommendations to the Navy that, if implemented, would preclude this type of failure from reoccurring.
- Two intercept flight tests in previous fiscal years and accredited high-fidelity M&S demonstrated that the Aegis Baseline 9.C1 system's SBT capability can successfully engage select SRBMs with SM-6 Dual I and SM-2 Block IV missiles. The SBT flight tests in FY17 demonstrated the ability to engage select MRBMs in the terminal phase of flight with SM-6 Dual I missiles, but the MDA has not yet performed M&S analyses with accredited models. The MDA plans to conduct M&S studies for select MRBM threats in FY19 and COMOPTEVFOR plans to accredit the M&S in the same timeframe.
- SM CTV-03 in October 2017 demonstrated the capability of the Aegis BMD 4.1 upgrade to fire an SM-6 Dual I missile. The BMD 4.1 build incorporates Baseline 9.C1 capabilities into the BMD 4.0 baseline.
- SM-6 Dual I and SM-2 Block IV missiles have been reliable in SBT flight tests. Missile reliability estimates for these missiles meet the specification, but not with statistical confidence due to the limited number of firings. To date, the MDA and Navy have conducted nine firings of the SM-6 Dual I or SM-6 Processor Replacement Program missile, and five firings of the SM-2 Block IV missile after modification for the SBT mission.
- Reliability, maintainability, availability, and supportability (RMA&S) data that the MDA collected during Aegis Baseline 9.1 BMD-related testing through FY17 show that the system's availability is less than desired due to large repair and logistics delay times. However, the DOT&E estimate of availability is consistent with the specification.
- The MDA demonstrated the Aegis Baseline 9.C1 system IAMD capabilities to a limited degree in flight testing. IAMD flight test engagements to date have included at most two cruise missile surrogates and a single ballistic missile target.
- MDA ground test events routinely demonstrated that inter-element coordination and interoperability need improvement to increase situational awareness. The tests also highlighted an Aegis BMD problem related to track management when it operates with other elements of the BMDS.
- The FS-17 fleet exercise demonstrated the ability of Aegis BMD 4.0.3 to interoperate with NATO partners over operational communication architectures during cruise missile and ballistic missile engagements, and to use remote data provided by NATO partners to prosecute remote engagements.

Recommendations

- Status of Previous Recommendations. The MDA:
  1. Partially addressed the second recommendation from FY13 to conduct operationally realistic testing that exercises Aegis BMD 4.0's improved engagement coordination with Terminal High-Altitude Area Defense (THAAD) and Patriot, when it conducted Flight Test Operational-02 (FTO-02) Event 2a (FY16) using an Aegis Baseline 9.C1 destroyer and THAAD firing assets. This flight test did not include Patriot. The MDA plans to include Patriot in FTO-03 Event 2 in FY18.
  2. Partially addressed the third recommendation from FY14 to ensure that the Aegis Baseline 9.C1 system conducts sufficient flight testing to allow for verification, validation, and accreditation (VV&A) of the M&S suite to cover the

full design to Aegis BMD battlespace. The MDA has collected sufficient flight test data to allow the BMDS Operational Test Agency (OTA) to accredit the high fidelity M&S suite over a portion of the engagement battlespace for Aegis Baseline 9.B1. The MDA and the BMDS OTA plan to conduct VV&A over the remaining battlespace for Baseline 9.C1 in FY18.

3. Has not addressed the second recommendation from FY15 to conduct stressing simultaneous air and ballistic missile defense engagements with the Aegis Baseline 9.C1 system operating in IAMD radar priority mode, with simultaneous engagement of multiple ballistic missile and anti-ship cruise missile threats.
4. Has not addressed the first recommendation from FY16 to conduct high-fidelity M&S runs-for-the-record for Aegis Baseline 9.B2 and 9.C2 to assess performance across the expected engagement battlespace in all Combatant Command areas of responsibility and develop an appropriate M&S VV&A plan to support that effort. The MDA developed a VV&A plan, but it will not perform Aegis Baseline 9.2 runs-for-the-record until FY20.
5. Has not addressed the second recommendation from FY16 to conduct a live-flight test demonstration of a fully remote engagement. The MDA plans to conduct this type of engagement in FY18 during FTM-29.
6. Partially addressed the third recommendation from FY16 to include BMDS OTA RMA&S data collectors in all flight test missions to improve the accuracy and statistical confidence of future suitability assessments. COMOPTEVFOR works with the program to have data collectors present at each flight test event. However, the MDA has not always funded data collectors for follow-on system-level flight tests like FTO-02 Event 1a and FTO-02 Event 2a.

- FY17 Recommendations. The MDA should:
  1. Conduct an in-depth review of SM-3 missile reliability to ensure ground testing is adequately simulating the in-flight environment as observed during recent test failures.
  2. Implement processes to fix failures and anomalies identified during SM-3 ground testing prior to flight testing.
  3. Ensure that SM-3 production configuration management, manufacturing control processes, and reporting requirements are adequate.
  4. Conduct high-fidelity M&S analysis of the performance of an Aegis Baseline 9 variant ship operating in IAMD radar priority mode when simultaneously engaging multiple ballistic missile and AAW threats.
  5. Work with the Navy to implement recommendations from the SFTM-02 FRB report, including the implementation of fail-safe software designs, to preclude future inadvertent operator actions from breaking engagements against hostile ballistic missile tracks.

Terminal High-Altitude Area Defense (THAAD)

Executive Summary

- The Missile Defense Agency (MDA) conducted two Terminal High-Altitude Area Defense (THAAD) flight tests in July 2017, intercepting two ballistic missile targets. In the first test, THAAD demonstrated the ability to defend territory in the U.S. Pacific Command (USPACOM) area of regard. In the second test, THAAD intercepted a complex, separating target in the endo-atmosphere.
- THAAD participated in two Ballistic Missile Defense System (BMDS) ground tests, providing information on THAAD interoperability and functionality within the BMDS for various regional/theater scenarios.
- The THAAD program continued work on resolving liens from the first Conditional Materiel Release in February 2012 and completed Urgent Materiel Releases for six Configuration 2 batteries with THAAD 2.8 software and Lot 4, 5, and 6 interceptors.
- Flight testing in FY17 demonstrated that THAAD training and documentation deficiencies worsened in FY17.
- The THAAD launcher and radar suffered reliability problems in flight tests. The launcher, particularly its 3-kilowatt generator, continued to experience failures and the radar experienced failures in the cooling electronic unit and prime power unit.

System

- THAAD complements the lower-tier Patriot system and the upper-tier Aegis Ballistic Missile Defense (BMD) system. It is designed to engage threat ballistic missiles in both the endo- and exo-atmosphere.
- THAAD consists of five major components:
  - Missiles
  - Launchers
  - AN/TPY-2 Radar (Terminal Mode)
  - THAAD Fire Control and Communications
  - THAAD Peculiar Support Equipment
- THAAD can accept target cues for acquisition from Aegis BMD, from other regional sensors, and through command and control systems.

Mission

The U.S. Northern Command, USPACOM, U.S. European Command, and U.S. Central Command intend to use THAAD to intercept short- to intermediate-range ballistic missile (IRBM) threats in their areas of responsibility. The U.S. Strategic Command deploys THAAD to protect critical assets worldwide from these same threats.

Major Contractors

- Prime: Lockheed Martin Corporation, Missiles and Fire Control – Dallas, Texas
- Interceptors: Lockheed Martin Corporation, Missiles and Fire Control – Troy, Alabama
- AN/TPY-2 Radar (Terminal Mode): Raytheon Company, Integrated Defense Systems – Tewksbury, Massachusetts

Activity

- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- Two BMDS ground tests using THAAD hardware-in-the-loop representations provided information on THAAD interoperability and functionality in various regional/theater scenarios:
  - In Ground Test Integrated-07a (GTI-07a) in June 2017, the MDA examined homeland and USPACOM defenses using THAAD 2.8 software.
  - In Ground Test Distributed-07a (GTD-07a) in September and October 2017, the MDA again examined homeland and USPACOM defenses using THAAD 2.8 software.

- The MDA conducted two flight tests in July 2017 at the Pacific Spaceport Complex Alaska on Kodiak Island and the surrounding broad ocean area.
  - Flight Test THAAD-18 (FTT-18), an integrated operational/developmental test, tested against a separating IRBM target.
    - THAAD engaged the target using a salvo of two THAAD interceptors. The THAAD battery consisted of THAAD Configuration 2 hardware, THAAD 2.8.1 software, two launchers equipped with Lot 4 and Fire Unit Fielding interceptors, THAAD Fire Control and Communications, and an AN/TPY-2 radar (Terminal Mode).
    - Additionally, the MDA and the BMDS Operational Test Agency (OTA) conducted BMD simulations with the deployable Simulation-Over-Live Driver (SOLD) to provide data supporting interoperability and effectiveness assessments.
  - Flight Experiment THAAD-01 (FET-01; formerly FTT-15), a developmental test, tested against a complex medium-range ballistic missile (MRBM) re-entry vehicle (RV) at a low endo-atmospheric altitude. This test used the same hardware and software configurations as in FTT-18.
- The THAAD program continued work on resolving liens from the first Conditional Materiel Release and completed Urgent Materiel Releases for six Configuration 2 batteries with THAAD 2.8 software and Lot 4, 5, and 6 interceptors.
- The FY17 Urgent Materiel Releases included the THAAD Portable Planner and THAAD Table Top Trainer to provide battle planning and training functions that would typically be conducted on the tactical system.

Assessment

- During GTI-07a and GTD-07a, the MDA demonstrated aspects of THAAD functionality in different theater scenarios to support the system-level assessment of enhanced homeland defense capabilities as part of BMDS Increment 4. The BMDS OTA reported several findings, consistent with findings from earlier ground tests that affect THAAD interoperability, track management, and radar functions.
- In FTT-18, the MDA demonstrated, for the first time, THAAD's capability to intercept an RV from a separating IRBM target. The MDA also demonstrated THAAD and the Command and Control, Battle Management, and Communications (C2BMC) Spiral 8.2.1-Link 16 functionality. This demonstration of C2BMC functionality did not involve other BMDS elements (such as Patriot or Aegis BMD) in theater.
- In FET-01, the MDA demonstrated THAAD's ability to discriminate and intercept an RV from a separating MRBM target with countermeasures at an endo-atmospheric altitude. The MDA will use these data to improve interceptor seeker algorithms and to validate modeling and simulation.
- Flight testing in FY17 demonstrated that THAAD training and documentation deficiencies worsened in FY17, despite the addition of the THAAD Table Top Trainer.
  - THAAD Service members continue to be resourced from the existing Patriot Soldier population. Many of the institutional courses provide insufficient time to effectively train operators for their missions, and the operators often encounter software mismatches between institutional training and operational environments.
  - The increasing use of Ground Maintenance Action Messages to address system workarounds or procedures not defined in the technical manuals complicates soldier, crew, and unit operations and training.
  - The BMDS OTA and Service members identified specific training and documentation gaps in communications capabilities, cybersecurity, and system capability understanding at both the institutional and unit levels.
  - The SOLD simulations provided valuable training opportunities during FTT-18 and FET-01; however, the simulation capability that SOLD can provide is not currently available to deployed units.
- The THAAD launcher and radar suffered reliability problems in flight tests. The launcher, particularly its 3-kilowatt generator, continued to experience the failures that were noted in 2015 during Flight Test Operational-02 (FTO-02) Event 2, FTO-02 Event 2a, and the Reliability Growth Test. The radar experienced failures in the cooling electronic unit and prime power unit.
- Problems previously discovered during testing, if not corrected, could adversely affect THAAD effectiveness, suitability, or survivability. The classified 2015 DOT&E assessment of the BMDS details these problems, which include:
  - Training and documentation are still immature.
  - Environmental testing revealed some deficiencies, which the MDA has not corrected.
  - Some specific aspects of discrimination and classification need improvement.
  - Survivability and cybersecurity shortfalls exist, which the MDA continues to assess and decide whether to fix, mitigate, transfer, or accept risks.
- The THAAD program continued to resolve problems noted in the Army's first Conditional Materiel Release in FY12.
  - In FY17, the Army closed the following three conditions: 1) provide a capability for soldiers to electronically transfer battle plans, 2) address a radar inertial measurement unit concern, and 3) address a radar alignment accuracy concern.
  - Of the original 39 conditions, 14 conditions remain open. The MDA and the Army continue to address materiel release conditions for the Institutional Conduct of Fire Trainer, THAAD Configuration 1 hardware, and THAAD 2.2.0 software that apply to THAAD Configuration 2 hardware and THAAD 2.8.2 software.

Recommendations

- Status of Previous Recommendations. The classified 2012 DOT&E THAAD and AN/TPY-2 Radar OT&E and LFT&E

report contained 7 recommendations in addition to the Army's 39 conditional materiel release conditions. The MDA should continue to address the two remaining classified recommendations (Effectiveness #2 and Effectiveness #5, which are not provided here due to classification levels). The MDA and the Army should:

1. Implement equipment redesigns and modifications identified during natural environment testing to prevent problems seen in testing (Suitability #11). Hardware modifications included in THAAD Configuration 2 have addressed some of these deficiencies. Additional ground testing with Configuration 2 (a standing FY14 recommendation) would also provide data to address this recommendation.
2. Conduct electronic warfare testing and analysis (Survivability #3). The MDA conducted preliminary testing during FY13, but it should conduct additional testing.
3. Conduct thorough end-to-end testing of THAAD Configuration 2. Configuration 2 incorporates considerable obsolescence redesigns of hardware and software. While the program partially addressed this FY14 recommendation, the MDA should continue to rigorously ground test the THAAD system to verify that these changes can withstand the range of environments and conditions required.
4. Prioritize flight and ground testing that involves THAAD and Patriot engagement coordination to determine if the information passed between THAAD and Patriot disrupts organic intercept capabilities or reduces interceptor wastage and threat missile leakage. The MDA and the Army are planning to conduct Flight Test Other-36 (FTX-36), a combined THAAD/Patriot test in FY18, to address this FY15 recommendation.
5. Conduct high-fidelity, end-to-end modeling and simulation runs against longer range threats including endgame and lethality analyses. The MDA and the BMDS OTA should continue working on this FY16 recommendation following model verification and validation using the FTT-18/FET-01 flight campaign data.

- FY17 Recommendations. The MDA and the Army should:
  1. Improve the effectiveness of THAAD training at the Fires Center of Excellence schoolhouse located in Fort Sill, Oklahoma, and in the units. This training should include network-capable virtual training aids in the institutional training base.
  2. Improve the quality and means by which they provide documentation to the Service members.

Live Fire Test and Evaluation

Live Fire Test and Evaluation

Live Fire Test and Evaluation (LFT&E)

Summary

- In FY17, DOT&E conducted LFT&E oversight for 124 acquisition programs, managed 3 LFT&E investment programs (Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME), Joint Aircraft Survivability Program (JASP), and Joint Live Fire (JLF)), and participated in 2 special interest programs (Warrior Injury Assessment Manikin (WIAMan) and Small Boat Shooters' Working Group).
- In support of a range of acquisition decisions and activities, DOT&E published three LFT&E reports and one combined OT&E and LFT&E report. The reports include recommendations to the Services to further improve the survivability of the subject systems for a range of operationally relevant scenarios in existing and expected combat environments.
- In support of the respective investment portfolio charters:
  - JASP funded 42 multi-year projects addressing aircraft survivability enhancement technologies and aircraft survivability evaluation tools needed to increase the ability of our aircraft to counter near-peer and second-tier threats, to reduce combat-induced aircrew injuries, and reduce combat-induced aircraft fires.
  - JLF funded 21 projects and delivered 16 reports. Focus areas for JLF included projects that either: 1) characterized new survivability issues; 2) characterized new lethality issues; 3) improved accuracy and fidelity of weapon data; 4) improved test methods; or 5) improved modeling and simulation (M&S) methods.
  - JTCG/ME enhanced the capabilities of its two major products – the Joint Munitions Effectiveness Manual (JMEM) Weaponeering System (JWS) and Joint Anti-air Combat Effectiveness (J-ACE) – to meet new Combatant Command (CCMD) requirements while supporting real-time operations with collateral damage mitigation analysis packages for high value target precision strikes.
- Special projects continued to make progress in addressing a test instrumentation shortfall for assessing injuries to vehicle occupants during combat-induced, underbody blast (UBB). WIAMan has produced four fully integrated first generation WIAMan prototypes that exhibit improved human-like response, and the program is on track to verify, validate, and accredit the prototypes in anticipation of full-up system-level testing in FY20.

LFT&E ACQUISITION PROGRAMS

- The primary objective of LFT&E is to evaluate the survivability and lethality of acquisition programs and to identify system design deficiencies to be corrected before those systems get deployed or enter full-rate production. Of the 124 acquisition programs under LFT&E oversight, 19 operated under the waiver provision of section 2366, title 10, U.S. Code, by executing an approved alternative LFT&E strategy in lieu of full-up system-level testing. DOT&E published three LFT&E reports and one combined OT&E and LFT&E report in FY17.
- The four reports provided system survivability evaluations for use by the Service and Program Office:
  - The Mine-Resistant Ambush Protected Cougar Category I A1 Block 1 Upgrades and Category II A1 Seat Survivability Upgrade Report evaluated the protection against UBB afforded to occupants of the Marine Corps Cougar Category I A1 Block 1 Upgrades and Category II A1 Seat Survivability Upgrade MRAP vehicles. DOT&E made two recommendations to further improve the survivability of these Cougar variants and their crew.
  - The update to DOT&E's January 2014 Modernized Expanded Capacity Vehicle – Survivability (MECV-S) Survivability Assessment Report updated the 2014 evaluation with comparative data from Joint Light Tactical Vehicle (JLTV) testing. The report update indicated that although the MECV-S and JLTV have similar survivability against underbody threats, the current JLTV design exceeds the mission capability of the MECV-S.
  - The M1070A1 Heavy Equipment Transporter (HET) Urban Survivability Kit (HUSK) Report evaluated the protection against small arms, IEDs, artillery rounds, and blast mines afforded to the occupants of the HUSK. DOT&E made four recommendations to further reduce the crew vulnerabilities to underbody threats and vehicle egress.
  - The CH-53K Heavy Lift Replacement Program Operational Assessment and Live Fire Test and Evaluation Report evaluated the survivability against small arms, automatic weapons fire, and legacy man-portable defense system threats prior to the Milestone C decision. The report indicated that when compared to the legacy CH-53E aircraft, the CH-53K is significantly more survivable. DOT&E made three recommendations to further improve the survivability of the CH-53K system.

LFT&E INVESTMENT PROGRAMS

JOINT AIRCRAFT SURVIVABILITY PROGRAM (JASP)

The mission of JASP is to increase military aircraft combat survivability in current and emerging threat environments. This is accomplished directly and indirectly. The mission is directly supported through funding and oversight of Research, Development, Test, and Evaluation to develop aircraft survivability technologies and assessment methods. The mission is indirectly supported through cross-Service coordination, educating the community about aircraft survivability, maintaining and improving core survivability tools, and taking a lead role in combat data collection. In FY17, JASP funded 42 multi-year projects and delivered 22 final reports. In FY17, JASP focused on projects intended to 1) defeat near-peer and second-tier adversary threats by developing measures to avoid detection and counter engagement of advanced radio frequency (RF) and infrared (IR)-guided threats; 2) improve aircraft force protection; and 3) improve aircraft survivability to combat-induced fires.

Defeat Near-Peer and Second-Tier Adversary Threats

To defeat near-peer and second-tier adversary threats, JASP focused on developing: 1) measures to counter adversary RF-guided threats and anti-access/area-denial capabilities, coupled with quantifiable improvements in Enhanced Surface-to-Air Missile Simulation (ESAMS) and hardware-in-the-loop (HWIL) capabilities; and 2) measures to counter emerging IR homing threats with advanced counter-countermeasures, coupled with quantifiable improvements in the Modeling System for Advanced Investigation of Countermeasures (MOSAIC) and HWIL capabilities.

- In the RF domain, JASP has funded projects to develop and implement algorithms to detect Digital RF Memory (DRFM)-based jamming, mitigate DRFM jamming, and employ DRFM jamming to counter advanced RF threat weapons systems.
  - In FY17, the Naval Research Laboratory (NRL) completed a multi-year project to develop algorithms that enable a friendly system to detect hostile DRFM emissions and then provide an electromagnetic screen for friendly radar systems to operate freely behind. NRL completed testing with the ALQ-214 system and published the results.
  - In FY17, the Air Force Special Operations Command completed a 3-year project to develop 12-bit DRFM techniques against three RF threat systems with non-traditional signals of interest. The Special Operations Command has transitioned the first technique into the ALQ-211(V)2 (utilized by a variety of fixed-wing and rotorcraft) and is working to add the second and third techniques to ALQ-211(V)6 & 9 in FY18.
- ESAMS is a primary tool used by Government and industry to assess the engagement of U.S. aircraft by radar-directed surface-to-air missile systems. JASP, in coordination with the Air Force Life Cycle Management Center, developed several upgrades to ESAMS to maintain its relevancy to current and future threat environments. These upgrades include:
  - Models of chaff as an RF countermeasure to improve the model accuracy and credibility.
  - Improved capability of two threat engagement radar models by adding their electronic counter-countermeasure features. The first system was released in ESAMS 5.4 in FY17; the second system will follow in ESAMS 5.5 in FY18.
  - Improved ESAMS signal architecture to represent and analyze dynamic and reactive signal interactions between multiple players and signals. JASP intends to release this capability in ESAMS v5.5 in FY18.
- Two new JASP projects will take advantage of the recent ESAMS enhancements:
  - First is a study that will determine requirements for future RF expendable decoys. The team will apply modeling, simulation, and analysis to assess the sensitivities and optimal ranges of various Key Performance Parameters for RF expendable decoys. Metrics will include missile break-lock, miss distance, and the size, weight, power, and cost of the candidate decoy technologies. Additionally, the team will study the impacts of maneuver and decoy deployment timings and the increased effectiveness of salvos of decoys.
  - A second effort will develop a new electronic attack (EA) capability against an advanced RF threat radar using a combination of: developing theoretical threat surrogate M&S software; executing HWIL lab testing of the actual threat surrogate to collaborate the M&S model; developing generic advanced coherent EA techniques and testing against the HWIL threat surrogate in the lab; and finally conducting EA jammer flight tests against the threat surrogate in the field to determine EA effectiveness. The successful EA techniques will then be transitioned to existing operational EA jammer systems (such as the ALQ-214 and Next Generation Jammer), subject to their current hardware/software/firmware limitations, and/or be used to generate specifications for upgrading current or developing future EA jammer systems.
- A continuing need across the DOD is valid countermeasure models. The ability to model countermeasures is a critical component in the threat engagement simulations used to develop and optimize tactics, techniques, and procedures (TTPs) in response to near-peer and second-tier adversary threat improvements.
  - JASP funded the development of a physics-based model of chaff dispensed in airflow around fixed- and rotary-wing aircraft. This will improve modeling of chaff effectiveness as a countermeasure; current models do not optimize chaff dispersion based on the influences of aircraft flow field vortices. Additionally, chaff models estimate cloud growth based on empirical test data rather than physics-based modeling of individual particles on the Radar Cross Section (RCS) or Doppler effects. The Naval Air Systems

Command (NAVAIR) and the Office of Naval Intelligence completed development of a model for prediction of the chaff cloud RCS based on the physics-based chaff dispense model and developed datasets for use in ESAMS.

- Helicopter loss rates during Operation Iraqi Freedom, Operation Enduring Freedom, and subsequent counterinsurgency operations were significantly reduced by employment of Missile Warning Systems and effective countermeasures. JASP funded the following efforts to develop technologies and techniques to counter newer classes of IR-guided seekers:
  - NRL development of missile warning algorithms using two-color IR imagery for early identification of threat missiles to enhance countermeasure effectiveness. The main goals are to develop missile identification algorithms capable of exploiting two-color IR imagery, determine the ability to perform missile identification in urban clutter, and characterize jamming performance for Distributed Aperture Infrared Countermeasure (DAIRCM). In FY17, the NRL completed missile identification algorithm development, established performance metrics, and updated its jamming concept of operation in preparation for testing in FY18.
  - The Naval Surface Warfare Center Carderock Division (NSWCCD) and the Air Force Research Lab (AFRL) are conducting a study to determine the advantage of using guided infrared countermeasure (IRCM) expendables to counter advanced IR-guided missiles. In FY17, the team developed three basic concepts for guided IRCM expendables. Each of these concepts seeks to improve IRCM effectiveness against a particular threat or class of threats in the near-peer category. Implementation of the concepts in the Flare Aerodynamic Modeling Environment five degree-of-freedom (5-DOF) equations-of-motion (EOM) implementation in Simulink was completed. A MATLAB/Simulink application was also developed to allow the analyst to pick decoy waypoints in aircraft-continuous coordinates. Integration of the models into the MOSAIC simulation is in progress.
  - In FY16, NSWCCD and the Army Armament Research, Development and Engineering Center (ARDEC) completed development of the JASP-funded Common Setback Measurement Tools, a standardized test set to measure expendable countermeasure launch setback forces. In FY17, NSWCCD and ARDEC received requests from the Services and Industry to use the equipment for future testing and the data to support flight clearance requirements. NSWCCD also agreed to take responsibility for managing, maintaining, and distributing expendable countermeasure setback data for the tri-Service community.

Improve Aircraft Force Protection

To improve the ability of U.S. aircraft to avoid threat detection and to mitigate damage when hit, JASP funded multiple projects focused on the following objectives: improve situational awareness; counter unguided threats; harden aircraft systems; and improve the accuracy and confidence of vulnerability assessments.

- **Improve Situational Awareness.** JASP funded the NRL to develop a sensor package that incorporates both mid-wave infrared and acoustic waveforms for detecting hostile fires and determining the location of the shooter. In FY17 (the final year of a 3-year program), the project completed DAIRCM live fire validation testing. Data analysis and reporting will be completed in 1QFY18 to support DAIRCM Joint Urgent Operational Need fielding on Navy H-60, H-1, and H-6 helicopters in FY18.
- **Counter Unguided Threats.** Aircraft and crew losses to rocket-propelled grenades (RPGs) and other unguided threats are a concern for rotary-wing aircraft. JASP funded NAVAIR and the ARDEC to develop and test anti-RPG warhead concepts. In FY16, ARDEC and NAVAIR developed and tested Dust and Aluminum Frag warhead concepts. In FY17, NAVAIR and ARL researched, designed, and fabricated Consumable Fragmentation warheads for testing in FY18.
- **Harden Aircraft Systems.** During the past year, JASP vulnerability reduction efforts focused on three major areas to improve aircraft force protection: RPG defeat, innovative opaque and transparent armors, and aircraft hardening against high-energy lasers (HEL). In FY17, JASP:
  - Began development of a test capability to replicate Helicopter Active RPG Protection (HARP) RPG countermeasure kill vehicle engagements. HARP is a Future Naval Capabilities program designed to intercept incoming RPGs to reduce rotary-wing vulnerabilities against the RPG threat. The JASP project will provide live fire test data for threat model development, platform and personnel vulnerability analyses including the resultant RPG debris, and support evaluation of kill vehicle effectiveness for milestone decisions.
  - Undertook a major study to develop a scalable nomograph on the amount of aircraft hardening against HEL system threats that will provide a tactically significant survivability improvement. The solution set is mapped to mission profile, altitude, velocity and time on station and is based on intelligence data defining near-, mid-, and far-term HEL irradiances as a function of altitude. The nomograph will define the conditions for testing potential HEL hardening solutions in FY18 and FY19.
  - Completed development and optimization of a composite metal foam armor in conjunction with the University of North Carolina. Target threats were 7.62 and .50 caliber armor piecing rounds, with some preliminary testing against larger blast and fragmentation threats. Although probably too heavy and bulky for aircraft applications, the energy absorption of the system proved promising and should be further evaluated for possible ground vehicle application against larger explosives and IEDs.
  - During live fire testing of a recent armor development program, a significant performance shortfall was uncovered when ultra-high molecular weight polyethylene laminate was impacted at 25 degree obliquity. This anomaly could have serious threat protection implications. JASP initiated a test program to determine the physical mechanism(s)

causing this phenomenon. Testing was completed in FY17; data reduction and analysis are in progress with a report release scheduled for March 2018.

- **Improve the Accuracy and Confidence of Vulnerability Assessments.** In FY17, JASP continued efforts to improve the accuracy and confidence of the prediction of projectile and warhead fragment penetration used to assess aircraft vulnerability.
  - JASP continued to refine the Computation of Vulnerable Area Tool (COVART) Integrated Analysis Environment (IAE) that will improve analysis quality and productivity. The COVART instantiation of the Modular UNIXTM-based Vulnerability Estimation Suite (MUVES) Tool Kit IAE provides a consistent environment for tri-Service vulnerability and lethality analysis in COVART, MUVES, and the Advanced Joint Effectiveness Model (AJEM). The JASP team completed the Beta 3 release for COVART Version 6.9 in FY17.
  - JASP continued to improve the DOD vulnerability/lethality analysis capability by modifying COVART to use the six degrees of freedom (6-DOF) projectile penetration capability JASP added to the ProjPen model in FY16. Coding to implement 6-DOF processing was completed in FY17. After software testing and documentation in FY18, the capability will be released in COVART Version 7.0.

Improve Aircraft Survivability to Combat-Induced Fire

Threat-induced fire is the largest potential contributor to fixed-wing aircraft vulnerability and the greatest source of uncertainty in aircraft vulnerability analysis. In FY17, JASP focused on developing solutions to maximize residual flight capability in the event of threat-induced onboard fires and a robust and reliable fire prediction capability.

- JASP completed a thorough compilation and review of self-sealing fuel bladder performance results from qualification, acceptance, live fire testing, and combat incidents. Analysis of the data and the resulting recommendations were presented to the tri-Service Fuel Bladder Roundtable for consideration of changes and improvements in the fuel bladder qualification testing standard MIL-DTL-27422. The results should also influence requirements and key performance indicators in future acquisition programs.
- JASP completed testing in an operationally relevant environment of the Smart Multiport Fire Suppression System designed to reduce aircraft vulnerability and mitigate occupant casualties from threat-induced fuel fires. A continued development from the first self-contained single ejection port nozzle for confined spaces, this effort completed system integration and optimization of a multi-port nozzle and sensor system for use in large open areas like a helicopter cabin. The system was installed in a CH-53E carcass and tested against RPGs and armor piercing incendiary projectiles.
- JASP continued data collection and module development for the Next Generation Fire Prediction Model (NEXTGEN FPM). JASP began development of a physics-based Hydrodynamic Ram Spurt model to predict the ballistically induced fuel spray/vapor cloud produced by the penetration of a ballistic threat into an aircraft fuel cell. When combined with models of fragment flash and projectile incendiary, the NEXTGEN FPM is expected to predict ballistically initiated aircraft fires with 80 percent accuracy and 80 percent confidence, a significant improvement over current models.

Combat Damage Assessment

JASP continued aircraft combat damage incident reporting in the Services and the DOD through the Joint Combat Assessment Team (JCAT). The JCAT is a team of Army, Navy, and Air Force personnel that deploy to investigate aircraft combat damage in support of combat operations. The team continued to support assessments remotely from the continental United States and is ready to deploy rapidly outside of the United States if necessary.

- The JCAT continued working with the U.S. Army Aeromedical Research Laboratory (USAARL) to study and document aviation combat injuries in Operation Iraqi Freedom and Operation Enduring Freedom. Analysis of UH-60 Black Hawk helicopter incidents was completed in FY17, release of the results and reports is pending USAARL leadership approval. JASP will begin review of AH-64 Apache helicopter incidents in FY18. The results will be documented in USAARL reports and the Combat Damage Incident Reporting System.
- The JCAT and JASP Program Office worked in coordination with the Office of the Deputy Assistant Secretary of Defense for Systems Engineering, Office of the Under Secretary of Defense for Personnel and Readiness, and the Joint Staff's Force Structure, Resource, and Assessment Directorate, J8, on an Aircraft Combat Damage Reporting (ACDR) Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Policy (DOTMLPF-P) Change Request (DCR) proposal that would institutionalize ACDR through changes in joint doctrine, training, information technology infrastructure, and policy. The DCR was approved by the Joint Requirements Oversight Council on November 29, 2016. The JCAT and JASP began working with the Services to implement the approved DCR recommendations.
- The JCAT trained the U.S. aviation community on potential aircraft threats and combat damage. This training includes but is not limited to: capabilities briefs, intelligence updates, recent "shoot-down" briefs to discuss enemy TTPs, and the combat damage collection and reporting mentioned above. The attendees include aircrews, maintenance personnel, intelligence sections, Service leaders, symposia attendees, and coalition partners.

JOINT LIVE FIRE PROGRAM (JLF)

In FY17, JLF funded 21 projects and delivered 16 reports. Focus areas for JLF included projects that either 1) characterized new survivability issues; 2) characterized new lethality issues; 3) improved accuracy and fidelity of weapon data; 4) improved test methods; or 5) improved M&S methods.

Characterization of New Survivability Issues

- **Rocket-Propelled Grenade (RPG) Subcomponent Aircraft Material Penetration Demonstration.** JLF is investigating the penetration characteristics of basic RPG subcomponents impacting aircraft structural material represented by an array of 2024-T3 aluminum target plates (Figure 1). Active Protection Systems (APS) are being developed to provide fixed- and rotary-wing aircraft with the means to intercept and defeat incoming line-of-site threats, including RPGs. When an RPG is intercepted by an APS, the threat RPG may be broken apart (with or without warhead detonation) forming irregular kinetic debris. Questions exist as to the extent of damage caused by such debris when striking an aircraft. In addition to aircraft design details, factors that influence the damage outcome include the type of threat, its orientation, position, and velocity in relation to the aircraft when intercepted, and physical aspects of the debris such as shape, material type, mass, and velocity.
  - The penetration capabilities of the sustainer motors and booster assemblies showed the need to account for vulnerability effects of RPG debris produced during an APS intercept.
  - Ongoing data analysis is occurring to determine what additional information/testing is needed for APS modeling to assess the required safe distance for the APS intercept requirement.

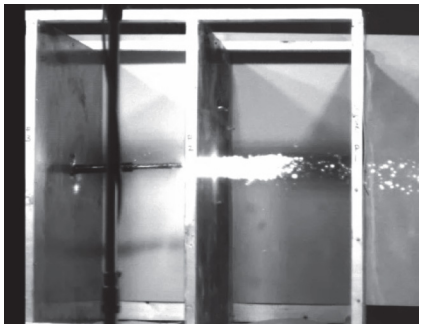


Figure 1. RPG Debris Penetration of Aircraft Structural Material

- **Large Engine Fan Vulnerability to Man-Portable Air Defense Systems (MANPADS).** JLF is investigating large engine fan vulnerability when directly impacted by a MANPADS missile. A fully functional and running JT9D turbofan aircraft engine combined with the inboard section of a B767 left wing and engine pylon were the test articles for this test (Figure 2).
  - This was the first time an operating turbofan engine, running at full power, has been impacted in the front low pressure compressor section, also known as the bypass fan section, by a representative MANPADS threat.
  - Analysis continues to assess MANPADS damage, estimate crew casualty issues, and estimate damage effects on ability to maintain controlled flight.

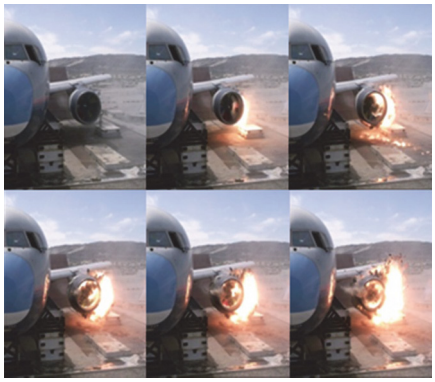


Figure 2. Still Video Images of MANPAD Impact upon an Operating JT9D Turbofan Aircraft Engine and the Ensuing Damage to the Aircraft

Characterization of New Lethality Issues

- **Fragment Penetration Testing of Concrete Masonry Unit (CMU).** JLF obtained fragment penetration data for CMU walls for implementation within the Fast Air Target Encounter PENetration (FATEPEN) model. The FY17 effort completed 45 of 80 planned tests; the remaining 35 tests will be conducted in FY18.
  - Warfighters require the ability to use FATEPEN to accurately predict damage to buildings constructed from CMU blocks. A CMU material model, however, does not currently exist in FATEPEN.
  - Gun-launched annealed 4340 rectangular steel rods impacted CMU block targets built to represent typical exterior walls of hardened and unhardened structures (Figure 3).
  - Impact locations were selected to characterize a wide range of impact conditions affecting penetration mechanics such as solid versus hollow cores, interior webs, mortar joints, obliquity, fragment mass, and impact velocity.
  - JTCG/ME will utilize the results to develop an accredited CMU material model for FATEPEN.

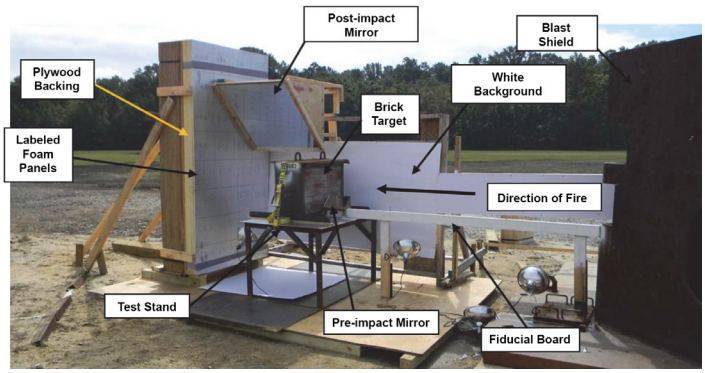


Figure 3. Test Setup for CMU Fragment Penetration Test

Improved Accuracy and Fidelity of Weapons Data Accuracy

- **Bomb Burial Lethality.** JLF is developing testing methods and formal test procedures for quantifying the effects of burial on warhead performance and collateral damage. A demonstration test of a buried HELLFIRE R9E warhead test will be conducted in 1QFY18.
  - Full or partial burial of warheads is a relatively new tactic being employed in military operations in urban terrain to reduce collateral damage from blast and fragment impact.
  - The lethality and collateral effects of weapon burial have not been sufficiently quantified.
  - This program will support a multi-year JTCG/ME test program (begins in FY18) to characterize the effects of burial depth, soil type, and impact orientation for four selected weapons: Small Diameter Bomb (SDB) 1, MK 82, MK 83, and MK 84.
  - JTCG/ME will utilize the results to improve collateral damage risk estimates from crater ejecta, fragmentation, and ground shock.
- **MK 84 Vertical Arena Test Number 2.** JLF obtained new vertical arena test data on the MK 84 general purpose bomb (Figure 4) due to concerns about the quality of existing MK 84 characterization data. JTCG/ME intends to incorporate the results of this test into JTCG/ME M&S and JMEM products. This testing complements similar testing done in FY15 and FY16 to produce a robust data set.
  - Initial examination of the fragment speeds from the test indicated a variance from the current characterization data. This variance has a strong potential to influence weapon usage for lethality, collateral damage estimates, and risk assessment.
  - In addition to the direct application of the characterization by the warfighter, JTCG/ME will compare the data with the output of shock physics predictive tools to improve the warhead detonation model in order to produce high fidelity results, potentially reduce the number of tests required for characterization of other warheads, and provide a better understanding of the fragment cloud.
  - Sandia National Laboratories utilized the test to explore optical fragment tracking techniques. These tracking techniques have the potential to provide additional data that will improve physics-based modeling.

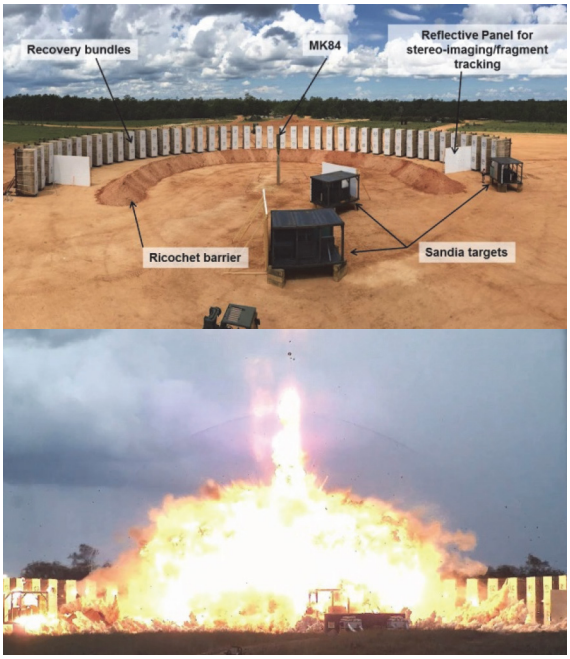


Figure 4. MK 84 Vertical Arena Test: Arena Setup (top); Still Image from High Speed Video after Detonation (bottom)

- **Building Debris Characterization.** JLF conducted a test to characterize the secondary debris produced by the detonation of a HELLFIRE R9E warhead inside a concrete masonry unit structure target (Figure 5). This testing complements similar testing done in FY16 using a PGU-44/B 105 mm High Explosive Projectile.
  - Warfighters require the ability to accurately predict risk to non-combatants from secondary debris. The current collateral damage methodology does not include damage from building debris although it has been operationally observed to be a hazard.
  - Building debris will be characterized in a manner similar to that of warhead fragments.
  - The results will be used to improve risk estimates of personnel injury resulting from both weapon fragments and building debris.

Figure 5. Still Image from Concrete Masonry Unit Building Debris Characterization Test

- **Updating the 1981 Armor Handbook (Initial Volume).** JLF began updating the "Ballistic Technology of Lightweight Armor" published by Francis Mascianica in 1981. This approximately 1,000-page compendium of ballistic data, referred to as the Mascianica Armor Handbook, provides a baseline performance for a wide variety of metal, composite, and ceramic systems against a wide spectrum of threat projectiles. The data in this handbook are useful for developing estimates of armor designs, analyzing the expected performance of armor systems, developing steel equivalencies for use in the MUVES vulnerability/lethality model, and determining the effectiveness of various models and simulations.

- In the intervening 36 years, many new materials (such as Dyneema, SpectraShield, and 7085 aluminum alloy) and threat munitions (both U.S. and foreign) have emerged that were not in the original handbook.
- Since updating the entire handbook cannot be accomplished in 1 year at a reasonable cost, this task updated the highest priority volume (of 11) of value to the vulnerability/lethality community: fragments and fragment simulating projectiles. Data mining is the only practical method to accomplish this update for a relatively modest cost within a reasonable timeframe.
- The data are provided in a format similar to the original Mascianica, such as mean penetration velocity (V_{50}) plotted as a function of armor material thickness (Figure 6). This figure also illustrates the efficiency of the data mining approach since magnesium alloy AZ31B was not included in the 1981 handbook.

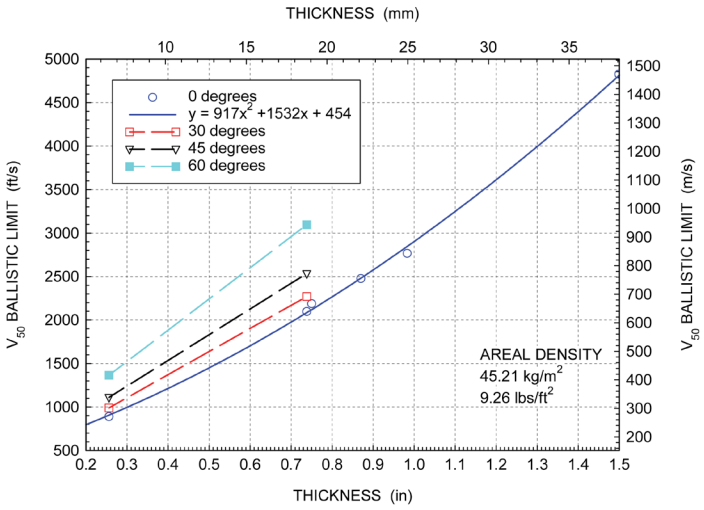


Figure 6. Protection Provided by Magnesium AZ31B-H24, MIL-DTL-32333, Class 1 (Plate Areal Density 45.21 kg/m2) against the .30-cal (44 grain) Fragment Simulating Projectile

Improvements of Live Fire Test Methods

- **Modified RG-31 Testing in Engineered Soil.** JLF conducted six identical UBB tests on a vehicle-like target and collected 410 channels of data to be analyzed and used to understand the sources of variability in UBB testing.
  - UBB testing is used during LFT&E to evaluate vehicle crew survivability in the event of a mine or IED attack. Variability exists in UBB testing, but the extent of that variability is unknown. The data collected from UBB testing drives the evaluation of vehicle crew survivability and influences future vehicle designs. The data are also used to support verification and validation of M&S tools that supplement the live fire data set used for evaluation. The results of this project provide a baseline understanding of the degree of variability in UBB testing.
  - The variability contributed by the soil type used in UBB testing is of special interest to the live fire community due to a 2016 change in the test standard. The new test standard, Engineered Soil with Roadbed Compaction (ERB), was designed to be more controlled and reduce the potential for variability as compared to the old test standard. However, there is limited repeat test data from ERB that includes a crew survivability assessment. Current ongoing analysis of the results from this JLF program will inform the test community regarding the variability from test to test using ERB in terms of vehicle jump height as well as crew survivability assessment.
  - The test series included one Warrior Injury Assessment Manikin (WIAMan) anthropomorphic test device (ATD) alongside four standard Hybrid III ATDs. The WIAMan is currently under development by the Army Research Laboratory and is the first ATD developed specifically for use in UBB testing.
- **Underbody Blast (UBB) Live Fire Test Threat and Blast Box Interaction Analysis.** In the execution of UBB live fire test events, steel box enclosures buried within the ground are used for preparation of soil test beds and emplacement of blast event threats (Figure 7). The current use of 24 by 24 by 10 feet test boxes are approved for use with engineered soil based on previous experimental tests and blast modeling. While maintaining box size sameness was essential to building a robust dataset across multiple UBB charge sizes, the current 24 by 24 by 10 feet blast boxes present a logistical challenge for LFT&E program execution due to their limited number, increased emplacement times, and increased labor and materials costs (especially when testing relatively small UBB LFT&E charge sizes).

Figure 7. UBB Live Fire Test: Soil Being Placed in Test Box (top); Test Bed Complete (middle); Detonation (bottom)

- The majority of primary live fire test ranges utilize 15 by 15 by 6 feet boxes, which currently do not support the use of engineered roadbed soil. Therefore, the need exists to explore charge size limits, utilizing realistic LFT&E charge weights, in both "small" (15 by 15 by 6 feet) and "intermediate" (18 by 18 by 7 feet) boxes to determine how large of charge weight can be used in each blast box without undesirable wall effects.
- JLF funded the Aberdeen Test Center to generate data in terms of impulse, wave velocity through the soil, and overpressure to define the influence exerted on the blast response as a result of interaction with an intermediate size blast box. This would enable establishment of guidelines to define the minimal test box size applicable to relevant live fire test threat sizes.
- This program is being conducted in concert with an ongoing Army Research Laboratory effort currently executing a complementary series at smaller explosive weights in a 15 by 15 by 6 feet box.
- Upon completion of this effort, results will be coordinated and the Aberdeen Test Center will update IOP-SLV-005 "Procedures for Preparation of an Engineered Soil Test Bed in Support of Blast Testing of Vehicles and Test Structures" and publish TOP 02-2-630 "Engineered Soil Test Bed Emplacement Procedures for Live Fire Testing." This will reduce or remove test throughput constraints, increase test execution throughput three-fold, and reduce LFT&E program costs.

• **Instrumented Inert Threat Systems for Active Protective System (APS) Applications.** JLF funded the Army Redstone Test Center to develop a unitary RPG instrumented inert threat system for use in counter-munition effectiveness evaluation during live fire hard-kill APS testing.
  - The development and use of this system will provide a realistic threat that yields more accurate countermeasure impact location and time, while lowering risk to APS vehicle platforms and reducing the dependency on high-speed cameras that do not yield accurate kill or intercept measurements.
  - The instrumentation system design, undergoing field tests and integration development, is composed of transmitters installed inside an inert RPG warhead. Three transmitter circuits will identify three unique zones of the warhead – the front tip (green), the front ogive (blue), and the explosives area (red), as seen in Figure 8. A flexible mesh screen, shaped to the contour of the inner surface area of each zone, will act as a break screen to identify a break in the circuit caused by a counter-munition impact – identifying the impact zone.
  - With the dependable transmitters, high signal resolution, and post-test analysis capabilities, testers/evaluators will be able to more precisely evaluate an APS's claims at reducing threat lethality, more accurately analyze the reduction in platform vulnerability, and ultimately reduce risk to the APS platform.

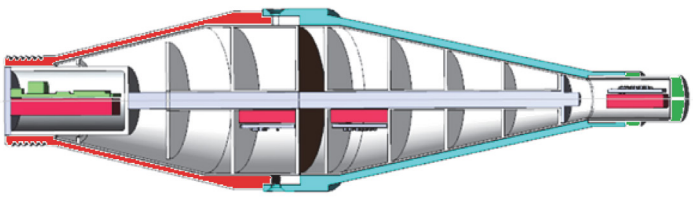


Figure 8. Unitary RPG Instrumented Inert Threat System

• **Assessing Local Accelerative Loading.** JLF funded the improvement of evaluation protocols for accelerometers utilized in live fire and ballistic shock testing. This project complements FY15 efforts that characterized the current state of accelerometer instrumentation and established a basic test protocol for evaluating gauges in the future. The FY17 project is extended to ultimately characterize the effectiveness of accelerometers used in live fire testing, develop and evaluate concept accelerometers, and write a user's guide to educate testers on the advantages and disadvantages of using specific accelerometers in a range of blast environments.
  - This work is being completed in two phases with over 500 individual test events. The first phase consists of characterizing the accelerometers in the laboratory using bench tests that stress the accelerometers at multiple frequency ranges. The second phase of testing consists of characterizing the accelerometers in repeatable explosive tests using a symmetrical blast rig (pictured in Figure 9) that can accommodate multiple accelerometers and that is designed to mimic the frequency response of a ground vehicle.
  - As a result of this effort, testers will have more insight and guidance to help them select the appropriate instrumentation to use in live fire testing based on the expected loads and desired type of data output, improving the DOD's ability to capture accurate and informative data from ground vehicle live fire blast testing.

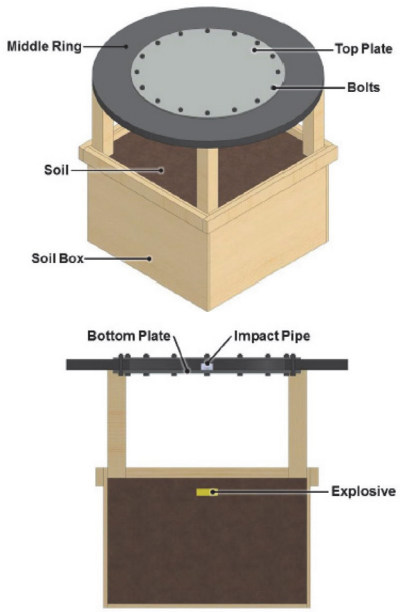


Figure 9. Explosively Driven Test Rig Isometric View (left) and Section View (right)

Improvements of Live Fire Modeling and Simulation (M&S)

- **Enhanced Modeling of Behind Armor Debris (BAD) Velocity Field for Explosively Formed Penetrators (EFPs).** JLF continued to support the improvement of the BAD algorithm by collecting unprecedented, high-speed images of EFP BAD using a pulsed laser illumination system (Figure 10). This testing complements similar testing with shaped-charge and kinetic energy warheads completed in FY15 and FY16, respectively. The BAD algorithm is in both the Army's (MUVES) and joint test and evaluation communities' (AJEM) vulnerability/lethality models. This series of test data builds confidence in modeling the damage produced from BAD fragments to internal vehicle components (including personnel) and will improve future vulnerability/lethality analyses that incorporate BAD.
  - Test data was collected from six shots, including three different EFP warhead sizes.
  - Three-dimensional analyses of these images produced fragment speeds as a function of the fragment's angle from the residual jet.

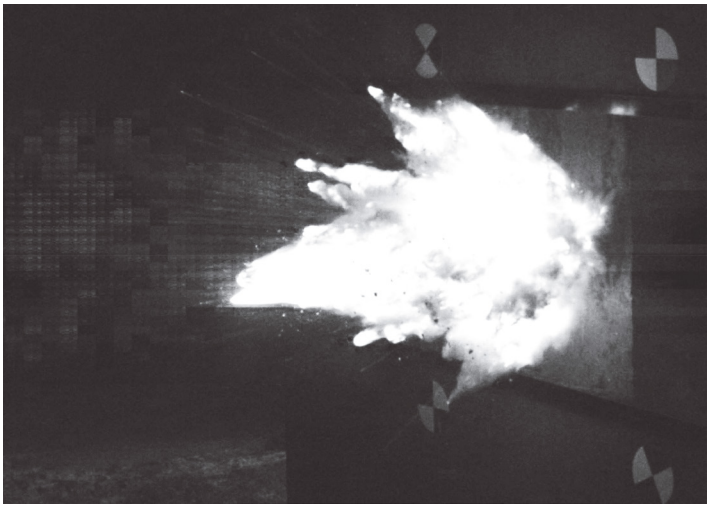


Figure 10. High-speed Image of BAD Fragments Resulting from an EFP

- **Statistical Quantification for LFT&E Planning of Small Arms Munitions.** JLF is investigating a new procedure to improve development of live fire test matrices for small-caliber terminal-ballistics testing by quantifying variation in the collected test data. This work will improve lethality evaluation against personnel as well as potentially reduce the time/cost of performing small-caliber LFT&E testing.
  - The current procedure for weapons effectiveness evaluation relies strongly on M&S to convert the fragments captured during terminal-effects test events into human injury estimation. In the current procedure, all M&S is run after the conclusion of all terminal-effects test events.
  - By interleaving the terminal-effects test events with M&S runs evaluating the terminal performance, it is possible to optimize the distribution of future test events across the predictor space of the system under test and may even be possible to cut the testing short if the variation in results is sufficiently small.
- **OG-7V Fragmentation Grenade Threat Model Development.** JLF is developing an OG-7V grenade threat model based on empirical data. Live fire testing against UH-60A partial fuselages is in execution and will allow for fragment/blast damage mapping comparison between M&S outputs of impacted components and observed test results.
  - JLF encountered a large number of dud OG-7V test articles. JLF then had five munitions X-rayed and visually inspected. No discernable defects were observed that suggested there would be problems preventing detonation. JLF is inspecting the possibility of dud fuzes.

JOINT TECHNICAL COORDINATING GROUP FOR MUNITIONS EFFECTIVENESS (JTCG/ME)

JTCG/ME continued to update and develop weapons effectiveness and target vulnerability data, standards, and methods to evaluate munitions effectiveness, including target vulnerability characterization, munitions lethality, weapon system accuracy, and specific weapon-target pairings driven primarily from current operational lessons learned, Joint Staff Data Calls, and CCMD needs. These capabilities are crucial for developing theater commander force employment options as well as the execution tasking orders to tactical units.

The principal products of the JTCG/ME are the JMEMs. JMEMs enable users to plan the mission by determining the effectiveness of weapon systems against a specified target for a range of weapon delivery modes. JMEMs include: detailed data on the physical characteristics and performance of weapons and weapon systems; descriptions of the mathematical methods that employ these data to generate effectiveness estimates; software that permits users to calculate effectiveness estimates; and pre-calculated weapon effectiveness estimates. This information enables a standardized comparison of weapon effectiveness across all Service communities. Current JMEM product lines products include JWS, J-ACE, Digital Precision Strike Suite (DPSS) Collateral Damage Estimation (DCiDE) tool, and the Digital Imagery Exploitation Engine (DIEE). New product lines include Joint Non-Kinetic Effectiveness (J-NKE) capabilities. There are also specialized solutions that are driven by the needs of CCMDs, coalition partner interoperability, and lessons learned from current operations. Such solutions include Probability of kill (Pk) Lookup Tools; Collateral Damage Estimation (CDE) tables; scenario specific CDE analysis packages; munitions weaponeering guides; rapid response target surrogation; and foreign military sales. Since JTCG/ME products are user focused and requirements driven, considerable effort goes into working with users to establish warfighter requirements for current and future JTCG/ME products, as well as continued training events and day-to-day support.

Air-to-Surface and Surface-to-Surface Weaponeering: Joint Munitions Effectiveness Manual Weaponeering System (JWS)

JWS is the DOD source for air-to-surface and surface-to-surface weaponeering, munitions, and target information used daily by the U.S. Central Command (USCENTCOM), U.S. Special Operations Command (USSOCOM), and U.S. Africa Command (USAFRICOM) in the deliberate planning process directly supporting Joint Publication 3-60, "Joint Targeting." JWS enables CCMDs to prosecute their target sets. JWS incorporates accredited methods, certified munition characteristics, delivery accuracy, target vulnerability data, and numerous user aids to support the operational use of JWS to predict weapons effectiveness for fielded weapons and delivery systems. In FY17, JTCG/ME:

- Continued to facilitate coalition interoperability and information exchange forums. It delivered multiple JWS version releases and standalone Pk Lookup tools to key coalition partners in support of current operations under foreign military sales agreements. This capability improves the effectiveness of U.S. fires and targeting personnel working in combined environments. JTCG/ME also held successful information exchange forums via information exchange agreements with the United Kingdom and Republic of Korea. These exchanges help leverage methods and efforts of mutual interest in the area of weapons effectiveness.
- Supported 19 rapid response surrogations and developed Pk Lookup data for 7 weapons against 13 targets and 119 surrogations based on urgent operational needs for target vulnerability data. These specialized products directly assisted CCMDs to meet the requirements of a dynamic environment as formal products are developed.
- Initiated and finished JWS v2.3 final phase development; fielding is scheduled for FY18. JWS v2.3 will include enhanced data sets and capabilities with a focus on connectivity to other targeting and mission planning capabilities for improved estimates and more seamless planning. More specifically, JWS v2.3 enhanced capabilities include:
  - Improvements to information assurance and cybersecurity.
  - Connectivity to the Modernized Integrated Database, Joint Targeting Toolbox (JTT), and DIEE. This will permit automatic and more optimum transfer of data and information between planning tools.
  - Fast Integrated Structural Tool (FIST) enhancements, such as connectivity to DIEE and JTT and updated target options (building type, material, and features). These updates will improve weapons effectiveness estimates and planning optimization for structural targets.
  - Improvements to the Ship Weaponeering Estimation Tool that optimize database use and improve the user interface. These updates will improve weapons effectiveness estimates and planning optimization for maritime targets.
  - Inclusion of a weapon delivery accuracy module along with updates for the Gunship Delivery Accuracy Program, Rotary Wing Delivery Accuracy Program, and Joint Delivery Accuracy Program. This will provide enhanced calculations for F-35 gun munitions and C-130 gunship effectiveness in JWS.
  - The Dilution of Precision Tool, which improves the predicted accuracy of GPS/Inertial Navigation System weapons from satellite time and space calculations.
  - The Target Location Error Tool, which enables a single JWS tool to provide Target Location Error from airborne- and ground-based sensors.
  - Updates on weapons delivery accuracy and characterization data for multiple systems. This included trajectory model updates based on available Guided Weapon Trajectory Software, Joint Direct Attack Munition, and Small Diameter Bomb (SDB).
  - Over 65 target vulnerability data sets across ground, aircraft, small boats, ships, and submarines, as well over

375 updated images and Quickfacts, which provide the Weaponeer quick-reference characteristics of systems for analysis.

- Continued development of JWS v2.4. JWS v2.4 will provide enhanced data and connectivity capabilities, while maximizing the final JWS v2.x product line and laying the groundwork for the next JWS series (JWS v3.x). Development highlights include a more streamlined database-driven product with enhanced, separated business logic and user interfaces. This will allow for accelerated weapons and target data updates; tailored product versions for releasability; and more effective, focused testing. Specific capabilities will include updated weapons and targets, as well as FIST v2.1 with inclusion and updates to WinBlast, Bridge Analysis System, Linear Target Module, and surface response and penetration functions in burst point editor. These capabilities will enable more options for the Weaponeer and improve the underlying phenomenology representation in JWS.
- Continued development on the next JWS series, JWS v3.x. With the architecture strategy established and a JWS v3.x Capability Needs Statement (CNS) developed in FY17, plans for FY18 include determining the methods to best meet the CNS-established requirements. To ensure long-term viability of the down-selected methods, the characteristics of developmental munitions will be surveyed and included in the decision matrices.
- Supported current use and future development requirements by hosting and supporting JWS training sessions, Operational Users Working Groups (OUWG), and user help desk support via the JMEM Product Information Access System and JWS newsletter. Specifically, JTCG/ME supported approximately 30 JWS sessions at 19 locations with over 400 students. The training sessions allow users to optimize use of JWS capabilities, while providing JTCG/ME with critical input on warfighter use for future development. OUWGs are critical venues for receiving direct user feedback and development of future requirements from the operational community in regards to needed software enhancements and capabilities to support air-to-surface and surface-to-surface weaponeering. JTCG/ME continued to chair OUWGs, with participation from USCENTCOM, USAFRICOM, U.S. Strategic Command (USSTRATCOM), U.S. Pacific Command, USSOCOM, the Services, the Defense Intelligence Agency, the Defense Threat Reduction Agency, the Fires Center of Excellence, Service School Houses, the Marine Aviation Weapons/Tactics Squadron, Operations Support Squadrons, Intelligence Squadrons, and numerous other operational units.

Collateral Damage Estimation, Reach Back, and Planning Connectivity: Digital Precision Strike Suite (DPSS) Collateral Damage Estimation (DCiDE) Tool and the Digital Imagery Exploitation Engine (DIEE)

With the changing complex strategic environment, urban and close-combat operations have become a focal point of military restructuring. Using lessons learned from traditional-based strategies, military commanders and leaders have sought innovative answers in decreasing collateral damage, saving innocent lives, and reducing military costs. Decreasing these measures meant progressing computing and communications equipment, enhancing lines of communication, increasing response times to High Value or Time Sensitive Targets, improving mission planning objectives, and increasing situational awareness on the battlefield. JTCG/ME continues to support these complex needs by developing and providing accredited collateral effect radii (CER), interoperable CDE capabilities, enhanced methodology, and reach back support for the warfighter. In FY17, JTCG/ME:

- Continued to enhance the Collateral Effects Library (CEL) tool in support of advanced CDE mitigation techniques.
- Updated the accredited CER Reference Tables for selected air-to-surface and surface-to-surface weapons, which are the basic data that support the CDE methodology. The JTCG/ME CER tables and CDE methodology are used in every planned kinetic strike in all Areas of Responsibility (AORs) to meet commanders' intent and to minimize civilian casualties. JTCG/ME implements the CER and CDE methodology within the DCiDE tool, an accredited and automated tool that expedites and simplifies the CDE process. DCiDE enables JTCG/ME to continuously support the Chairman of the Joint Chiefs of Staff Instruction 3160.01B, "No-Strike and the Collateral Damage Estimation (CDE) Methodology." DCiDE is the only automated CDE tool authorized for use in the USCENTCOM and USAFRICOM AORs.
- Supported the fielding of DIEE v2.0 and development of DIEE v2.1, with expected fielding in late 2017. DIEE is an enterprise targeting solution that provides both seamless planning and linkage to various mission planning systems and tools in operational units. It interconnects precision point mensuration, weaponeering, and collateral damage estimation applications, allowing targeting or planning personnel to develop strike plans, while linked to mission planning systems for target execution.
  - DIEE v2.0 included full DCiDE functionality for automated CDE, quick weaponeering tables for automated weaponeering solution development, production of standard targeting package graphics, and connectivity to mission planning systems. DIEE v2.1 will include user requested enhancements, JWS interface, and updated Common Geopositioning Services for precision point mensuration capability. Future versions will include 3D viewer capability.
  - Supported DCiDE and DIEE training sessions for approximately 100 personnel.
- Leveraged CEL and other high fidelity techniques to deliver 25 collateral damage mitigation analysis packages to operational users for high value targets. JTCG/ME also provided collateral damage mitigation tables for use by the broader operational community. These efforts directly assisted CCMDs to meet commander's intent and minimize collateral damage.

- Planned, in conjunction with JLF, a focused program (beginning in FY18) to enhance and validate collateral damage. The enhancement will support improvements in weaponeering methodology to minimize risk to mission and forces while not increasing risk of collateral damage by providing foundational data for the development of higher fidelity predictive tools. Specific efforts will generate buried ordnance characterization data based upon usage statistics from CCMD expenditure reports, and AOR specific building debris data to enhance and validate current weaponeering/collateral damage estimation methods required by Strike Approval Authorities to make their strike decision calls. FY18 efforts build off three FY17 JLF testing events and multiple collaboration forums.
- Provided direct forward presence support to Combatant Commanders, which enabled target materiel development, weaponeering, and CDE solution development.

Air-to-Air and Surface-to-Air Combat Tactics, Techniques, and Procedures Development: Joint-Anti-air Combat Effectiveness (J-ACE)

J-ACE provides authoritative air-to-air and surface-to-air weapons effectiveness information, and serves as the primary tool used by the Air Force and Navy to underpin air combat tactics, techniques, and procedures (TTPs) development. J-ACE (Figure 11) is the umbrella program that includes both the Joint Anti-air Model (JAAM) and Endgame Manager, which provides a full kill chain end-to-end capability. Other users include National Test and Training Ranges for air-to-air and surface-to-air shot validation and various members of the analytical community for air combat studies and planning. USSTRATCOM leverages J-ACE capabilities to support route planning for the execution of strike packages. JAAM supports operational squadrons' mission debrief tools such as the Personal Computer Debriefing System. In FY17, JTCG/ME:

- Finished J-ACE v5.3, which extended and updated data sets for missile and aircraft target aero performance, anti-air missile lethality, and air target vulnerability. These data include over 40 air-to-air missile models (blue and threat), over 50 surface-to-air missile models (threat), and approximately 40 aircraft models (blue and threat). New capabilities include:
  - Initial Hybrid Integration and Visualization Engine computer architecture interface, which will allow for increased future leveraging and modularity for enhancements.
  - The BLUEMAX6 (6-DOF aero performance) model for increased aircraft aero performance modeling, with Hands-on Throttle and Stick allowing for actual flight control of the aircraft.
  - Increased ability to estimate countermeasure effectiveness by leveraging Enhanced Surface-to-Air Missile Simulation (ESAMS) to assist planning in ever-increasing area denied environments.
  - Factoring in the effect of weapon system reliability when calculating the probability of a successful engagement.
- Developed a standalone weaponeering guide for an electronic attack/warfare capability that will be integrated into future J-ACE versions.
- Continued J-ACE v5.4 development, with expected completion in 2018. J-ACE v5.4 fielding will include an enhanced BROWSE module for descriptive material to support new weapons in the JAAM and Endgame Manager. J-ACE v5.4 will enhance Personal Computer Debriefing System capability, and further evaluate enhancement of aircraft maneuverability modeling with Hybrid Integration and Visualization Engine (HIVE)/BLUEMAX6 data and models. In addition, JAAM will include initial capability to evaluate two-sided Suppression of Enemy Air Defense (SEAD) and Destruction of Enemy Air Defense (DEAD); improved target detection capability leveraging National Air and Space Intelligence Center Radio Frequency (RF) models and data; and increased ESAMS capability.
- Worked and performed requirements analysis for longer development needs for future J-ACE versions, to include rotary-wing aircraft capability, increased SEAD/DEAD capability, and increased electronic warfare and countermeasure capabilities. Specifically, JTCG/ME worked several aspects needed for rotary-wing capability to include review of potential aero performance models, as well as data and methodology needs to address the broader threat and operational effect spectrums as compared to fighters and bombers already on the product (slower, lower altitude with more terrain effects). Additionally, JTCG/ME reviewed opportunities to address increased SEAD/DEAD capability by leveraging existing air-to-surface weapon trajectory models and interaction with JWS effectiveness estimates. JTCG/ME continued to investigate how to best leverage electronic warfare and countermeasures engineering level investments in an operational modeling environment.
- Led and hosted External Interface Working Group (EIWG) forums. These forums are pivotal for J-ACE developers to understand requirements and align development with other external debrief and analytical capabilities that use J-ACE as the underlying analytical engine to underpin results. The

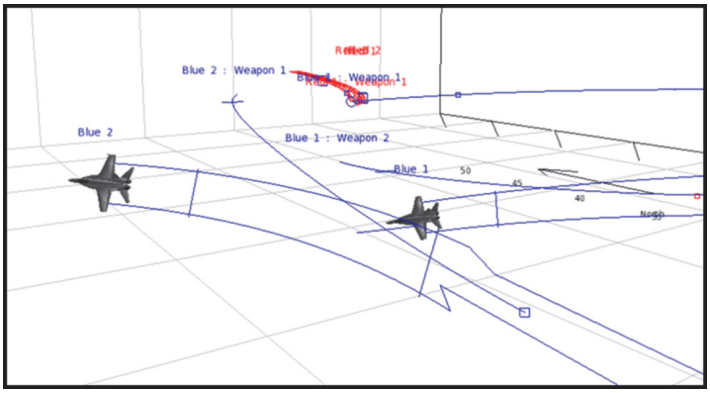


Figure 11. The primary J-ACE interface is through the Joint Anti-Air Model (JAAM). JAAM is a fast running simulation of air-to-air missiles and surface-to-air missiles as well as aircraft aerodynamic performance.

EIWG meeting allowed J-ACE external application developers to receive an update on the upcoming J-ACE v5.3 release and continued development of J-ACE v5.4. The forums included user agreement process updates, application programming interface changes, final v5.3 product review, v5.4 development review, and use case presentations. Participants included the Air Force Weapons School, TOPGUN, Intelligence Community, USSTRATCOM, Air Force Life Cycle Management Center, Naval Air Warfare Center, as well as contract developers of J-ACE, Personal Computer Debriefing System, Individual Combat Aircrew Display System, Joint Debriefing Subsystem, Common Mission Debrief Program, and Extended Air Defense Simulation.

Cyber and Directed Energy Effectiveness: Joint Non-Kinetic Effectiveness (J-NKE) - Cyber and Directed Energy JMEMs

Joint Non-Kinetic Effectiveness is intended to be the single source for operational warfighters, analysts, targeteers, and planners to analyze offensive cyber capabilities and directed energy effects. In FY17, JTCG/ME, in conjunction with other stakeholders:

- Continued planning and development of cyber effects estimations with a focus on standardization of data required to address weapon characterization, target vulnerability, operational environment, and uncertainty metrics to support the development of a Cyber Operation Lethality and Effectiveness tool. Efforts continue with linkages to the U.S. Cyber Command and other key stakeholders to ensure Combatant Command and Service warfighter requirements are articulated and understood. DOT&E will receive additional funding to address some of these shortfalls in FY18.
- Coordinated with a FY18/19 Joint Test Project to leverage, enhance, and develop directed energy effects estimation and standardization tools. The FY18/19 Joint Test Project, Joint Laser Systems Effectiveness (JLaSE), was approved as a conduit for warfighters to solve joint laser operational issues and provide a non-materiel solution to the warfighter. Efforts will take advantage of work completed by the High Energy Laser Joint Technology Office and various planned Use Cases throughout the 2-year cycle. Focus will be on various Service near-term capabilities that take advantage of the directed energy laser (DEL) weapons low cost per shot, deep magazine, precision engagement, and scalable effects. Collateral Damage concerns will also be addressed. Results of the tasking will provide Joint Fire Support Planners and Targeteers the Tactics, Techniques, and Procedures for Weaponeering and Collateral Damage Estimation, to adequately plan for and execute Directed Energy Laser Weapons in the joint battlespace.

LFT&E SPECIAL INTEREST PROGRAMS

WARRIOR INJURY ASSESSMENT MANIKIN (WIAMan)

- The WIAMan Engineering Office (WEO) is currently leading the WIAMan project (Figure 12) on behalf of the Army Research, Development, and Engineering Command (RDECOM), with the Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) supporting acquisition-related preparation activities. RDECOM and PEO STRI have a memorandum of agreement defining the leadership, responsibilities, and funding relationships between these two organizations.
  - The WIAMan project plans to enter the acquisition cycle as a post-Milestone A program of record via a Materiel Development Decision in 1QFY18. The WEO will transition leadership of the WIAMan project to PEO STRI at Milestone B, but will continue to support PEO STRI in certain non-severable activities related to the WEO's expertise in biomechanics, ATD development, and LFT&E.
  - The WEO continued to demonstrate that the current ATD used in LFT&E, the Hybrid III, lacks biofidelity in the UBB test environment, meaning it does not exhibit a human-like response when exposed to UBB loading conditions. ATD biofidelity is assessed via compliance with biofidelity response corridors (BRCs) for the human body regions and response parameters of interest.
  - In FY17, the project delivered the remainder of the 15 whole-body BRCs, completing planned BRC testing. These BRCs focused on human response to different combinations of parameters that vary in LFT&E, such as loading rate inputs, occupant posture, and use of Personal Protective Equipment.
  - The project continued injury biomechanics research to support development of both human injury probability curves (HIPCs) and injury assessment response curves (IARCs). IARCs provide the probability of human injury as a function of the various measurements recorded by the ATD during test events. The WEO delivered the first two preliminary HIPCs and IARCs to evaluators in 4QFY17, in support of armored multi-purpose vehicle (AMPV) system-level LFT&E testing scheduled for FY18.
- The WEO continued its 3-year pilot study to investigate the effects of the UBB environment on female soldiers. The objective of this study is to determine if UBB loading conditions affect females differently than males and, if so, for what reasons. The WEO intends to use the results of this pilot study to inform a decision about the need to develop unique injury assessment capability for female soldiers. A total of five whole-body female biomechanics tests were executed in FY17, with an additional test planned for FY18. The component testing phase (approximately 80 tests) of this study will occur in FY18. The WEO plans to complete this study in FY18.
- Diversified Technical Systems delivered on schedule four fully integrated first generation WIAMan ATD prototypes in June 2017. The WEO has started to use these prototypes during IARC testing, and is completing the verification, validation, and accreditation plan for these prototypes. When

the opportunity presented itself, the WEO successfully incorporated a WIAMan Technology Demonstrator ATD in a series of UBB experiments to gain insight on the WIAMan's biofidelic response, design, and durability.

- The WEO continued its refinement of an optimized ATD finite element model (FEM), with a view to evaluating how well the FEM will work when integrated as a sub-system of the Army's current UBB modeling methodology. The WEO is also refining the FEM to reflect the final configuration of the delivered prototypes.
- The WEO continues to accomplish its technical goals regarding establishing human body response to the UBB load regime, to include expanding its investigation into potential gender-based differences. The Army has refined its previous plan and schedule to more rapidly develop and deliver an initial WIAMan capability. The acquisition program is funded through FY19 and will procure additional prototypes that will be used for AMPV full-up system-level testing in FY20. The Army is working to fund WIAMan beyond FY19.

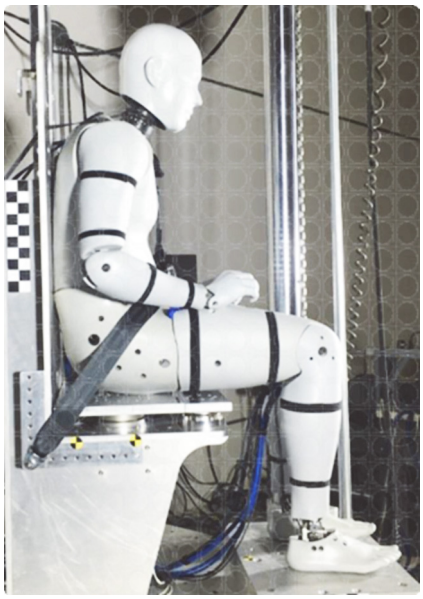


Figure 12. Generation 1 WIAMan ATD

SMALL BOAT SHOOTERS' WORKING GROUP

Small boats are a significant asymmetric threat to ships operating in littoral waters. Several weapon systems that can provide defense against these threats are being developed, tested, and evaluated by the Army, Navy, Air Force, and Marine Corps. The Small Boat Shooters' Working Group facilitates the coordination and collaboration of the various efforts underway to counter and defeat this threat.

- In FY17, DOT&E sponsored the sixth annual Small Boat Shooters' Working Group meeting. At this meeting, the current small-boat threats were reviewed, and updates were provided on defensive system programs, including test results. Information on related programs, such as targets, instrumentation, test ranges, and lethality models, was also provided. Specific topics included results from HELLFIRE longbow missiles vertically fired from a ship against High-Speed Mobile Surface Targets (as part of the Littoral Combat Ship program), results from Air Force tests of various weapons against high speed boat targets at test ranges near Eglin AFB, and plans for upcoming Joint Air-to-Ground Missile tests against the High Speed Maneuverable Surface Target and Coast Guard 41 Fast Attack Craft surrogate targets.

Cybersecurity

Cybersecurity

Cybersecurity

SUMMARY

DOT&E assessments over the past fiscal year confirmed that the conclusion from previous years is still valid – DOD missions and systems remain at risk from adversarial cyber operations. Operational tests consistently discovered mission-critical vulnerabilities in acquisition programs. Assessments during Combatant Command training exercises confirmed that DOD cyber defenses are improving, but not enough to stop adversarial teams from penetrating defenses, operating undetected, and degrading missions. Tests and assessments continue to identify previously undetected vulnerabilities, and DOT&E remains committed to facilitating the remediation of these vulnerabilities and verifying that adequate solutions or mitigations are in place.

DOT&E's use of realistic, long-duration adversarial portrayal in assessments for Combatant Commands continues to show that a persistent adversary can gain significant accesses and a deep understanding of warfighter missions and plans. However, most exercises provide only limited time for realistic cyber-attacks; a short-duration (e.g., 5-day) exercise is barely long enough to confirm warfighter readiness in their basic, non-cyber-related missions. Hence, Combatant Commands usually conduct training in a relatively benign cyber environment, which is unlikely to exist for DOD. This may provide warfighters a false sense of confidence about the scope and magnitude of the cyber-attacks facing the Department.

In FY17, DOT&E cyber assessment efforts continued to focus on the ability of warfighters to execute critical missions in the expected operational environment. The demand associated with the planning and conduct of operational tests of acquisition programs remained high, as did the demand for cybersecurity assessments for Combatant Commands and Services. These demands, as well as cyber assessments of DOD weapons systems mandated by section 1647 of the FY16 National Defense Authorization Act (NDAA), resulted in a continuing shortfall for certified DOD Red Teams capable of portraying realistic threats. Operational tests and assessments associated with offensive cyber tools and processes grew, reflecting the increasing DOD interest and effort in this aspect of cyberspace operations.

Well-trained personnel are critically important for executing effective defensive and offensive cyberspace operations and for emulating cyber opposing forces. The best cyber defensive and offensive operations always included knowledgeable and skilled personnel and network users who practiced good cybersecurity. Cyber-related technology was only useful when its operators understood how to operate it effectively. When DOD fielded technology prior to adequate training of operators, as in the case of Joint Regional Security Stacks, the technology did not provide significant benefits to operators.

CYBER ASSESSMENT ACTIVITY

DOT&E continued to oversee cybersecurity OT&E for major defense acquisition programs, and to perform congressionally directed cybersecurity assessments of operational networks and systems during Combatant Command and Service training exercises. DOT&E also expanded involvement in operational assessments for offensive cyber capabilities and tools.

Based on results from operational tests and exercise assessments, DOT&E publishes reports on overarching cybersecurity topics of interest. DOT&E published two classified reports in 2017. The first report discussed special topics in cybersecurity, including defensive best practices, cross-domain solutions, capture of credentials, programmable logic controllers, and incident reporting. The second report presented findings on defensive cyberspace operations that involved a new method for evaluating how well a network can support defensive cyber operations.

Table 1 shows those acquisition programs on oversight that completed operational tests including cybersecurity, and the DOT&E-funded cybersecurity assessments of Combatant Commands and Services conducted during FY17. Table 2 shows the DOD test organizations and agencies that supported the conduct of these activities.

TABLE 1. CYBERSECURITY OPERATIONAL TESTS AND ASSESSMENTS IN FY17	
PROGRAMS COMPLETING OPERATIONAL TESTS OF CYBERSECURITY	
Amphibious Assault Vehicle Survivability Upgrade	Joint Light Tactical Vehicle
AC-130J Ghostrider	Joint Regional Security Stack
Amphibious Combat Vehicle	Joint Warning and Reporting Network
Advanced Field Artillery Tactical Data System	Key Management Infrastructure
AN/SQQ-89A(V) Integrated Undersea Warfare (USW) Combat Systems Suite	LHA 6 *America*-class Amphibious Assault Ship
Ballistic Missile Defense System	Air Force Mission Planning Systems
Common Analytical Laboratory System	Next Generation Diagnostic System
Consolidated Afloat Networks and Enterprise Services	P-8A Poseidon
Chemical Demilitarization	Patriot Advanced Capability 3
Defense Agencies Initiative	Paladin/Field Artillery Ammunition Supply Vehicle (FASSV) Integrated Management
Defense Enterprise Accounting and Management System	Spider XM-7 Network Command Munition
DOD Healthcare Management System Modernization	Ship Self-Defense System
Defense Medical Information Exchange	SSN 784 *Virginia*-class Submarine
F-35 Joint Strike Fighter	Stryker Engineering Change Proposal
Ground/Air Task Oriented Radar	Warfighter Information Network – Tactical
Joint Air-to-Ground Missile	
CYBER READINESS CAMPAIGNS WITH ASSOCIATED EXERCISE	
U.S. Africa Command Judicious Response 2017	U.S. Northern Command Alaska North American Aerospace Defense Command (NORAD) Region Event
U.S. Air Force 603rd Air Operations Center Event	U.S. Pacific Command Pacific Sentry 2017
U.S. Army Reserve Command Event	U.S. Southern Command Integrated Advance 2017
U.S. European Command Austere Challenge 2017	U.S. Special Operations Command Epic Guardian 2017
U.S. European Command Steadfast Cobalt 2017	U.S. Special Operations Command Jade Helm 2017
U.S. Forces Korea Ulchi Freedom Guardian 2017	U.S. Strategic Command Global Lightning 2017

TABLE 2. CYBERSECURITY TEST COMMUNITY	
OPERATIONAL TEST AGENCIES	
Military Services	Air Force Operational Test and Evaluation Center
	Army Test and Evaluation Command
	Navy Operational Test and Evaluation Force
	Marine Corps Operational Test and Evaluation Activity
Defense Agencies	Joint Interoperability Test Command
CYBER TEAMS	
Air Force	57th Information Aggressor Squadron
	177th Information Aggressor Squadron
	92nd Cyberspace Operations Squadron
	46th Test Squadron
	18th Flight Test Squadron
	Air Force Information Operations Center
	688th Information Operations Wing
Army	1st Information Operations Command
	Threat Systems Management Office
	Army Research Laboratory, Survivability/Lethality Analysis Directorate
Navy	Navy Information Operations Command
	Space and Naval Warfare Systems Command
	Navy Operational Test and Evaluation Force
Marine Corps	Marine Corps Information Assurance Red Team
Defense Agencies	National Security Agency
	Defense Information Systems Agency Red Team

Operational Test and Evaluation with Cybersecurity

DOT&E continued to emphasize the planning and conduct of operational tests that include cybersecurity testing. DOT&E recommends cybersecurity testing for all systems that transmit, receive, or process electronic information, by direct, wireless, or removable means. These tests identify vulnerabilities that developers should fix so that secure and resilient systems are developed and fielded, enabling units or agencies equipped with the systems to complete assigned operational missions in a cyber-contested environment. In FY17, DOT&E monitored operational tests with cybersecurity phases for 30 acquisition programs, and continued efforts to enhance the operational realism of cybersecurity tests by researching techniques and tools for testing cross-domain solutions, non-Internet Protocol data buses, and programmable logic controllers.

Assessment of Offensive Cyber Capabilities

In January 2017, DOT&E issued a memorandum that highlighted concerns with the limited operational realism of tests for offensive cyber capabilities. DOT&E is working with capability developers and their testers to explore how best to integrate operationally realistic testing into the non-traditional acquisition lifecycles of these capabilities, which often involve compressed timelines. Concurrently, DOT&E is working with the Joint Technical Coordinating Group for Munitions Effectiveness to identify the data required to build predictive analysis tools for planners to predict cyber effects.

The Combatant Commands are maturing their operational processes for targeting and employing offensive cyber capabilities. U.S. Pacific Command (USPACOM) and U.S. Forces Korea (USFK) requested that DOT&E assist in assessing their cyber fires planning and execution processes during Pacific Sentry 17-2 and 17-3, as well as Ulchi Freedom Guardian 2017. DOT&E assessed the synchronization of cyber fires with component schemes of maneuver, integration of intelligence support, and support to commander objectives, and made recommendations to improve these critical procedures. DOT&E also observed, on closed ranges, the demonstration of several offensive cyber capabilities.

Cybersecurity Assessment Program

DOT&E's Cybersecurity Assessment Program continued to provide resources for operational test agencies, intelligence subject matter experts, and DOD Red Teams to create and assess cyber activities and effects on operational networks and systems during Combatant Command and Service training exercises. DOT&E implemented cyber readiness campaigns that help address vulnerabilities and improve cyber defenders through a series of focused events throughout the year, that culminate in an assessment during a training exercise. The larger number of cyber-readiness campaign events provides more assessment

opportunities to assist Combatant Command and Services with specific areas or items of interest.

Engagement with the Intelligence Community

DOT&E is working closely with the Intelligence Community to share independent cyber testing results and analysis of DOD networks and weapon systems. DOT&E's analysis helped inform a National Security Agency assessment and a National Intelligence Council Memorandum for the Deputy Secretary of Defense. DOT&E participated in threat intelligence briefings to the Under Secretary of Defense for Intelligence and the National Security Council as part of a combined Intelligence Community team. The collaboration between the Intelligence Community and DOT&E demonstrates the importance of testing results and how those results can be applied to better understand cyber threats against the DOD and the Nation.

There were numerous reports in FY17 of unclassified data being stolen from cleared defense contractors. DOT&E is forming a team of engineers, system designers, system operators, cyber Red Team members, Intelligence Community experts, and program representatives to characterize the risk posed by the exfiltration of critical data of a DOD system via unclassified networks. The DOD should deploy more personnel to the task force that is identifying vulnerabilities based on information stolen from cleared defense contractors, and direct defense contractors to demonstrate, via cyber Red Team exercises, that they can adequately protect DOD weapons and sensitive information.

Coordination with USD(AT&L) on Statutory Cybersecurity Assessments

In FY17, DOT&E collaborated with USD(AT&L) in planning cyber vulnerability assessments for major DOD weapons systems, as directed by section 1647 of the FY16 NDAA. DOT&E invited USD(AT&L) representatives to observe cybersecurity assessments that DOT&E's Cybersecurity Assessment Program performed with several Combatant Commands, and developed concepts and processes for how best to share assessment results and align future DOT&E activities with statutory cyber assessments. DOT&E and USD(AT&L) also agreed to collaborate on the creation of a global persistent cyber opposing force that expands upon the activities that DOT&E began with USPACOM and U.S. Northern Command (USNORTHCOM).

OBSERVATIONS AND RECOMMENDATIONS

FY17 Cyber Defense Improvements

DOD network defenses against cyber adversaries portrayed in training exercises are improving over defenses observed in prior years. Adversarial teams consistently commented on the improved network defenses due to improved patching and configurations, which resulted in the teams having greater difficulty penetrating assessed networks.

Detection rates of adversarial teams following the initial network penetration were much higher when the teams had to use unauthorized tools instead of their preferred method of using tools already in the network, such as operating system administrator tools, to conduct attacks. The probability of DOD network defenders detecting the adversarial teams improved over the 3-year period starting in FY14, and they are detecting cyber-attacks that previously went undetected.

To improve detection of adversaries in the network, the DOD should:

- Continue improving the speed and completeness of fielding patches, implementing signed patches and updates to remove the ability of an adversary to modify software without authorization. DOD cybersecurity would improve and afford adversaries fewer exploitable vulnerabilities if network defenders implemented U.S. Cyber Command's directives in a timely manner.
- Reduce access to credentials and system administrator tools that adversaries can use as attack tools.
- Expand the practice of "whitelisting" to limit data and applications to authorized users.
- Actively audit system configurations to ensure they remain secure.

Vulnerabilities Remain in DOD Network Defenses

Despite improvements in network defenses, almost every assessment and test demonstrated that DOD network defenses still contain exploitable problems that provide cyber adversaries opportunities for access to DOD networks. Some adversarial teams had longer periods to plan and execute attacks, which was more representative of the time an actual cyber adversary has. These teams often found more vulnerabilities and gained a better appreciation of the operational implications of these vulnerabilities.

Once adversarial teams gained access, they were frequently able to maneuver undetected in a network and exploit trust relationships and systems connected to the network. With these system-level accesses, adversarial teams continued to demonstrate that they can exfiltrate mission-critical information and/or create effects that degrade or prevent mission accomplishment.

Assessment teams for tests and exercises persistently find and report serious vulnerabilities, many of which involve unpatched or misconfigured devices and software. Reasons for problems in basic network hygiene include ineffective operational and administrative network procedures, poor physical security surrounding network components, and shortfalls in net-defender staffing and expertise.

Defender Expertise is Essential

Effective cyber defense requires effective cyber technology coupled with well-trained operators and defenders. Fielding new technology without the support of capable operators can reduce and even eliminate the potential benefits of that technology. A

prime example of this is the fielding of Joint Regional Security Stacks (JRSSs), which are expensive, room-sized technology suites with complex integration challenges. JRSSs are intended to centralize and standardize network security into regional architectures.

The Army and Air Force started fielding JRSS in 2016 without performing the independent cybersecurity assessments that are normally required for major acquisition programs. The Defense Information Systems Agency (DISA) performed an operational assessment in September 2017, which discovered key cybersecurity deficiencies with JRSS technology, processes, and training. New JRSS program leadership intends to address these deficiencies. In the meantime, network defenders who already struggled with legacy network security problems must deal with additional JRSS-related problems.

In recent years, DOT&E has observed well-defended networks only where mature and well-configured network technology supported well-trained and experienced network defenders. The expedited fielding of immature network technology and training packages helps neither the warfighter nor the teams who strive to support the warfighter with enabling technologies.

DOT&E observations continue to highlight that human expertise is essential for effective cyber operations, including defensive cyberspace operations, offensive cyberspace operations, and cyber adversarial teams. System and network users must understand that they are both users and defenders of their mission space. Users and cyber defenders must understand the networks and systems under their purview at least as well as potential adversaries. They must be well-versed in the procedures for reporting and responding to cybersecurity incidents and conduct clear and timely communications between cyber-defense organizations.

Major training events should include periods where a threat-representative cyber adversarial team demonstrates attacks and stresses the networks, systems, and missions; the network users and defenders should demonstrate whether they can sustain critical missions in such a contested environment. Although directed by The Chairman of the Joint Chiefs of Staff in 2011, and endorsed by two subsequent Secretaries of Defense, DOT&E has not observed many demonstrations that Commands can "fight-through" a major cyber-attack and sustain their critical missions. The Combatant Commands and Services should perform frequent training that includes disruptions in order to prepare for expected cyber-attacks, and develop and document well-coordinated responses in operational playbooks.

Adversarial teams must understand adversarial capabilities and intent, but to portray an advanced adversary they must also understand DOD mission objectives and defensive capabilities. Armed with this aggregated knowledge, adversarial teams can perform representative cyber-attacks to train operators and defenders, and help identify the most likely and critical vulnerabilities for mitigation.

Hiring, training, and retaining people with cyber knowledge, awareness, and skills is both more efficient and more difficult than simply buying the latest technology. Retention of an expert cyber workforce – including operators, defenders, adversarial teams, and assessors – is essential to achieving the goals of the DOD Cyber Strategy.

Maturation of cyber skills and capabilities requires experience and knowledge from testing and training in realistic conditions. To this end, the DOD should:

- Allow disruptions caused by threat-representative cyber effects in all major exercises in order to demonstrate mission resiliency to cyber-attacks.
- Consider additional ways to retain highly skilled personnel that the DOD requires for effective cyber-defense, offense, and assessment missions.
- Ensure operators of new cyber technology receive adequate training prior to fielding the technology.
- Hold users who commit serious violations that degrade DOD cybersecurity more accountable.
- Minimize the use of and improve the monitoring of cross-domain solutions.
- Consider reducing the connection between the Non-classified Internet Protocol Router Network and the Internet for most DOD users. This could reduce the cyber-attack surface and allow defenders to focus their time and energy on attacks by more advanced adversaries.

Defender Span of Control

The concept of cyber span of control must mature to understand how many defenders can cover assigned network terrain. To-date, defenders of small headquarters networks (networks that host a few hundred users) have been more likely than defenders of large networks to succeed against a realistic cyber opposing force. Cyber Red Teams find it easy to operate undetected across large networks like the Air Force Information Network, which supports approximately 800,000 users.

DOT&E has observed a number of cases of successful network defense during exercises and operational tests. These successful defenses occurred in small networks, including those at Combatant Command headquarters. These small networks typically had at least one defender for every few hundred user accounts, enabling defenders to monitor network and user activity, and to apply cybersecurity best practices effectively. DOD should continue to implement the following best practices:

- Operators and defenders have expert knowledge of their missions and networks, are familiar with normal operations and can recognize anomalies, have current playbooks for rapid and effective response actions to counter detected attacks, and do not have to defend more cyber terrain than their resources can support.
- Network authorities implement effective password policies and practices that address password storage, reuse, and complexity to reduce opportunities for adversaries to masquerade as legitimate users.
- Defenders implement up-to-date configurations and timely patching of systems to remove known paths for access and exploitation.

- Network authorities implement authentication for use of externally accessible websites or place such websites in special network zones to minimize attack paths to better protect sensitive information.
- Network authorities implement segmented networks and matching of user privileges and services with operational needs. This reduces adversary access to restricted software and information, and forces adversaries to use more detectable tools and techniques.

The size and scope of cyberspace precludes defending everything, requiring operators and defenders to implement the concept of cyber key terrain. Cyber key terrain is the subset of information, networks, and devices within cyberspace upon which critical missions depend. Organizations must consider how sharing information with other organizations and networks outside of their direct control affects security, such as when sharing information in the joint and coalition environments. DOT&E observed instances where judicious selection and monitoring of cyber key terrain enabled defenders to focus their defensive efforts and prevent cyber adversarial teams from degrading critical missions.

Evolving Requirements for Cyber Tests and Assessments

It is good news that the DOD's cyber defenses are improving, especially in smaller networks, but it also highlights that the DOD must improve the cyber adversarial teams to realistically portray advanced cyber adversaries and continue driving cybersecurity improvements. Operational Test Agencies and DOD Red Teams must become capable of portraying cyber adversaries in accordance with known doctrine, tactics, and capabilities in both offensive and defensive operations.

Technical capability needs include:

- Non-Internet Protocol data transmission systems. The Services are developing tools and test capabilities for some non-Internet Protocol components, but some operational tests in FY17 had limitations related to needed tools and expertise.
- Supervisory control and data acquisition systems. Testing protocols are needed for components such as programmable logic controllers.
- Multiple spectrum cyber threats. More tools and expertise is needed to conduct cybersecurity tests using radio frequency, acoustic, and radar data.

The Service cyber Red Teams do not have the capacity to fully meet the demands for tests, assessments, and training exercises. This has resulted in an increasing number of operational test-related conflicts and delays. The Cyber Protection Teams (CPTs) include an element to assist in portraying a threat, but these elements do not possess the National Security Agency certification or skills required of a DOD Red Team operating on DOD networks. The DOD should provide resources to expand capacity and capabilities of DOD cyber Red Teams for more representative threat portrayal in exercise assessments and operational tests.

Cyber Protection Team Observations

CPTs encountered operational challenges in deploying and integrating with local defenders to defend networks assessed in large-scale training exercises.

- Some CPTs were understaffed and members had minimal operational experience with tools and operations.
- Some CPTs did not have the knowledge and experience on the intended networks to rapidly integrate with and supplement existing defenders.
- Some CPTs spent a disproportionate amount of time on local administrative requirements that reduced their dwell time working on the intended networks.

In a few cases, DOT&E observed network authorities attempting to offset these CPT shortfalls, for example:

- U.S. African Command (USAFRICOM) established an out-of-band connection between their headquarters enclave and their assigned CPTs at Fort Gordon, Georgia. This connection allows those teams to operate continuously on the USAFRICOM enclave, resulting in better network familiarity and mission support.
- The U.S. Navy plans to deploy teams of cyber defenders with major combatant ships, equipping them with a standard toolkit to rapidly detect abnormal activity on shipboard networks and capture data for analysis, forensics, and remediation.
- The U.S. Air Force plans to develop specialized cyber defenders to support specific operational mission areas.

DOT&E will continue to observe and record observations from the operational employment of the CPTs in assessed Combatant Command training exercises.

Confidence in Offensive Cyber Capabilities

Maturing the processes for planning and employing cyber fires is essential for cyber fires to become a more effective option for commanders. The synchronization and coordination of cyber fires with kinetic and non-kinetic effects continued to improve, with Combatant Commands exploring how to modify existing operational processes to match the operational characteristics of cyber fires. Assessments of operational processes during training exercises identified challenges from mismatches in terminology, differences in expectations for operational timelines for cyber and other fires, and delays associated with the level of approval and authorities required to employ offensive cyber capabilities.

In FY17, DOT&E performed a preliminary review of ongoing Service testing for offensive cyber capabilities, and identified some inconsistencies with OT&E methods and varying degrees of operational realism. DOT&E also noted that most testing performed by the Services does not include an opposing force or human element responsible for defending or maintaining the target of the offensive capability. Adversaries, through their responses, affect the scope and duration of cyber effects on systems they control; Services should include this element when testing capabilities for critical missions. The DOD should conduct appropriate operational testing of critical offensive

cyber capabilities to provide confidence in intended effects. DOT&E will continue to oversee operational testing of offensive capabilities and assess related processes to provide a complete operational perspective on the efficacy of cyber fires.

Persistent Cyber Operations

Threat-representative cyber activity is essential for operational tests, operational assessments, and realistic training. Although most test and training events are of relatively short duration (1 to 2 weeks), real-world adversaries have a much longer window to acquire access and prepare for potential cyber-attacks. Persistent Cyber Operations (PCO) authorities afford DOD-certified Red Teams the ability to perform longer-duration planning and network-access development that is more representative of an advanced, persistent cyber threat. In FY17, DOT&E continued engagement with U.S. Cyber Command to establish global standing ground rules to simplify and enable PCO elements to portray the threats needed for operationally realistic tests and training.

Assessments supported by PCO elements with U.S. Strategic Command, USPACOM, and USNORTHCOM in FY17 demonstrated the feasibility and value of having PCO to enable representative training and assessment events. PCO assessments also demonstrated the means to identify vulnerabilities that would otherwise have gone undetected, thereby increasing both the security of networks and warfighter preparation for cyber warfare. Standing ground rules will provide the foundation for expanding the presence and benefits of the PCO across the DOD. The DOD should implement authorities for global persistent cyber opposing force operations to be replicated on DOD networks.

Challenges for Coalition Operations in Cyberspace

The DOD expects to fight side-by-side with coalition partners in many scenarios, in many theaters. In scenarios where a cyber adversary is present, coalition operations may be degraded by the restrictions that preclude sharing knowledge of cyber-attacks, status of networks, and any information that involves a vulnerability on a U.S. network. These restrictions reduce the utility of coalition training and leave the U.S. and coalition partners ill-prepared to operate effectively in combined environments that are contested by a cyber adversary. Coalition networks often do not receive the same network defense support as other DOD networks, even though they are owned and operated by the DOD. The DOD should revise cyber classification guidance to enable effective cyber-related collaboration, training, and assessment with coalition partners.

DOT&E is helping prototype cyber-range environments that may help with coalition training. These environments could also assist in the demonstration of the effects of vulnerabilities and best practices, thereby improving the cybersecurity of coalition networks. The following section discusses these efforts in more detail.

Cyber Ranges and Executive Agents

For the last several years, DOT&E has advocated for a cyber range structure that supports both test and training requirements. Because of the similarity of functions in test and training, a common architecture across these ranges is needed to provide efficiency and flexibility to address the increasing demand for cyber range resources, and to effectively respond to rapidly evolving and increasingly sophisticated cyber threats.

The FY15 NDAA directed the DOD to establish an Executive Agent (EA) for cyber training ranges and an EA for cyber testing ranges, and required their collaboration to achieve a common architecture. In FY16, the DOD established the Army as the EA for training ranges and the Test Resources Management Center (TRMC) as the EA for test ranges. In the FY17 budget, the DOD allocated funds separately for a Persistent Cyber Training Environment (PCTE) and for cyber test ranges. More than two-thirds of the approximately $750 Million allocated for cyber ranges falls within the PCTE program element, which underscores the importance for dual-use capabilities.

DOT&E has engaged with the PCTE program to advocate for the acquisition of effective and suitable range capabilities, to collaborate in the development of a test and evaluation approach, and to encourage dual use across test and training ranges. DOT&E is also interacting with both EAs to promote clear understanding of requirements, common architectures, and standards.

In FY17, assisted by DOT&E funding and liaison, the Joint Staff J6 provided a representative command-and-control range environment and hosted tests and training for USPACOM and the Australian Defence Force during Talisman Saber 17. Hosted by USPACOM's Cyber War Innovation Center and the 613th Air Operations Center, the event constructed a distributed classified mission rehearsal platform for the Combined Air Operations Center and Joint Operations Center. This event helped meet key objectives for U.S. and Australian cyber defense teams and Red Teams to build relationships, conduct combined operations, hone technical skills, and exchange and build new tactics, techniques, and procedures. Teams participating in this exercise found the integration with joint and coalition forces to be invaluable.

Following an exercise assessment with USFK and South Korean forces, USFK leadership requested help in executing training and assessments with their coalition partner. DOT&E is working with USFK to develop a preliminary cyber-range environment where U.S. and South Korean forces may be able to train as a coalition force on matters of critical importance to operations in the cyber domain.

EFFECTIVE DEFENDER PRACTICES

The DOD's cyber defenses are improving. In FY15 and continuing through FY17, DOD cyber Red Teams in training exercises had more difficulty accessing and exploiting networks. Defenders must have good situational awareness of the network, and activity within the network, to properly react to an adversary and provide a successful defense. The following is a summary of best defender practices, which correlate to DOT&E observations of defenders successfully reacting to DOD cyber Red Teams.

Unity of Effort for Operations, Intelligence, and Cybersecurity

As in other warfare domains, successful cyber operations require unity of effort and integration across functional elements. Reactive defenses were most successful when commanders made cybersecurity and cyber operations a focus and priority similar to other operational domains, and when they were organized to coordinate both offensive and defensive activities, including cyber. Commands where cybersecurity was a high-interest item, and where Joint Cyber Centers have been established, were more successful countering activities by DOD Red Teams.

Successful reactive defenses used knowledge of operations and intelligence to prioritize areas of the network for enhanced monitoring based on strategic intelligence analysis regarding threat intent. DOT&E observed several cases where resources were prioritized to defend cyber key terrain and provide cyber defenders information to concentrate their efforts and tools to detect malicious activity.

Successful reactive defenses also integrated external resources to enhance local defenders. For example, augmenting local defenders with CPTs allowed more timely review of sensor alerts and logs to identify and investigate suspicious or malicious activities. CPTs have been effective network defense players where they have been well-trained or given opportunities to learn and operate on the networks they defend.

Span of Control

As discussed above, a fixed number of network defenders can only successfully defend a limited set of network assets; automated tools and sensors can only extend that reach so much. DOT&E observations confirm that local defenders typically experience more success with smaller and well-defined networks than with larger and more open networks. This observation is relevant to the Joint Information Environment, which the DOD is implementing and which may expand the span of control for network defenders beyond what is practical.

Experience and Proficiency

Networks defended by experienced personnel with proven proficiency more consistently hindered and challenged the DOD Red Teams. Network defenders must sort through data provided by sensors and detection devices to identify malicious actions from normal activity. DOT&E is increasingly observing proprietary tools developed by defenders (often best described as "skilled hobbyists") who create tools, build on their performance, and integrate them into their standard procedures.

It is critical to hire and retain skilled cyber personnel. Military personnel on timelimited duty rotations often lack the opportunity to acquire adequate cyber experience, or leave the DOD after achieving that experience. DOT&E observed that selective hiring and continuity of civilian and contractor personnel allowed local defenders to develop familiarity with the networks defended, recognize normal modes of operation, and better plan for abnormal activities.

DOT&E observed that some successful network defenders were able to identify indicators and warnings for likely threats. This enhanced their understanding of adversary tactics, techniques, and procedures to include how the sensors and network logs will record and report such activity. In some cases, defenders developed software scripts and signatures to detect and alert on suspicious indicators.

Commensurate Authorities

The cybersecurity defense structure within the DOD is built around three tiers of authorities and responsibilities, although the specific duties of each tier differ from location to location. Organizations demonstrating successful reactive defenses often deviated from the formal doctrine. In some locations, cybersecurity sensors provide data only to the non-local or regional tiers. However, local defenders tended to experience success when they had direct access to sensor feeds such as the Host-Based Security System on their networks to enable improved situational awareness at the tactical level. CPTs report that when their span of view of network sensors is widened, their ability to predict and anticipate anomalous activity improves. Organizations that maintain relationships with acquisition program offices for fielded systems in their area of responsibility can work directly with materiel suppliers to solve problems. Finally, local defenders having authority to implement selected response actions with minimal external coordination can lead to improved speed of defense.

Test and Evaluation Resources

Test and Evaluation Resources

Test and Evaluation Resources

Public law requires DOT&E to assess the adequacy of test and evaluation resources and facilities for operational and live fire testing. DOT&E monitors and reviews DOD- and Service-level strategic plans, investment programs, and resource management decisions so that capabilities necessary for realistic operational tests are supported. This report highlights areas of concern in testing current and future systems and discusses significant challenges, DOT&E recommendations, and T&E resource and infrastructure needs to support operational and live fire testing. FY17 focus areas include:

- Increased DOT&E Funding in the DOD Appropriations Act, 2017
- Army Support of OT&E
- Personnel to Support Cyber-related Operational Testing
- Threat Representation for OT&E of Space Systems
- High-Altitude Electromagnetic Pulse Test Capability
- Joint Strike Fighter Advanced Electronic Warfare Test Resources
- Point Mugu Sea Test Range Enhancements to Support OT&E of Air Warfare Programs
- Fifth-Generation Aerial Target
- Electronic Warfare for Land Combat
- Navy Advanced Electronic Warfare Test Resources and Environments
- Equipping a Self-Defense Test Ship for Aegis Combat System, Air and Missile Defense Radar, and Evolved Seasparrow Missile Block 2 Operational Testing
- Multi-Stage Supersonic Targets
- Torpedo Surrogates for Operational Testing of Anti-Submarine Warfare Platforms and Systems
- Submarine Surrogates for Operational Testing of Lightweight and Heavyweight Torpedoes
- Aircraft Survivability Equipment Test Capability Gaps
- Foreign Materiel Acquisition Support for T&E
- Tactical Engagement Simulation with Real Time Casualty Assessment
- Warrior Injury Assessment Manikin
- Test and Evaluation of Army Software-Defined Tactical Radios
- Range Sustainability

Increased DOT&E Funding in the DOD Appropriations Act, 2017

The FY17 appropriations act added $8 Million to the DOT&E budget for threat systems. The increased funding supported the following test capability enhancements:

- Development and demonstration of a prototype system to support threat electronic warfare (EW)-enabled cyber operations for laboratory and anechoic chamber T&E by collecting classified and open-source data on cyber electronic warfare (C/EW) threats, analyzing DOD and Service requirements for C/EW testing, and acquiring U.S.-targeted systems for lab test articles
- Development of a cyber cloud to address current intelligence analyst pitfalls
- Identification of gaps in the cyber threat library development process such as the lack of a standardized threat library structure across the cyber community and the absence of a centralized storage location for the cyber threat library
- Improved understanding of "wireless" cyber threats to support U.S. weapon systems testing
- Utilization of investments in U.S. weapon systems that blend cyber and EW capabilities comparable to threat T&E assets
- Support for test programs with documented C/EW threat shortfalls such as tactical communications; datalinks; radio communications; networking; data transportation; and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) sensors and systems
- Initiation of actions to evaluate growing and evolving cyber threat requirements and analyze the convergence of C/EW affecting the baseline required for operational testing
- Continued identification of initiatives to improve:
  - Cyberspace threat representation and prediction
  - Cyber-economic threats to DOD systems
  - Representative threat offensive and defensive cyber operations capabilities
  - Scalable cyberspace threat test environments that can interface with cyber test networks
- Continued efforts to maintain a standard set of threat performance models

This support helped DOT&E carry out its Title 10 responsibilities to assess test adequacy and promote common solutions to Service threat representation needs.

Army Support of OT&E

Beginning with the 2014 Annual Report, DOT&E expressed concern with the continued budget and staffing reductions at the Army Test and Evaluation Command (ATEC) and the office of the Army Test and Evaluation Executive. During the FY17 DOT&E review of the Army's T&E budget and resources, the Army indicated that the office of the Army Test and Evaluation Executive was understaffed to fulfill its mission and there would be further staffing reductions at the Army Evaluation

Center and Operational Test Command through FY19. The Army acknowledged that this may cause the inability to conduct simultaneous operational test events and increased costs to customers. Operational tests planned in 2018 that will overlap include Paladin Integrated Management, Joint Light Tactical Vehicle, and Stryker 30 mm and Stryker Common Remotely Operated Weapon Station – Javelin. Substantial growth in the areas of autonomy, EW, cybersecurity, and big data analysis continue to put new demands on the Army T&E workforce and infrastructure. In addition to staffing reductions, the Army must contend with competition from industry as it struggles to recruit, retain, and grow an analytically and technically competent workforce. The Army currently has four major studies ongoing that are intended to help inform T&E funding and staffing requirements. The Predictive Resource Staffing Model will become operational in December 2017 and is intended to support the planning of workforce requirements. DOT&E is concerned that these budget and staffing reductions may affect test planning, execution, and reporting and may result in delayed acquisition decisions. DOT&E will continue to monitor the Army T&E workforce regarding its capability and capacity to support the evaluations of Army acquisition programs.

Personnel to Support Cyber-related Operational Testing

Well-qualified personnel are essential to planning and executing adequate, threat-representative operational test events involving cybersecurity. The Service Operational Test Agencies (OTAs) and cyber Red Teams do not have enough experienced cybersecurity professionals to accommodate the increasing number and complexity of test events projected in FY18 and beyond.

Two recent changes in DOD cybersecurity test procedures drove the increasing demand for cyber test expertise. In July 2016, DOT&E issued a memorandum describing improvements needed in cybersecurity operational testing to adequately emulate an advanced nation-state threat. To meet the intent of the memorandum, OTAs and Red Teams need additional expertise in the areas of non-Internet Protocol data transmission, industrial control systems, and multi-spectrum cyber threats. Although the OTAs and Red Teams made progress filling these gaps during FY17, most OTAs still do not have the capability to execute adequate operational testing in these areas. In February 2017, USD(AT&L) issued a revision to DOD Instruction 5000.02 that requires operationally realistic cybersecurity testing during a program's developmental testing phases as well as during operational testing. This approach is critical to helping programs find and fix mission-critical cybersecurity vulnerabilities, but it draws upon OTA and Red Team cybersecurity experts to help plan and execute numerous developmental test events as well as operational test events.

In order to acquire and retain experienced cybersecurity test personnel, the Services should develop cyber expertise career options with incentives that are competitive with the private sector and other Federal agencies. The Services should also provide experienced cybersecurity test personnel with interesting, mission-critical work; many cyber experts find mission-critical work as rewarding as pay and benefits increases.

Threat Representation for OT&E of Space Systems

U.S. adversaries are actively pursuing offensive space control capabilities to diminish and overcome U.S. military space superiority, and thus threats to space systems are continually advancing. Although the Services normally test space systems against representative natural hazards and space phenomena, they have not adequately tested them against representative threats emulating a wartime environment. The OT&E of space systems must reflect all threats that U.S. space systems will face, and the Services should provide the additional resources required to ensure these threats are realistically represented and assessed during OT&E.

To achieve operational realism, the Service acquisition officials and OTAs should act in advance of OT&E to develop or procure those space threat resources. If acquisition and employment of actual threats is not practical, would violate U.S. or DOD policy, or would introduce unmitigated and unacceptable operational, security, or safety risks, then the Services should use realistic, accredited threat surrogates to include accredited threat models and simulations in lieu of the actual threat system.

To help ensure adequate testing of threat systems and threat surrogates against satellites for OT&E, the Services should fund pre-launch testing of either first articles or production-representative "test satellite" articles against all validated threats. Representative operational crews should operate satellites being threat tested for OT&E using the control segment and capabilities intended for operational employment. Post-launch, the Services should fund mission-representative articles through the operational life of space systems to support ground testing of those systems against an evolving threat; system of systems assessments; ongoing tactics, techniques, and procedures development; and exercises.

In a memorandum dated March 2016, DOT&E provided guidance to the Service acquisition officials and OTAs to improve their ability to identify and track space threat representation capabilities; identify space threat representation gaps, and request funding to fill those gaps; and to develop modeling and simulation (M&S) capabilities to support the assessment of space threats. DOT&E continues to enforce this guidance, requiring that all space system Test and Evaluation Master Plans (TEMPs) and test plans include the resources for realistic threat representation. The Services should use this guidance, and follow-on efforts such as the studies conducted in 2017 by the Threat Resource Management Center (TRMC) and the Air Force Director of Test and Evaluation, to resource adequate space threat test capabilities for all military space systems.

High-Altitude Electromagnetic Pulse Test Capability

Military Standard 4023 (MIL-STD-4023), "High-Altitude Electromagnetic Pulse (HEMP) Protection for Military Surface Ships," requires full-ship electromagnetic pulse (EMP) testing

to support surface vessel survivability assessments. In addition, because the DDG 51 Flight III destroyer is expected to be capable of operating in an EMP environment, section 407 of the DDG 51 Ship Specification establishes requirements for DDG 51 EMP Protection. Section 407 states that during the guarantee period of the ship, the government will conduct a full-ship EMP test to determine the performance of the ship's electronic systems under simulated EMP conditions.

The Navy does not have a capability to conduct a survivability assessment of a full ship subjected to EMP effects. Current Navy practice is to conduct limited testing on ship systems and sub-systems and then extrapolate these results to the entire ship. This testing method does not provide the data needed to adequately assess full ship EMP survivability at sea in an operational mode. Existing EMP M&S capabilities provide very limited information on ship survivability, with significant uncertainties.

In FY15, the OSD Chemical, Biological, Radiological, and Nuclear Survivability Oversight Group – Nuclear identified a full-ship EMP Threat Level Simulator (TLS) for warships as their most important test capability gap. The Tri-Service Technical Working Group, responsible for the development of MIL-STD-4023, agreed that a full-ship EMP TLS is required for warship EMP threat survivability assurance. The Defense Threat Reduction Agency also determined that testing using a full-ship EMP TLS is the best approach to demonstrate ship threat-level EMP protection and mission assurance in accordance with standing Navy requirements. Currently, surface vessel acquisition programs (e.g., DDG 51) have no plans to conduct a full-ship EMP test because the Navy has no capability to do so. In order to address this testing capability shortfall, in FY16 the Naval Sea Systems Command (NAVSEA) directed the Navy's EMP Program Office to develop a method using a Low-Level Continuous Wave Illuminator to conduct EMP testing on one to-be-determined test ship. Evaluation of this trial will help determine the way forward for development of a full-ship EMP TLS.

In conjunction with NAVSEA, the Defense Threat Reduction Agency estimated the costs to build a full-ship EMP TLS capability to be $49-54 Million. Once operational, the total cost to conduct nine tests is estimated at $17.5-18.6 Million. Full-ship EMP TLS testing at sea will support mission assurance by providing test data for EMP modeling and realistic EMP training scenarios for ship crews. At-sea testing using this capability will demonstrate full-ship EMP survivability and support the U.S. nuclear deterrent posture. DOT&E supports these efforts to address current EMP testing shortfalls as soon as possible.

Joint Strike Fighter Advanced Electronic Warfare Test Resources

In February 2012, DOT&E identified significant shortfalls in EW test resources – in particular surface-to-air threat representation on the open-air ranges, which resulted in nearly $500 Million of funding for the Electronic Warfare Infrastructure Improvement Program (EWIIP). EWIIP was intended to buy both open- and closed-loop threat ground radar emulators for the open-air ranges, provide corresponding upgrades to anechoic chambers and the Joint Strike Fighter (F-35) mission data file reprogramming lab, and provide intelligence products to support the development of the threat emulators.

Significant progress has been made in some instances, but is lacking in others. The open- and closed-loop threat emulators, in addition to the lab upgrades, are key to the development, testing, and timely fielding of numerous U.S. aircraft and airborne EW systems that are critical for prevailing against near-peer adversary threats. These aircraft and EW systems include the F-35, F-22 Increment 3.2 A/B, B-2 Defensive Management System, Long Range Strike Bomber, and the Next Generation Jammer for the EA-18G. The status of various components of the EWIIP effort is displayed in Table 1.

DOT&E championed an effort that resulted in $172 Million of additional funding for the Services for additional range infrastructure for testing, training, and readiness of U.S. aircraft and airborne EW systems. This funding will enable test ranges and M&S (that must be validated with test data) to assess the performance of U.S. systems against near-peer threat air-defense networks of the 2020s. These capabilities include conventional radars with advanced digital signal generation and processing, networked together via advanced track fusion processing systems; multi-static radar networks; passive detection systems; and passive coherent radars. The proposed enhancements are constrained to materiel solutions that can be procured rapidly and off the shelf where possible in order to be available for testing of critical systems such as the Next Generation Jammer.

TABLE 1. RECOMMENDATIONS ON ELECTRONIC WARFARE TEST RESOURCES	
DOT&E Recommendation	**Current Status**
Develop a combination of open- and closed-loop ground radar emulators in the numbers required for operationally realistic open-air range testing of the Joint Strike Fighter (F-35) and other systems beginning in 2018.	EWIIP was scheduled to deliver the first 2 open-loop systems (called Radar Signal Emulators (RSEs)) in 2016, 12 systems in 2017, and the final 2 in early 2018, for a total of 16 RSEs – in time to support F-35 IOT&E and other testing in 2018 and beyond. All 16 are on track to deliver by March 2018. Acceptance and integration testing is underway and on track to support F-35 IOT&E spin-up; this testing will establish procedures for use of RSEs in the F-35 IOT&E and provide validation data for accreditation of the systems for use in OT&E. Two closed-loop systems are in development but are not scheduled to be available until mid-to-late 2019, after completion of the planned F-35 IOT&E. The integration architecture developed for the open-loop RSE systems will provide adequate test capabilities for F-35 Block 3F IOT&E in lieu of closed-loop systems.
Upgrade the government anechoic chambers with adequate numbers of signal generators for realistic threat density.	Initial studies of materiel solutions to achieve realistic densities have begun. • The Navy chamber has procured improved interim signal generation capabilities and initial test support equipment for direct signal injection capability for the F-35. The Navy chamber executed F-35 electronic warfare testing for compliance and simulation validation in September and October 2016. The facility introduced a more substantial upgrade in the summer of 2017 that will allow high-fidelity replication of very high signal density threat environments. • The Air Force chamber has completed one stage of hardware upgrades, improving its ability to replicate high signal density environments, and has identified a path forward covering more extensive upgrades through 2020.
Upgrade the F-35 mission data file reprogramming facility, known as the U.S. Reprogramming Laboratory (USRL), to include realistic threats in realistic numbers.	An F-35 Program Office-sponsored study to determine upgrade requirements for the USRL was completed in December 2014. It confirmed the shortfalls identified by DOT&E in February 2012 and identified many other critical shortfalls preventing effective and efficient mission data file development and reprogramming. Delays since completion of the study have pushed the schedule for upgrades beyond Block 3F IOT&E and fielded operations. Additionally, the program intends to procure fewer signal generators than the study recommended, further jeopardizing the program's ability to generate effective mission data in the future. Hardware and software changes planned for F-35 follow-on modernization will require a significant redesign of the USRL. The point by which the USRL follow-on modernization requirements must be defined to support long lead time equipment purchases is fast approaching. DO&TE is unaware of any formal planning activities that have been conducted for the USRL upgrades required to support follow-on modernization.
Provide Integrated Technical Evaluation and Analysis of Multiple Sources intelligence products needed to guide threat simulations.	Products have been delivered and are being used to support development of the open- and closed-loop threat radar emulators.

Point Mugu Sea Test Range Enhancements to Support OT&E of Air Warfare Programs

In 2015 and 2016, DOT&E and USD(AT&L) allocated $22 Million to fund integration of the Air Warfare Battle Shaping (AWBS) system and the open-loop Radar Signal Emulators (RSEs) at Point Mugu Sea Test Range (STR), California. AWBS is a variant of the Air-to-Air Range Instrumentation system at the Air Force Western Test Range (WTR), Nevada, where it is used for scoring and post-mission reconstruction and analysis of OT&E missions. Use of RSEs at the STR for the F-35 IOT&E will provide operationally realistic scenarios and lessen some of F-35 IOT&E trials at the WTR. Additionally, conducting test trials at the STR could shorten the duration of F-35 IOT&E.

In 2016, Navy and Air Force personnel participated in RSE range integration working groups and, together with DOT&E, observed initial acceptance testing of the first two RSEs. Navy personnel are currently undergoing training for RSE operation, maintenance, and programming. Two RSEs will be temporarily transferred from the Nevada Test and Training Range (NTTR) to the STR during 2017 and early 2018 to complete integration testing at the STR. At the outset of F-35 IOT&E, all 16 RSEs will be stationed at NTTR for F-35 IOT&E trials. Once those scenarios are completed, 12 RSEs will move to the STR for additional F-35 IOT&E trials.

Fifth-Generation Aerial Target

DOT&E has been investigating the means to develop a full scale aerial target to adequately represent the characteristics of fifth-generation threat aircraft. The Fifth-Generation Aerial Target (5GAT) study effort began in 2006 and examined the design and fabrication of a dedicated 5GAT that would be used

in the evaluation of U.S. weapon systems effectiveness. The 5GAT team – comprised of Air Force and Navy experts, retired Skunk Works engineers, and industry experts – completed the preliminary design in 2016. The fully owned Government design includes the aircraft outer mold line, internal structures, loads analysis, propulsion, and subsystems. The 5GAT effort is currently building the first of two demonstration prototypes, including flight propulsion, system integration, and flight simulation/verification activities. The team built one full-scale, flight-representative wing that will be used for structural load tests and a system integration laboratory, as well as a full scale test article for radar cross-section testing. The DOD provided additional funding in FY18-19 to complete the final design, tooling, fabrication, and flight tests (FY19) and to build a second prototype. The prototyping effort will provide cost-informed alternative design and manufacturing approaches for future air vehicle acquisition programs, and verified cost data for all-composite aircraft design/development, alternative tooling approaches, and innovative management applications. The 5GAT effort can also be used to assist with future weapon system design/development, planning and investment, and future analysis of alternative activities. It will also demonstrate reduced signature, basic aerodynamic performance, alternative cost models for aircraft development, and provision for special mission systems.

Electronic Warfare for Land Combat

The Army's Mission Command Network is a key enabler that supports mission execution across the Brigade Combat Team (BCT). Integrated network systems including mobile satellite, digital radio, and mission command applications are distributed throughout a combat formation and its support elements, from the brigade command posts down to the individual dismounted soldier. The Army intends commanders to have rapid access to the information needed to complete their mission and to have the ability to transfer information such as voice, video, text, position location information, and high-resolution photographs throughout the BCT. The expanded use of radio frequency (RF)-based networks expose the BCT to contemporary EW threats, including electronic support (ES) and electronic attack (EA) capabilities. Recent conflicts have demonstrated the paralyzing effects that EW can have on the modern battlefield. As the Army becomes more dependent on RF-based network technologies, it is critical that the developmental and operational test communities continue to identify and assess their vulnerabilities. Decision-makers must understand the inherent vulnerabilities and the ways an enemy may choose to exploit and/or degrade the tactical network.

During operational testing, threat EW is part of a broader combat force that is made available to the opposing force (OPFOR) commander. When possible, the EW systems, tactics, techniques, and procedures employed by the OPFOR during test should represent those of potential adversaries. The Threat Systems Management Office (TSMO) is responsible for developing, operating, and sustaining the Army's suite of threat EW capabilities. There is a gap in the Army's ability to perform ES in higher frequency bands, which TSMO is addressing through the Advanced Networked Electronic Support Threat Sensors project. TSMO has demonstrated a continued commitment to providing realistic threat EW for operational test and mitigating limitations when possible. Because these developing threat test capabilities support increased operational realism in testing, they are critical to support future testing of Warfighter Information Network – Tactical Increment 2, Nett Warrior/Leader Radio, Manpack Radio, Joint Battle Command – Platform, and Assured Positioning Navigation and Timing.

Navy Advanced Electronic Warfare Test Resources and Environments

Improving Capability to Realistically Represent Multiple Anti-Ship Cruise Missile (ASCM) Seekers for Surface Electronic Warfare Improvement Program (SEWIP) Operational Testing

A gap in the ability to realistically represent multiple ASCM seekers during test was initially identified in the DOT&E FY13 Annual Report as "Additional Electronic Warfare Simulator Units for Surface Electronic Warfare Improvement Program (SEWIP) Operational Testing." The Navy subsequently developed a programmable seeker simulator that could represent different ASCM seekers by specifying electronic waveform emission characteristics for one of several possible threats. However, the effective radiated power (ERP) was not among those characteristics, resulting in simulated attacks by ASCM representations displaying disparate levels of ERP that are unlikely to be encountered during a stream raid attack of two ASCMs (along the same bearing and elevation and within close proximity of one another). The programmable seeker simulator, termed the "Complex Arbitrary Waveform Synthesizer," should be modified such that its ERP more realistically represents the second ASCM of a dual ASCM stream raid.

The next SEWIP Block 2 OT&E is projected for FY19, to be followed by FOT&E on a Product Line Architecture-compliant DDG 51 with Block 2 integrated with the Aegis Combat System. This integration was not part of the Block 2 IOT&E. Subsequent FOT&E is intended with the DDG 1000 destroyer and CVN 78 aircraft carrier combat systems. The estimated cost to add the ERP improvement is $5 Million.

Improving the Fidelity of ASCM Seeker/Autopilot Simulators for Electronic Warfare Testing

DOT&E initially identified a gap in the fidelity of ASCM seeker/autopilot simulators in the FY13 Annual Report. The gap arose because of continued reliance on manned aircraft for captive-carry of ASCM seeker simulators. Captive-carried simulators can neither demonstrate a kinematic response to EA by SEWIP Block 3 nor demonstrate the effect that such kinematic responses will have on ships' hard-kill systems (e.g. missiles, guns). Manned aircraft fly too high and too slowly for credible ASCM representation and are unable to perform ASCM maneuvers. Credible ASCM representation requires a vehicle that can fly at ASCM speeds and lower altitudes than the current Learjets; can home on a platform representing a SEWIP Block 3-mounted

ship, using a threat-representative radar seeker and autopilot; and can respond realistically to Block 3 electronic jamming. Currently, discrete combat system components are tested as a subset of the integrated combat system, leaving integrated combat system capability unknown. SEWIP Block 3 IOT&E is projected for FY21 on a DDG 51-class ship. FOT&E of SEWIP Block 3 integrated with the CVN 78 combat system should occur subsequent to the IOT&E.

Developing Test Surrogates for Hostile Airborne and Surface Radar Systems

In addition to the ASCM surrogates described above, adequate operational testing of active EA systems like SEWIP Block 3 requires development of threat airborne and surface (e.g., coastal defense) radars that active EA systems may be required to thwart. The Navy tests such capababilities at the Shipboard Electronic Systems Evaluation Facility (SESEF). At SESEF, the Navy uses a pulse generator, known as the Combat Electromagnetic Environment Simulator (CEESIM), an amplifier, and an antenna to emulate hostile radars. Such test facilities provide some capability to demonstrate an electornic warfare system's ability to detect and identify threat radars, but the existing capability is not adequate to test EA systems. To test such systems, the threat radar surrogate should better emulate the RF aspects of the threat radar, the signal processing of the radar, and the electrnonic protection aspsects of the radar. On October 20, 2016, DOT&E directed the Navy to develop such threat radar surrogates. Without such test assets, it is unclear how the Navy will credibly test active EA systems like SEWIP Block 3.

Equipping a Self-Defense Test Ship for Aegis Combat System, Air and Missile Defense Radar, and Evolved Seasparrow Missile Block 2 Operational Testing

The close-in ship self-defense battlespace is complex and presents a number of challenges. For example, this environment requires:

- Weapon scheduling with very little time for engagement
- The combat system and its sensors to deal with debris fields generated by successful engagements of individual ASCMs within a multi-ASCM raid
- Rapid multi-salvo kill assessments for multiple targets
- Transitions between Evolved Seasparrow Missile (ESSM) guidance modes
- Conducting ballistic missile defense and area air-defense missions (i.e., integrated air and missile defense) while simultaneously conducting ship self-defense
- Contending with stream raids of multiple ASCMs attacking along the same bearing, in which directors illuminate multiple targets (especially true for maneuvering threats)
- Designating targets for destruction by the Close-In Weapons System (CIWS)

Multiple hard-kill weapon systems operate close-in, including the Standard Missile 2, the ESSM, and the CIWS. Soft-kill systems such as the Nulka MK 53 decoy launching system also operate close-in. The short timelines required to conduct successful ship self-defense place great stress on combat system logic, combat system element synchronization, combat system integration, and end-to-end performance.

Navy range safety restrictions prohibit close-in testing on a manned ship because targets and debris from successful intercepts will pose an unacceptable risk to the ship and personnel at the ranges where these self-defense engagements take place. These restrictions were imposed following a February 1983 incident on USS *Antrim* (FFG 20), which was struck with a subsonic BQM-74 aerial target during a test of its self-defense weapon systems, killing a civilian instructor. The first unmanned, remotely controlled self-defense test ship (SDTS) – ex-USS *Stoddard* – was put into service that same year. A similar incident occurred in November 2013, when two sailors were injured when an aerial target struck USS *Chancellorsville* (CG 62) during a test of its combat system. The *Chancellorsville* incident underscores the inherent dangers of testing with manned ships in the close-in battlespace.

The investigation into the *Chancellorsville* incident caused the Navy to rethink how it will employ subsonic and supersonic aerial targets near manned ships. The Navy has always considered supersonic ASCM targets high risk to safety and will not permit flying them directly at a manned ship. The Navy has invested in a seagoing, unmanned, remotely-controlled test asset (the SDTS) and is using it to overcome these safety restrictions. The Navy is accrediting a high-fidelity M&S capability – utilizing data from the SDTS as well as data from manned ship testing – so that a full assessment of the self-defense capabilities of non-Aegis ships can be completely and affordably conducted. The Navy recognizes that the SDTS is integral to the test programs for certain weapons systems (the Ship Self-Defense System, Rolling Airframe Missile Block 2, and ESSM Block 1) and ship classes (LPD 17, LHA 6, Littoral Combat Ship, LSD 41/49, DDG 1000, and CVN 78). However, it has not made a similar investment in an SDTS equipped with an Aegis Combat System, Air and Missile Defense Radar (AMDR), and ESSM Block 2 for adequate operational testing of the DDG 51 Flight III destroyer self-defense capabilities. The current SDTS lacks appropriate sensors and other combat system elements to test these capabilities.

On September 10, 2014, DOT&E submitted a classified memorandum to USD(AT&L) with a review of the Design of Experiments study by the Navy Program Executive Office for Integrated Warfare Systems. The Navy study attempted to provide technical justification to show that an Aegis-equipped SDTS was not required to adequately assess the self-defense capability of the DDG 51 Flight III class destroyers. DOT&E found that the study presented a number of flawed justifications and failed to make a cogent argument for not using an Aegis-equipped SDTS for operational testing.

On December 10, 2014, the Deputy Secretary of Defense (DEPSECDEF) issued a memorandum directing the Director of Cost Assessment and Program Evaluation (CAPE) to identify viable at-sea operational testing options that meet DOT&E adequacy requirements and to recommend a course of action

(with cost estimates, risks, and benefits) to satisfy testing of the AMDR, Aegis Combat System, and ESSM Block 2 in support of the DDG 51 Flight III destroyer program. The CAPE study evaluated four options to deliver an at-sea test platform adequate for self-defense operational testing. Each option required funding beginning in FY18 to support operational testing of these systems in FY22.

On February 10, 2016, the DEPSECDEF directed the Navy to adjust funds within existing resources to procure long lead items to begin procurement of an SDTS equipped with the Aegis Combat System and AMDR. He further directed the Navy to work with DOT&E to develop an integrated test strategy for the DDG 51 Flight III, AMDR, Aegis Modernization, and ESSM Block 2 programs. The DEPSECDEF required the Navy to document that strategy in draft TEMPs for those programs and submit them to DOT&E by July 29, 2016. The Navy has not complied with the direction to provide an integrated test strategy or TEMPs for those programs. Despite initially budgeting for long lead AMDR components, the Navy did not program funding in the Future Years Defense Plan to complete other activities and equipment required to modify the SDTS to support adequate operational testing of the self-defense capabilities of the DDG 51 Flight III, AMDR, and ESSM Block 2 in FY23 as planned. The Navy subsequently removed funding for the long-lead AMDR components.

On November 21, 2016, the DEPSECDEF directed the Navy to fully fund the Aegis SDTS and aerial targets required for testing the DDG 51 Flight III, AMDR, and ESSM Block 2 programs. The Navy initially complied with the direction but subsequently removed all funding for the Aegis SDTS and aerial targets.

On May 4, 2017, the DEPSECDEF directed the Navy to reinstate funding for the Aegis SDTS and associated test firings in compliance with the November 21, 2016, guidance. DOT&E continues to recommend equipping an SDTS with capabilities to support Aegis Combat System, AMDR, and ESSM Block 2 OT&E to test ship self-defense systems' performance in the final seconds of the close-in battle and to acquire sufficient data to validate ship self-defense performance M&S.

Multi-Stage Supersonic Targets

The Navy initiated a $297 Million program in 2009 to develop and produce an adequate multi-stage supersonic target (MSST) required for adequate operational testing of Navy surface ship air-defense systems. The MSST is critical to the DDG 1000, CVN 78, DDG 51 Flight III destroyer, LHA(R), AMDR, Ship Self-Defense System, Rolling Airframe Missile Block 2, and ESSM Block 2 operational test programs. The MSST underwent restructuring and rebaselining from 2013 – 2015 in order to address technical deficiencies as well as cost and schedule breaches, which would have postponed its Initial Operational Capability (IOC) to 2020 and increased the total program cost to $962 Million. Based on the restructured/rebaselined MSST program's high cost and schedule delays, as well as new intelligence reports, the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN(RDA)) in 2014 directed that alternatives be examined to test against these ASCM threats and subsequently terminated the MSST program. While the details of the final Navy alternative are classified, DOT&E determined that it would be very costly (the Navy estimates $739 Million), very difficult to implement, dependent on the results of highly segmented tests, and would suffer from severe artificialities that would confound interpretation of test results. DOT&E informed the Navy that the proposed alternative was not adequate for operational testing and recommended that the Navy not pursue it. MSST aerial target capabilities are still required to complete end-to-end operational testing of Navy surface ship air-defense systems and to validate M&S capabilities for assessing the probability of raid annihilation for Navy ships.

Torpedo Surrogates for Operational Testing of Anti-Submarine Warfare Platforms and Systems

Operational testing of anti-submarine warfare (ASW) and torpedo defense-related systems for all Navy and Navy support ships includes the ability to detect, evade, counter, and/or destroy an incoming threat torpedo. The determination of system or platform performance is dependent on a combination of the characteristics of the incoming torpedo (e.g., dynamics, noise, sensors, logic, etc.). Due to differences in technological approach and development, U.S. torpedoes are not representative of many highly proliferated torpedoes, particularly those employed in anti-surface warfare (ASuW) by other nations. The need for threat-representative torpedo surrogates to support operational testing is detailed in DOT&E memoranda to the ASN(RDA) dated January 9, 2013, and June 18, 2015. Acquisition programs that require threat torpedo surrogates for future operational testing include: *Virginia* and *Columbia* class submarines, *Zumwalt* class destroyer, AN/SQQ-89 surface ship ASW combat system, Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI) submarine sonar system, and Navy Torpedo Warning System and Countermeasure Anti-torpedo Torpedo acquisitions systems. Based on the 2014 Naval Undersea Warfare Center (NUWC) Division study, the Navy has taken the following actions to address the gaps in threat representation of torpedo surrogates:

- NUWC Division Keyport commenced a prototype technology development project that is expected to deliver a threat-representative, high speed quiet propulsion system. This effort was funded as an FY16 Resource Enhancement Program project at approximately $1 Million. This project experienced cost and schedule overruns and will complete within the following project, General Threat Torpedo (GTT).
- NUWC Division Keyport is pursuing development of a GTT that will complete development of the high-speed quiet propulsion system prototype and provide threat-representative tactics and countermeasure logic. The GTT project is funded as a Resource Enhancement Program for FY17 with funding of approximately $6.2 Million. DOT&E expects the GTT to fill in many of the gaps in threat representation of torpedo surrogates, however DOT&E remains concerned

that cavitation-generated noise may not be reprentative at ASuW depths. The ability of a successfully developed GTT to adequately support operational testing futher depends on future Navy decisions to procure a sufficient quantity of GTT and achievement of threat representative cavitation noise.

Submarine Surrogates for Operational Testing of Lightweight and Heavyweight Torpedoes

The Navy routinely conducts in-water operational testing of lightweight and heavyweight ASW torpedoes against manned U.S. Navy submarines. Although these exercise torpedoes do not contain explosive warheads, peacetime safety rules require that the weapons run above or below the target submarine with a significant depth to avoid collision. While this procedure allows the torpedo to detect, verify, and initiate homing on the target, it does not support assessment of the complete homing and intercept sequence. One additional limitation is the fact that U.S. nuclear attack submarines may not appropriately emulate the active target strength (sonar cross-section) of smaller threats of interest, such as diesel-electric submarines. During the MK 50 lightweight torpedo operational test in May 1992, the Navy conducted some limited set-to-hit testing against manned submarines, which included impact against the target hull, but that practice has been discontinued.

In preparation for the 2004 MK 54 lightweight torpedo operational test, DOT&E supported the development and construction of the unmanned Weapon Set-to-Hit Torpedo Threat Target (WSTTT) using Resource Enhancement Project funding. The WSTTT was a full-sized steel mock-up of a small diesel-electric submarine, with an approximate program cost of $11 Million. As a moored stationary target, the WSTTT could not emulate an evading threat, but its use in the MK 54 operational test demonstrated the value of such a dedicated resource. Unfortunately, the Navy did not properly maintain the WSTTT and abandoned it on the bottom of the sea off the California coast in 2006. In subsequent years, the Navy was able to make some limited use of the WSTTT hulk as a bottomed target for torpedo testing.

In a separate effort, the Navy built the Mobile Anti-Submarine Training Target (MASTT), designed to serve as a mini-submarine (SSM) sized threat surrogate for use in training by surface and air ASW forces. The Chief of Naval Operations initiated the program in 2010 with the goal of achieving operational capability by late 2011. An engineering assessment of the MASTT reveales the surrogate cannot be used as a set-to-hit target for torpedo testing. After 5 years and an expenditure of approximately $15 Million, the Navy started using the MASTT in limited search training. The Navy resisted design input from the operational test community and made it clear that the MASTT was not intended to support torpedo testing.

In support of a 2010 Urgent Operational Need Statement, the Navy funded the construction of the Steel Diesel-Electric Submarine (SSSK), a SSM-sized, moored, set-to-hit target consisting of an open steel framework with a series of corner reflectors to provide appropriate sonar highlights. This surrogate does provide a basic sonar signature. The Navy used the SSSK as a target for the MK 54 torpedo in a 2011 Quick Reaction Assessment and 2013 FOT&E. As part of the TEMP approval for the latter, DOT&E sent a memorandum indicating that the Navy must develop an appropriate mobile target to support future MK 54 testing.

Since early 2013, DOT&E has participated in a Navy working group attempting to define the requirements for a mobile set-to-hit torpedo target. The group has identified a spectrum of options and capabilities, ranging from a torpedo-sized vehicle towing a long acoustic array to a full-sized submarine surrogate. At the very least, the target is expected to be capable of mobile depth changes and high speeds, autonomous, and certified for representative lightweight torpedo set-to-hit scenarios. More advanced goals might include realistic active and passive sonar signatures to support ASW search, and reactive capability to present a more realistically evasive target. Cost estimates range from under $10 Million for a towed target to over $30 Million for a SSM-sized submarine simulator.

Aircraft Survivability Equipment Test Capability Gaps

Aircraft Survivability Equipment (ASE) is an integral part of military fixed- and rotary-wing platforms. ASE provides aircraft and crew protection and is vital to mission effectiveness in hostile environments. T&E resources, such as foreign threat systems, threat system surrogates, and M&S are needed to effectively evaluate ASE. However, acquiring enough actual threat systems for testing is not always possible. Threat surrogates and M&S require high fidelity information along with intelligence on the actual threats to be able to replicate them accurately. To achieve this, one of DOT&E's objectives is to improve the fidelity and consistency of threat representations and M&S at T&E facilities while reducing overall test costs.

DOT&E has taken the initiative to meet these challenges through various means. DOT&E and the TRMC co-led the Infrared Countermeasure Test Resource Requirements Study (ITRRS), which identified shortfalls in infrared countermeasure (IRCM) testing and developed a prioritized IRCM investment roadmap of projects to mitigate current testing shortfalls. DOT&E, in conjunction with TRMC, is developing a T&E Threat M&S capability/investment roadmap. This comprehensive roadmap will address threat M&S investment needs for both infrared (IR) and RF threats, ensuring adequate evaluation of airborne combat systems. Both roadmaps recommend that programs address EW test capability gaps.

M&S and threat representative systems require accurate data be collected to characterize threats. DOT&E works with both the intelligence and T&E communities to gather threat information and develop test equipment such as the Joint Standard Instrumentation Suite (JSIS) to characterize threat systems that can be used to increase the fidelity of M&S and threat representations. However, the requirements to collect all threat

data have historically been underfunded to a considerable degree, leaving substantial capability gaps in ASE testing.

Throughout the T&E process, M&S representations of threat systems have been used when the actual threat components have limited availability or are not available at all. M&S representations of threat systems also support testing when flight safety precludes live fire testing (i.e., missile launches against manned aircraft). For example, test programs may only conduct 10-20 live missile firing events; whereas, using a threat model or simulation, a test program may extend those results across a broader range of test conditions with different threats, ranges, altitudes, aspect angles, atmospheric conditions, and other variables affecting weapon system performance. Moreover, M&S representations can provide a more complete assessment of a system's operational performance than is possible using open-air facilities alone. However, as models fill a larger role within T&E and new requirements are leveraged on them, significant capability gaps exist in some M&S. Some do not have the appropriate fidelity while other M&S instantiations of the same threat(s) may produce different results.

To help close this gap, DOT&E's T&E Threat Resource Activity (DOT&E/TETRA) provided DOT&E-funded, standardized, and authoritative threat M&S to multiple T&E facilities operated by the Army, Navy, and Air Force. During FY17, DOT&E/TETRA provided over 140 IR threat models to the T&E community. The Services integrated and used this threat M&S to support ASE testing. Furthermore, DOT&E/TETRA developed a T&E Threat M&S Configuration Management System and an M&S Configuration Control Board (CCB) process to implement configuration control and distribution management for threat M&S to ensure model consistency and integrity among various T&E facilities. The management system provides mechanisms to identify and correct anomalies between a threat and its M&S representation. It also assists in controlling model configuration changes, maintains critical documentation such as interface control and validation documents, and provides updated threat models to multiple T&E facilities for developmental and operational T&E requirements. The T&E Threat M&S CCB, comprised of representatives from the T&E and intelligence community, prioritizes existing threat M&S developments and changes to ensure updates are provided efficiently and with minimal effect to T&E user facilities. As of this publication, DOT&E is expanding the CCB role. To successfully bridge this capability gap for RF and IR, additional funding is required to assure consistent and accurate results across the board, and to stay linked with evolving T&E M&S needs that can ultimately reduce T&E costs and time.

A high priority project on the ITRRS list is the ability to measure threat signature data for the development or improvement of the threat models for IR-guided missiles and unguided hostile fire munitions used for the T&E of ASE. These signature models drive a large number of T&E simulation tools. The DOT&E's Center for Countermeasures (the Center) is the executing activity for the JSIS project. JSIS is a Central T&E Investment Program (CTEIP) Resource Enhancement Project designed to mitigate the threat signature data gap, as well as provide ground truth for live fire missile and hostile fire tests for IRCM system testing. At IOC, JSIS will support Advanced Threat Warner (ATW) and the Common Infrared Countermeasures (CIRCM) operational testing. JSIS can be deployed to static live fire venues outside the continental United States, where opportunities exist to measure and collect data for threat assets that are either not available or of insufficient quantities, domestically.

However, the JSIS IOC capability only partially addresses the needs identified by the ITRRS study. For example, it will not provide the capability to measure missile attitude information for the entire missile fly out, nor does the JSIS IOC capability meet all needs related to signature collection fidelity (e.g., frame rates and resolution). Full Operational Capability (FOC) is required to meet all the needs of the Army's CIRCM program, the Navy's ATW program, the Air Force's Large Aircraft Infrared Countermeasure (LAIRCM) program, and the Naval Research Laboratory's Distributed Aperture Infrared Countermeasure (DAIRCM) program. JSIS FOC is needed to collect signature data in support of T&E of advanced IRCM systems, currently in development, that operate in other wavelength bands. However, to do this, JSIS will require additional investment to close this IRCM T&E gap.

Similarly, the ITTRS roadmap has designated projects to address gaps for ground-based missile plume simulators; airborne missile plume simulators; hardware-in-the-loop test facilities; installed system test facilities; surrogate threat missiles; instrumentation suites; open-air test range improvements; and threat system acquisition and storage. Following is a list of these projects:

- Upgrades to both open-air test ranges and indoor test facilities needed to test the latest missile warning systems and IRCM
- Open-air test range improvements that include additional firing points for multi-threat environments and angular separation, upgrades to improve test efficiency, improved instrumentation, and jitter and atmospheric distortion measurement capability
- Upgrades to hardware-in-the-loop and installed system test facilities to better represent the latest threats in an operational simulated environment
- Expansion to heavily-utilized, hardware-in-the-loop, and installed system test facilities to better meet program test schedules
- Increased dynamic range and fidelity for ground-based missile plume simulators to expand their testing envelopes
- Improved surrogate threat missiles to support open-air testing
- Increased cooperation among the military and intelligence agencies to collect more threat systems
- Threat system storage facilities to store actual threats as they become available

The DOT&E threat RF M&S study collected, analyzed, and presented information regarding the design, distribution, integration, and use of RF-related threat M&S across multiple organizations and the Services. The RF study provided a consolidated list of authoritative threat models developed by the Intelligence Production Centers (IPCs). The RF study team surveyed subject matter experts at the IPCs and T&E facilities to

determine common concerns with the implementation of M&S for T&E. The RF study provided the following preliminary top level list of capability gaps to stakeholders for T&E M&S improvements:

- Improve threat M&S management and infrastructure
- Develop new threat models and update threat models for T&E scalability
- Improve multi-spectral signatures and RF data
- Improve threat M&S characterizations for T&E

Foreign Materiel Acquisition Support for T&E

DOT&E is responsible for ensuring U.S. weapons systems are tested in realistic threat environments. Use of actual threat systems and foreign materiel to create realistic threat environments in testing supports DOT&E's ability to determine a system's operational effectiveness in a combat environment. To acquire test capabilities, DOT&E/TETRA develops an annual prioritized list of foreign materiel required by upcoming operational tests. These requirements are submitted to the Defense Intelligence Agency (DIA) Joint Foreign Materiel Program Office and are consolidated with Service requirements to drive Service and Intelligence Community collection opportunities. DOT&E coordinates with the Department of State to identify other opportunities to acquire foreign materiel for use in OT&E.

Foreign materiel requirements span all warfare areas, but DOT&E continues to place a priority on the acquisition of Man-Portable Air Defense Systems (MANPADS) and Anti-Tank Guided Missiles (ATGMs). Foreign MANPADS are needed to address significant threat shortfalls that affect testing for IRCM programs like CIRCM, LAIRCM, and Department of the Navy (DON) LAIRCM. For some programs, a large quantity of MANPADS is required – for development of threat M&S, for use in hardware-in-the-loop laboratories, and for LFT&E, to present realistic threats to IRCM equipment. Using actual missiles and missile seekers aids evaluators in determining the effectiveness of IRCM equipment. Foreign ATGMs are required to support the testing of the Expedited Active Protection System.

Traditional sources have been fully consumed, and there is a critical need to identify and develop new sources and opportunities for acquiring foreign materiel. Foreign materiel acquisitions are usually very lengthy and unpredictable, making it difficult to identify appropriate year funding. Programs have funded as much as $60 Million a year for acquisition opportunities that arise. DOT&E recommends a no-year or non-expiring funding line for foreign materiel acquisitions, funded at a level of $10 Million per year.

Tactical Engagement Simulation with Real Time Casualty Assessment

Realistic operational environments and a well-equipped enemy intent on winning are fundamental to the adequate operational test of land and expeditionary combat systems. Force-on-force battles between tactical units represent the best method of creating a complex and evolving battlefield environment for testing and training. This environment causes commanders and soldiers to make tactical decisions and react to the real-time conditions on the battlefield. Tactical Engagement Simulation with Real Time Casualty Assessment (TES/RTCA) systems integrate live, virtual, and constructive components to enable these simulated force-on-force battles, and provide a means for simulated engagements to have realistic outcomes based on the lethality and survivability characteristics of both the systems under test and the opposing threat systems. TES/RTCA systems must replicate the critical attributes of real-world combat environments, such as direct and indirect fires, IEDs and mines, and simulated battle damage and casualties. TES/RTCA systems must record the time-space position information and firing, damage, and casualty data for all players in the test event as an integrated part of the test control and data collection architecture. Post-test playback of these data provide a critical evaluation tool to determine the combat system's capability to support soldiers and marines as they conduct combat missions.

New and upgraded ground combat vehicles are incorporating improved conventional armor, Active Protection Systems, and advanced weapons. These modern developments, as well as upgrades to threat vehicles, should be integrated into the Instrumentable – Multiple Integrated Laser Engagement System (I-MILES) prior to each respective IOT&E. I-MILES is a subsystem of TES/RTCA and is essential to ensuring that engagements have realistic outcomes. I-MILES was designed to replicate the weapons effects against conventional armor, and cannot simulate the dynamic missile defeat technology employed by Active Protection Systems. Updates will also support force-on-force training once these new and upgraded vehicles are fielded.

DOT&E has emphasized the need for sustained investment and regular upgrades in TES/RTCA capabilities since 2002. These capabilities are necessary for testing systems such as Amphibious Combat Vehicle, Bradley and Abrams Upgrades, Armored Multi-purpose Vehicle, AH-64E Block III, Mobile Protected Firepower, Joint Light Tactical Vehicle, and Stryker Upgrades.

Warrior Injury Assessment Manikin

Hybrid III is an anthropomorphic test device (ATD) currently used for LFT&E, but this ATD lacks biofidelity in an underbody blast (UBB) test environment. Therefore, it does not exhibit a human-like response when exposed to UBB loading conditions and lacks capability to fully assess operator survivability to vehicle threats yielding UBB environments. The Warrior Injury Assessment Manikin (WIAMan) Engineering Office (WEO) is developing WIAMan ATD to address this LFT&E capability shortfall. The LFT&E section describes the WIAMan project on page 313.

Test and Evaluation of Army Software-Defined Tactical Radios

Software-Defined Radios have become a cornerstone technology of the Army tactical radio communication systems.

Software-Defined Tactical Radios provide the Army with improved capabilities such as simultaneous voice, data, and video communications; voice and data retransmission; increased throughput; multi-channel operations; and interoperability with fielded radios. Because of the complexity of these tactical radio networks and the added capabilities they provide, improved test instrumentation and data collection methods are needed to support the evaluations of the Army Software-Defined Tactical Radios. Specific evaluation metrics that currently cannot be evaluated include voice quality, call completion rate, and the route each message takes through the network. The Army should investigate methods to collect these metrics and develop a plan to support upcoming IOT&Es. These improvements to instrumentation and data collection methods are necessary to support the test and evaluation of the Leader Radio and Manpack Radio.

Range Sustainability

For the past eight years, DOT&E has reported on land-, air-, sea-space, and frequency spectrum resource problems that limit the DOD's ability to test weapons systems in operationally realistic environments. As previously reported, adequate land-, air-, and sea-space are critical to test weapons and associated systems in operationally realistic conditions. Range sustainability and the preservation of those resources is challenged by factors such as incompatible infrastructure, urban development, natural and cultural resource protection, and frequency spectrum losses. Each of these factors may limit a range's capability to conduct operational test and evaluation.

From a range sustainability perspective, the DOD has had some success in preserving land-, air-, sea-space, and frequency spectrum. Additional work is required, as is a comprehensive plan to address future challenges.

Table 2 illustrates the increase of range sustainability challenges since 2001. While many problems have been mitigated, they have not been eliminated.

Those that are unshaded are being effectively mitigated/managed by the Services/Installations. Those that are shaded presently require additional effort to manage and/or resolve unmitigated challenges. Specific challenges include:

- Renewable Energy and Maritime Sustainability – Energy production infrastructure interference with test capabilities including weapons testing and operational launches, airborne radar, and aircraft systems testing
- Airspace – Insufficient overland range for test flight of hypersonic missiles and growing challenges to offshore airspace from potential energy development
- Cyber Intrusion of Range Instrumentation – Vulnerability of instrumentation and systems under test
- Frequency Spectrum – Inadequate frequency spectrum to accommodate increased data collection and transmission of test data
- Privately Operated Drones – Interference from privately operated aerial drones
- Endangered Species – Test limitations resulting from natural resource protection
- Foreign Investment – Compromise of test data as a result of foreign surveillance
- Cultural Resources – Requirements to conduct surveys

TABLE 2. TEST RANGE SUSTAINABILITY CHALLENGES, 2001-2017

	2001	2003	2005	2007	2009	2011	2013	2015	2017
Endangered Species	•	•	•	•	•	•	•	•	•
Unexploded Ordinance (UXO) and Munitions	•	•	•	•	•	•	•	•	•
Airspace	•	•	•	•	•	•	•	•	•
Maritime Sustainability	•	•	•	•	•	•	•	•	•
Airborne Noise	•	•	•	•	•	•	•	•	•
Frequency Spectrum	•	•	•	•	•	•	•	•	•
Air Quality	•	•	•	•	•	•	•	•	•
Urban Growth	•	•	•	•	•	•	•	•	•
Land Space	•	•	•	•	•	•	•	•	•
Cultural Resources	•	•	•	•	•	•	•	•	•
Adverse Weather Effects on Ranges				•	•	•	•	•	•
Water Rights					•	•	•	•	•
Renewable Energy					•	•	•	•	•
Privately Operated Drones							•	•	•
Foreign Investment							•	•	•
Cyber Intrusion of Range Instrumentation								•	•
Space									•

Unshaded areas are being effectively mitigated/managed by the Services/installations. Shaded areas require additional effort.

Renewable Energy

Siting of energy infrastructure, particularly wind turbines, adjacent to military test installations continues to be a challenge for the DOD. Interference with radar systems adversely affects DOD testing. Where interference has arisen, the effect must be mitigated to allow continued use of test capabilities. The trend toward taller wind turbines with longer blades has exacerbated the negative effects on radar performance. DOT&E continues to work with the DOD Siting Clearinghouse to evaluate projects referred by the Federal Aviation Administration's (FAA) Obstruction Evaluation process and from other sources. Legislation is pending which would strengthen Siting Clearinghouse authorities.

Maritime Sustainability

Outer Continental Shelf leasing for oil and gas exploration and exploitation poses a potential threat to the capability to conduct operational testing. In the Eastern Gulf of Mexico, potential expansion of oil and gas development conflicts with the DOD needs to test advanced weapons systems in an operationally realistic environment. Testing new hypersonic missiles and autonomous systems requires large safety envelopes to minimize risks to populations and infrastructure. These safety requirements likely will drive a change in the DOD test inputs to the current Bureau of Ocean Energy Management (BOEM) program plan because the DOD must now address changes in the threat environment. The DOD works closely with the BOEM to group areas considered for oil and gas development into categories where development can co-exist with DOD requirements and where it cannot.

Airspace

High technology weapons systems designed to counter future threats will require additional air-land space to conduct testing in operationally realistic environments. The DOD needs capabilities to test autonomous systems, hypersonic missiles, theater missile defense, swarm and counter swarm systems, and directed energy systems. These systems greatly stress the land-, air-, and sea-space available for operationally realistic tests. Very simply, test ranges secured in the 1940's were founded on the performance characteristics of weapons systems in that era, and current and proposed weapons systems far exceed those characteristics. The Army intends the Long Range Precision Fires (LRPF) program to extend the range of its tactical missile capabilities beyond 300 km. The LRPF missile must be tested from launch to impact at its maximum range to evaluate effectiveness. The footprint required for testing the maximum range of the LRPF missile exceeds the land area of any single Army test range. LRPF must also be tested in an EW environment to ensure the missile can survive launch, flight, and impact through a contested electromagnetic environment. The Army must develop a solution such that the LRPF can be launched through a threat EW environment at maximum range and impact the ground in a location with threat representative targets. To be able to perform these types of tests, the DOD must work with Federal and state agencies to expand or combine domestic resources or will need to test at overseas ranges where expanded test parameters can be accommodated.

Cyber Intrusion of Range Instrumentation

Recent intrusion to allegedly secure networks raises the issue of whether test range communications networks are as secure as they should be to avoid test data leakage to unauthorized sources. Therefore, vulnerabilities of instrumentation as well as weapons-under-test need to be addressed. Both the 96th Test Wing at Eglin Air Force Base and the White Sands Missile Range conducted tabletop exercises in late 2016 and 2017, and have plans underway to perform more in-depth testing of actual range systems. Other ranges will be conducting similar events going forward.

Frequency Spectrum

The RF spectrum is a vital resource needed to conduct test operations, transmit and receive critical test data, and is necessary to ensure test range safety. Increased weapon system complexity and test data transmission requirements in support of the Joint Strike Fighter, the future Long Range Strike Bomber, and Long Range Stand-Off Weapon, increase the need for RF spectrum to support test operations. Specifically, DOD T&E has a documented need for 865 megahertz (MHz) of RF spectrum required to support test operations by 2025. Meanwhile, national spectrum policy, fueled predominantly by increased demand for commercial cellular and wireless services, is reducing the available amount of RF spectrum to support T&E. For example, the Advanced Wireless Service (AWS-3) auction repurposed the 1755-1780 MHz portion of spectrum that is heavily used to support flight test operations and operational test missions. The main concern is supporting national spectrum policy while ensuring that the DOD has access to the required amount of the RF spectrum to support test operations. DOT&E, in conjunction with TRMC and Service partners, employs strategies to preserve the RF spectrum currently available for DOD use, and supports research initiatives for technologies and equipment that make the most efficient use of available spectrum. DOT&E will continue to monitor frequency spectrum availability related to operational test requirements, review policies and procedures ensuing from the DOD Spectrum Strategy, and engage in other issues that may adversely affect use of spectrum for T&E.

Privately Operated Drones

The widespread operation of recreational drones jeopardizes restricted airspace control. Their use in or near restricted airspace can impede the safe operations of military aircraft and systems, and also poses the threat of surveillance. DOD legal avenues to limit drone access are currently limited, but recent actions by the FAA and Congress to limit drone operations within national security zones are encouraging.

Endangered Species

As discussed in previous reports, DOD ranges contain environmentally sensitive flora and fauna, including those that migrate from disturbed areas external to our ranges. Threatened or endangered species listings have increased from 600 in 1990

to 1,656 in September 2017. The DOD manages and protects more than 400 threatened and endangered species, and more than 550 at risk species on its military installations. Integrated Natural Resources Management Plans (INRMPs) are the key documents that the DOD uses to address how each installation with natural resources will manage those resources – there are 346 INRMPs. To test, the DOD must balance requirements against species preservation, which can be a limiting factor on testing. DOT&E engages Federal, state, local, and private organizations to explore the means to minimize such limitations.

Foreign Investment

Foreign investments in the U.S. may enable foreign intelligence services to conduct surveillance of U.S. weapon systems testing through proximity to test ranges. Such investments may also allow information collection on critical technologies and personally identifiable information of the testers. DOT&E reviews projects submitted to the Committee on Foreign Investment in the United States (CFIUS) for possible security risks associated with foreign surveillance. During the past 12 months, 223 cases, with more than 3,300 supporting documents, were reviewed. Seven cases were assessed to pose a potential threat to test or training ranges and required further investigation and development of mitigation strategies. Submissions are on track to reach 300 cases by the end of calendar year 2017. However, CFIUS only reviews projects submitted by applicants; there is a potential risk that other, unrecorded transactions may create operational security vulnerabilities. DOT&E will continue to exercise vigilance in reviewing all identified cases of foreign investment to ensure that data from weapon system tests are not compromised.

Cultural Resources

Under the National Historic Preservation Act, Federal agencies are required to consult with state and local groups before cultural resources, such as historical or archaeological sites, are damaged. Results of cultural resource surveys are used to inform decision-making by determining how resources may be affected, and what alternatives exist to reduce risk of harm. Many test ranges contain cultural resources, and therefore must conduct surveys to determine where resources exist and to factor potential disturbance into test planning.

The DOD faces competition for many of the natural resources needed to conduct adequate testing. DOT&E will continue to assess the adequacy of resources needed to conduct adequate testing, will alert Department leadership to shortfalls in such resources, and will participate in interagency processes to promote resource adequacy.

Test Infrastructure Efficiency

The recent development and fielding of the Common Range Integrated Instrumentation System (CRIIS) by the TRMC under the Central Test and Evaluation Investment Program (CTEIP) is a major achievement in efficiency within the test and training communities. CRIIS is a family of systems for airborne data collection for all DOD aircraft that replaces the Advanced Range Data System (ARDS). It provides high-speed, real-time, mult-level secure data with position accuracies down to 0.5 meters. A funded software modification to CRIIS datalink capabilities will provide compatibility with Air-to-Air Range Infrastructure (AARI) messages currently in use for F-22 operational testing (OT) and planned for use during F-35 OT. CRIIS also provides an architecture to support live virtual constructive (LVC) testing including the capability to transfer weapon simulation data needed for training missions. The system started fielding this year and will be deployed on approximately 200 aircraft at 8 Major Range and Test Facility Base (MRTFB) locations.

In March 2017, Rockwell Collins, the system's lead developer for CRIIS, was awarded the Navy's Tactical Combat Training System Increment II (TCTS Inc II) contract to develop the next-generation training system. This system will have significant commonality with CRIIS, which will result in a common test and training instrumentation system for MRTFB ranges and Navy training activities. These CRIIS-based solutions will facilitate shared use of one another's assets and range facilities, and will pave the way for a life-cycle strategy that could save the Department millions of dollars in long-term sustainment. In order to save additional DOD operations and sustainment costs and realize the full potential of the CRIIS-based architecture, DOT&E encourages the Air Force to adopt CRIIS interoperable technologies for use by its training community.

Joint Test and Evaluation

Joint Test and Evaluation

Joint Test and Evaluation (JT&E)

The primary objective of the Joint Test and Evaluation (JT&E) Program is to rapidly provide non-materiel solutions to operational deficiencies identified by the joint military community. The program achieves this objective by developing new tactics, techniques, and procedures (TTPs) and rigorously measuring the extent to which their use improves operational outcomes. JT&E projects may develop products that have implications beyond TTPs. Sponsoring organizations submit these products to the appropriate Service or Combatant Command (CCMD) as doctrine change requests. Products from JT&E projects have been incorporated into joint and multi-Service documents through the Joint Requirements Oversight Council process, Joint Staff doctrine updates, Service training centers, and coordination with the Air Land Sea Application Center. The JT&E Program also develops operational testing methods that have joint application. The program is complementary to, but not part of, the acquisition process.

The JT&E Program uses two test methods – the Joint Test and the Quick Reaction Test (QRT) – and, on occasion, a Special Project focused on the needs of operational forces. These are explained below. Projects annotated with an asterisk (*) were completed in FY17.

The Joint Test is, on average, a 2-year project preceded by a 6-month Joint Feasibility Study. A Joint Test involves an in-depth, methodical test and evaluation of issues and seeks to identify their solutions. DOT&E funds the sponsor-led test team, which provides the customer with periodic feedback and usable, interim test products. The JT&E Program charters two new Joint Tests annually. The JT&E Program managed seven Joint Tests in FY17:

- Digitally Aided Close Air Support (DACAS)
- Joint Advanced Zensor to Zhooter (JAZZ)*
- Joint Counterair Integration (JCI)
- Joint Cyber Insider Threat (J-CIT)
- Joint Interoperability for Medical Transport Missions (JI-MTM)
- Joint Laser Systems Effectiveness (JLaSE)
- Joint Pre/Post-Attack Operations Supporting Survivability and Endurability (J-POSSE)*

QRTs are intended to solve urgent issues in less than a year. The JT&E program managed 22 QRTs in FY17:

- Aviation Radio Frequency Survivability Validation (AVRFSV)
- Critical Strategic Power Projection Infrastructure (CRSPPI)
- Cyber Degraded Training (CDT)*
- Homeland Underwater Port Assessment Plan (HUPAP)*
- Intelligence Prioritization for Cyberspace Operations (IPCO)
- Joint Accelerated Collaborative Targeting (J-ACT)*
- Joint Air Operations Center (AOC) Command and Control (C2) in a Contested Degraded Environment (JADC)*
- Joint Ballistic Missile Defense (BMD) Overhead Persistent Infrared (OPIR) Operational Space Track (J-BOOST)
- Joint Biological/Radiological Mortuary Affairs Contaminated Remains Mitigation Site (JBRM)*
- Joint Contaminated Human Remains (CHR) Recovery in a Chemical Environment (JCRCE)
- Joint Cyber Integration of DOD Information Network Operations (J-CID)*
- Joint Intelligence Production in a Cloud Environment (JIPCE)
- Joint Interagency - Cyber Enhanced Detection and Monitoring (JI-CEDM)*
- Joint Intercontinental Ballistic Missile (ICBM) Weapon Convoy (JIWC)*
- Joint Missile Seeker Defeat (JMSD)
- Joint Multi-Intelligence Correlation and Dissemination (JMCD)*
- Joint Personnel Recovery Information Digital Exchange (J-PRIDE)*
- Joint Radio Frequency-Enabled Cyberspace Operations (JRF-ECO)
- Joint Sensor to Tactically Responsive Integrated Kinetic Effects (J-STRIKE)
- Joint Talon Thresher Theater Integration (JT3I)*
- Non-classified Internet Protocol Router (NIPR) Enhanced Common Operational Picture (Ne-COP)*
- Optimization of Social Media and Open Source Information Support (OSMOSIS)*

As directed by DOT&E, the program executes Special Projects that address DOD-wide problems. Special Projects generally address emergent issues that are not addressed by any other DOD agency but that need a thoroughly tested solution. The program managed one Special Project in FY17:

- Joint National Capital Region Enhanced Surveillance Tactics, Techniques, and Procedures (J-NEST)*

JOINT TESTS

DIGITALLY AIDED CLOSE AIR SUPPORT (DACAS)

Sponsor/Start Date: Joint Staff J6/February 2016

Purpose: To develop, test, and evaluate standardized TTPs in order for Joint Terminal Attack Controllers (JTAC), Joint Fires Observers, and Close Air Support (CAS) aircrew to realize the advantage of DACAS capabilities, including shared situational awareness, increased confidence prior to weapons release, and improved kill chain timeliness.

Products/Benefits:
- TTPs that outline network management considerations and provide mission planning and execution procedures to ensure all users have standardized information to operate on the network and to deliver proper system configuration for first-try connectivity
- Decreased human input error through machine-to-machine data exchange leading to increased speed of CAS execution
- Enable JTAC and aircrew to access existing networks and exploit DACAS benefits
- Enhance operational effectiveness and increase confidence prior to weapons release by providing a common and accurate shared situational awareness

JOINT ADVANCED ZENSOR TO ZHOOTER (JAZZ) (CLOSED AUGUST 2017)

Sponsor/Start Date: U.S. Pacific Command (USPACOM)/ August 2015

Purpose: To develop, evaluate, and validate TTPs to more efficiently and effectively gain and maintain battlespace awareness through the integration of rapidly developed capabilities supporting combat operations in anti-access/area denial environments.

Products/Benefits:
- Sensor to shooter TTPs that enable sharing of advanced sensor and National-Tactical Integration (NTI) data between 5th and 4th generation fighters leading to increased situational awareness, improved engagement opportunities, and better utilization of weapon systems
- Documented roles and responsibilities for the Operational Air Component Commander and tactical datalink network designers to plan and execute integration of advanced sensors and NTI into any theater of operations
- An innovative tactical datalink design compatible for coalition operations and integration of advanced sensors and NTI
- DOT&E notification to CCMDs about the discovery of previously unidentified discrepancies for NTI reporting on tactical datalinks

JOINT COUNTERAIR INTEGRATION (JCI)

Sponsor/Start Date: USPACOM/February 2017

Purpose: To develop, test, and evaluate TTPs to provide counterair shooters and command and control (C2) operators with the ability to integrate joint defensive counterair (DCA) resources in a contested, degraded, and operationally limited (CDO) environment to protect defended assets from expected threats.

Products/Benefits:
- TTPs that enable operators to integrate DCA forces in a CDO environment to improve tactical-level operations, enhance coordination between assets, and minimize exploitation of gaps in area coverage
- Integration of Army, Air Force, Navy, and Marine Corps DCA assets to counter a peer threat in a CDO environment

JOINT CYBER INSIDER THREAT (J-CIT)

Sponsor/Start Date: U.S. Army Research Laboratory/ August 2016

Purpose: To develop, test, and evaluate TTPs to detect and report cyber insider threats in order to prevent harm to national security interests.

Products/Benefits:
- Cyber Insider Threat Detection and Reporting (CIDaR) TTPs that provide Cybersecurity Service Provider tier II operators with specific technical and configuration requirements to establish a cyber Insider Threat Advanced Detection (ITAD) capability to create unique analysis and reporting procedures for insider threats
- CIDaR TTPs that identify operational characteristics, such as staffing requirements, needed to monitor cyber insider threat activities
- CIDaR TTPs and ITAD capabilities that are software/hardware agnostic

JOINT INTEROPERABILITY FOR MEDICAL TRANSPORT MISSIONS (JI-MTM)

Sponsor/Start Date: DOD Chief Information Officer/ August 2017

Purpose: To develop, test, and evaluate standardized TTPs to access and utilize existing patient information from various health information systems across the DOD during the patient movement coordination and validation process.

Products/Benefits:
- Faster access to required information resulting in quicker validation of patient movement requests and movement to the appropriate care level
- Richer picture of patient history for better informed medical decisions
- Improved capability to plan and deliver appropriate transport and onboard medical staff in order to provide the best en route care for patients
- Reduced workload and potential for errors during manual information reentry into the patient movement planning system

JOINT LASER SYSTEMS EFFECTIVENESS (JLASE)

Sponsor/Start Date: Naval Surface Warfare Center, Dahlgren Division/April 2017

Purpose: To develop and test procedures that integrate emerging directed energy laser (DEL) weapon systems with weaponeering and Collateral Damage Estimation (CDE) methodology within the Joint Targeting Cycle.

Products/Benefits:
- Joint Targeting Cycle procedures for Laser Weaponeering and CDE in addition to Joint Munition Effectiveness Manual (JMEM) lethality data
- Integration of DEL systems into the Joint Targeting Cycle focusing on capabilities analysis, weaponeering, and damage estimation
- Development of JMEM data for use by weaponeers with joint targeting systems as part of the JMEM Weaponeering System
- Increased confidence of warfare commanders in the ability of laser weapons to provide scalable lethality ranging from degrading sensors to catastrophic destruction
- Recommendations to assist the Services in DEL system development and acquisition as well as with integrating DELs into the operational environment
- TTPs for the integration of high energy laser weapon systems into joint and Service operations in order to engage enemy targets according to the commander's intent

JOINT PRE/POST-ATTACK OPERATIONS SUPPORTING SURVIVABILITY AND ENDURABILITY (J-POSSE)
(CLOSED FEBRUARY 2017)

Sponsor/Start Date: U.S. Strategic Command (USSTRATCOM)/February 2015

Purpose: To develop, test, and evaluate TTPs to provide joint operators the ability to survive an electromagnetic pulse (EMP) event in order to ensure continuous mission functionality.

Products/Benefits:
- Standardized procedures that provide overarching guidance for required actions before and after an EMP event for survival
- Results to inform future resourcing decisions regarding physical enhancements
- TTPs that can be extended to other mission systems that are potentially vulnerable to EMP effects

QUICK REACTION TESTS

AVIATION RADIO FREQUENCY SURVIVABILITY VALIDATION (AVRFSV)

Sponsor/Start Date: U.S. Army Aviation Center of Excellence/October 2016

Purpose: To increase rotary-wing asset survivability effectiveness against the most widely proliferated radio frequency (RF) threats through the employment of a combination of aircraft survivability equipment, countermeasures, and maneuvers.

Products/Benefits:
TTPs for rotary-wing aircraft to maintain freedom of maneuver against and defeat RF threats.

CRITICAL STRATEGIC POWER PROJECTION INFRASTRUCTURE (CRSPPI)

Sponsor/Start Date: North American Aerospace Defense Command (NORAD)-U.S. Northern Command (USNORTHCOM)/June 2017

Purpose: To develop Interagency Infrastructure Assessment (IIA) TTPs to enable the assessment of select critical interagency infrastructures. Sponsor lacks specific agreements, procedures, and access to conduct assessments in areas that the DOD does not own or control. A lack of information and assessment of certain critical infrastructures, facilities, and transportation nodes significantly degrades the sponsor's ability to prepare for and rapidly respond to high consequence, multi-domain threats to U.S. critical strategic infrastructures.

Products/Benefits:
IIA TTPs, with an accompanying implementation plan, to prescribe all aspects of manning, agreements, funding support, and coordination to initiate an IIA program of record.

CYBER DEGRADED TRAINING (CDT)
(CLOSED JANUARY 2017)

Sponsor/Start Date: USPACOM/October 2015

Purpose: To develop, test, and evaluate concept of operations (CONOPS) and TTPs that address the characteristics of cyber-degraded training environments as well as how to select, employ, and overcome these capabilities relative to factors such as military training objectives, commander's risk tolerance, threat representation, and exercise complexity.

Products/Benefits:
- TTPs that provide USPACOM with standardized, comprehensive tools to support commanders at all levels with the ability to function in a cyber-degraded environment
- CONOPS that identify the different types of cyber-degraded environments that can be created and ways that trainers, planners, and subject matter experts can use them in training and exercise activities

HOMELAND UNDERWATER PORT ASSESSMENT PLAN (HUPAP)
(CLOSED OCTOBER 2016)

Sponsor/Start Date: NORAD-USNORTHCOM/June 2015

Purpose: To develop and evaluate TTPs for underwater port assessments to include specific details about the roles and responsibilities of the stakeholders; identify available local, state, and federal force multipliers; provide data collection, compilation, and sharing guidance; and identify gaps in response considerations.

Products/Benefits:
- Comprehensive TTPs that prescribe the standards and activities needed to gather interagency underwater port information for homeland ports and internal waterways in preparation for a catastrophic event
- Reference for port authorities when developing an Interagency Underwater Port Assessment to provide DOD and interagency partners with the preparation, response, and recovery information necessary to reopen ports and waterways

INTELLIGENCE PRIORITIZATION FOR CYBERSPACE OPERATIONS (IPCO)

Sponsor/Start Date: U.S. Special Operations Command/ February 2017

Purpose: To develop and assess TTPs for integration of cyber intelligence planning into mission execution. Joint Task Forces lack early allocation of intelligence resources to enable cyberspace operations. Significant lead time is needed for proper cyberspace operations planning.

Products/Benefits:
- TTPs to improve the timing and production of required basic level intelligence preparation of the operational environment products used by the joint force
- TTPs that facilitate the integration of cyberspace operations into the planning and execution of joint operations

JOINT ACCELERATED COLLABORATIVE TARGETING (J-ACT)
(CLOSED MAY 2017)

Sponsor/Start Date: USSTRATCOM/February 2016

Purpose: To develop and assess CONOPS that use an accelerated intelligence processing, exploitation, and dissemination (PED) process that streamlines intelligence analysis and coordination with targeteers to increase the speed of potential target object classification and verification.

Products/Benefits:
PED CONOPS that accelerate imagery analysis, target object classification, and target verification.

JOINT AIR OPERATIONS CENTER (AOC) COMMAND AND CONTROL (C2) IN A CONTESTED DEGRADED ENVIRONMENT (JADC)
(CLOSED JULY 2017)

Sponsor/Start Date: USPACOM/February 2016

Purpose: To develop TTPs to support joint AOC distributed planning, execution, and assessment in a contested, degraded, and operationally limited environment by distributing authorities and effectively employing airpower and supporting forces.

Products/Benefits:
- TTPs that enable delegation of operational airpower C2 from the joint AOC to subordinate commanders
- Distributed authorities that empower leaders at lower echelons of command to continue execution of the commander's intent with limited loss of operational or tactical initiative

JOINT BALLISTIC MISSILE DEFENSE (BMD) OVERHEAD PERSISTENT INFRARED (OPIR) OPERATIONAL SPACE TRACK (J-BOOST)

Sponsor/Start Date: U.S. Air Forces in Europe-Air Forces Africa/October 2016

Purpose: To develop TTPs to optimize existing space-based technology for active and passive defense. The goal is to better use current and near-term BMD capabilities resulting in earlier missile threat situational awareness, precision cueing, engagement opportunities, and improved architecture resilience.

Products/Benefits:
- TTPs that document configuration of communications networks to allow select C2 nodes, Aegis BMD, and Aegis Ashore systems to receive, interpret, and use Enterprise Sensors Processing Node tracks in testing, training, exercises, and operations
- Earlier and more refined development of defensive response options
- Increased warfighter confidence in the ability to use space-based data in support of the BMD mission set

JOINT BIOLOGICAL/RADIOLOGICAL MORTUARY AFFAIRS CONTAMINATED REMAINS MITIGATION SITE (JBRM)
(CLOSED DECEMBER 2016)

Sponsor/Start Date: U.S. Army Quartermaster School/ June 2015

Purpose: To develop TTPs for the safe processing, identification, and preparation for the evacuation of biologically or radiologically contaminated human remains. To improve the Mortuary Affairs Contaminated Remains Mitigation Site effectiveness and safety for operational mission requirements,

including mitigating hazards, preserving forensic evidence, establishing chain of custody, supporting positive identification processes, and preparing remains for evacuation.

Products/Benefits:
- Updates to U.S. Army and joint doctrine with the primary focus on Army Techniques Publication 4-46.2, "Mortuary Affairs Contaminated Remains Mitigation Site Operations," as related to biological or radiological contaminated human remains
- Verified data and tools for the mortuary affairs community to use in both USNORTHCOM homeland defense missions and DOD's worldwide contingency operations
- A Mortuary Affairs Contaminated Remains Mitigation Site Tactical Handbook

JOINT CONTAMINATED HUMAN REMAINS (CHR) RECOVERY IN A CHEMICAL ENVIRONMENT (JCRCE)

Sponsor/Start Date: U.S. Army Quartermaster School/ June 2017

Purpose: To identify gaps in current TTPs and provide TTPs improvement recommendations for the safe recovery of chemically contaminated human remains (C-CHR). To validate procedure effectiveness and safety for mitigating hazards, preserving forensic evidence, and accomplishing preliminary decedent identification tasks.

Products/Benefits:
- Joint TTPs for safe recovery of C-CHR
- Evaluations on the utility and suitability of new human remains pouch capabilities

JOINT CYBER INTEGRATION OF DOD INFORMATION NETWORK OPERATIONS (J-CID)
(CLOSED NOVEMBER 2016)

Sponsor/Start Date: USPACOM/June 2015

Purpose: To develop CONOPS and TTPs for the CCMD's Joint Cyber Center (JCC) that fully integrates the organization, authorities, and capabilities of DOD Information Network commands in support of joint theater cyber operations.

Products/Benefits:
CONOPS and TTPs that provide best practices for the support of regional operations, situational understanding, and decision-making for cyberspace operations between regional DOD Information Network commands and JCCs.

JOINT INTELLIGENCE PRODUCTION IN A CLOUD ENVIRONMENT (JIPCE)

Sponsor/Start Date: Air Combat Command/October 2016

Purpose: To develop TTPs to utilize Intelligence Community Information Technology Enterprise (IC ITE)-enabled tools and tradecraft to supplement Joint Intelligence Preparation of the Environment (JIPOE) processes.

Products/Benefits:
TTPs and quick reference guides that enable Joint Intelligence Operations Center intelligence analysts to optimize IC ITE cloud-based intelligence information and tools, particularly BRIMSTONE and its follow-on, in support of JIPOE Step Four, Determine Adversary Course of Action.

JOINT INTERAGENCY - CYBER ENHANCED DETECTION AND MONITORING (JI-CEDM)
(CLOSED JUNE 2017)

Sponsor/Start Date: Joint Interagency Task Force (JIATF) South/February 2016

Purpose: To develop TTPs that coordinate and utilize interagency cyber domain support from DOD, law enforcement, and intelligence community partners during detection and monitoring (D&M) missions. These TTPs promote the timely and efficient leveraging of internal and external cyber resources to support JIATF South requirements, eliminate redundancy, and maximize the impact of cyber domain information in conducting D&M operations.

Products/Benefits:
TTPs that identify specific procedures for the JIATF South staff to coordinate and utilize interagency cyber domain support from DOD, law enforcement, and intelligence community partners during illicit trafficking D&M missions.

JOINT INTERCONTINENTAL BALLISTIC MISSILE (ICBM) WEAPON CONVOY (JIWC)
(CLOSED SEPTEMBER 2017)

Sponsor/Start Date: Air Force Global Strike Command/ June 2016

Purpose: To develop TTPs to maintain persistent situational awareness and C2 in support of nuclear convoy movement operations. The objective of the TTPs is to optimize use of the Wave Relay Tactical Assault Kit cloud relay system during ICBM convoy operations.

Products/Benefits:
- TTPs that define how to integrate airborne firepower into nuclear weapon movements
- Increased situational awareness for improved safety and security of nuclear weapon convoy movement operations
- Enhanced C2 between the convoy commander and missile wings for improved accident and/or incident response during nuclear weapon movements

JOINT MISSILE SEEKER DEFEAT (JMSD)

Sponsor/Start Date: USPACOM/June 2016

Purpose: To develop and assess a missile seeker defeat concept of employment and associated TTPs.

Products/Benefits:
Specific TTPs that enable Major Weapon Systems/aircraft to employ missile seeker defeat concept against an existing adversary threat.

JOINT MULTI-INTELLIGENCE CORRELATION AND DISSEMINATION (JMCD)
(CLOSED SEPTEMBER 2017)

Sponsor/Start Date: Twenty-Fifth Air Force/June 2016

Purpose: To develop and assess TTPs to manage, fuse, and amplify intelligence information from a variety of national sources in order to provide the most accurate and complete air picture possible.

Products/Benefits:
- TTPs that enable management, fusion, and amplification of intelligence information from a variety of organic and non-organic sources
- Streamlined correlation and adjudication of tracks in support of the Common Operational Picture (COP)
- Framework for Data Link Operators to rapidly analyze multiple or conflicting tracks from nationally derived sources where necessary to streamline dissemination to the warfighter

JOINT PERSONNEL RECOVERY INFORMATION DIGITAL EXCHANGE (J-PRIDE)
(CLOSED OCTOBER 2016)

Sponsor/Start Date: Joint Staff J7/June 2015

Purpose: To develop TTPs to pass critical information across existing hybrid networks between isolated personnel, recovery forces, and C2 nodes during joint personnel recovery (PR) missions.

Products/Benefits:
- Enhanced mission effectiveness and increased survivability due to mission critical information being formalized across operational and tactical PR nodes
- Standardized 15-line PR message format for use across joint forces

JOINT RADIO FREQUENCY-ENABLED CYBERSPACE OPERATIONS (JRF-ECO)

Sponsor/Start Date: USSTRATCOM and USPACOM/ June 2017

Purpose: To develop a baseline CONOPS for the C2 of RF-enabled cyber operations.

Products/Benefits:
CONOPS for C2 of RF-enabled cyber operations.

JOINT SENSOR TO TACTICALLY RESPONSIVE INTEGRATED KINETIC EFFECTS (J-STRIKE)

Sponsor/Start Date: U.S. Army Pacific/February 2017

Purpose: To provide more timely and effective access for theater assets to sense and destroy high value enemy targets through the seamless integration of intelligence, surveillance, reconnaissance, and targeting information between all domains and Services.

Products/Benefits:
TTPs to fully exploit cross-domain fires capabilities with currently available systems.

JOINT TALON THRESHER THEATER INTEGRATION (JT3I)
(CLOSED FEBRUARY 2017)

Sponsor/Start Date: USPACOM/October 2015

Purpose: To develop CONOPS that clearly define the optimal operating parameters of the Talon THRESHER system and standardize user operating procedures to enhance air domain awareness within theater C2 nodes, joint AOCs, and NTI cells.

Products/Benefits:
- Standardized operating parameters and procedures to utilize and disseminate Talon THRESHER data
- Enhanced analysis of air track patterns of behavior
- Timely output of correlated air picture in multiple security formats

NIPR ENHANCED COMMON OPERATIONAL PICTURE (NE-COP)
(CLOSED SEPTEMBER 2017)

Sponsor/Start Date: USPACOM/June 2016

Purpose: To enhance the commander's situational awareness by leveraging open-source and partner nation unclassified information contributions, allowing interoperability for the warfighter from the operational level to decision makers at the tactical and strategic levels during Phase Zero operations.

Products/Benefits:
A handbook that will allow global commanders to have consolidated documentation of unclassified COP tools and set the conditions for a redundant, accurate, and advanced COP across multiple classification levels within the DOD and key partner nations.

OPTIMIZATION OF SOCIAL MEDIA AND OPEN SOURCE INFORMATION SUPPORT (OSMOSIS)
(CLOSED MAY 2017)

Sponsor/Start Date: U.S. Central Command/February 2016

Purpose: To develop TTPs to enable commanders to rapidly and effectively gain near real-time situational awareness using globally published digital media (new and traditional media sources). This TTPs will enhance decision-making, planning, and execution of the Civil Affairs, Psychological Operations/Military Information and Support Operations, and Public Affairs missions.

Products/Benefits:
- TTPs and training guide to improve information gathering from traditional and non-traditional sources
- Access to data needed to create value-focused, fused information for analysis to enhance the situational awareness of commanders at the tactical, operational, and strategic levels

SPECIAL PROJECTS

JOINT NATIONAL CAPITAL REGION ENHANCED SURVEILLANCE TACTICS, TECHNIQUES, AND PROCEDURES (J-NEST)
(CLOSED FEBRUARY 2017)

Sponsor/Start Date: NORAD/October 2014

Purpose: To develop TTPs to incorporate emerging sensor capabilities into the NORAD and USNORTHCOM family of systems to support the air defense mission.

Products/Benefits:
- TTPs that enable tactical, operational, and strategic C2 nodes to more fully employ expanded detection, improved identification, and enhanced engagement of cruise missile threats to the national capital region
- TTPs on utilization of advanced equipment capabilities to execute an effective joint engagement sequence for cruise missile defense

Center for
Countermeasures

Center for
Countermeasures

The Center for Countermeasures (CCM)

The Center for Countermeasures (the Center) is a joint activity that directs, coordinates, supports, and conducts independent countermeasure/counter-countermeasure (CM/CCM) T&E activities of U.S. and foreign weapons systems, subsystems, sensors, and related components. The Center accomplishes this work in support of DOT&E, the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation ((DASD(DT&E)), weapon systems developers, and the Services. The Center's testing and analyses directly support evaluations of the operational effectiveness and suitability of CM/CCM systems.

Specifically, the Center:

- Determines performance and limitations of missile warning and aircraft survivability equipment (ASE) used on rotary- and fixed-wing aircraft
- Determines effectiveness of precision guided weapon (PGW) systems and subsystems when operating in an environment degraded by CMs
- Develops and evaluates CM/CCM techniques and devices
- Operates unique test equipment that supports testing across the DOD
- Provides analyses and recommendations on CM/CCM effectiveness to Service Program Offices, DOT&E, DASD(DT&E), and the Services
- Supports Service member exercises, training, and pre-deployment activities

In FY17, the Center completed 34 T&E activities, summarized in the following sections. In the course of these activities, the Center analyzed more than 30 DOD systems or subsystems and reported the results. The Center placed special emphasis on rotary-wing survivability. The majority of its T&E efforts were focused on Joint Urgent Operational Needs Statements (JUONS) and Urgent Universal Needs Statements (UUNS) in support of ASE. Additionally, the Center:

- Supported other types of field testing for PGW and other systems
- Provided realistic Man-Portable Air Defense System (MANPADS) threat environments for Service member aircrew training
- Continued to improve its T&E capabilities and test methodologies
- Provided subject matter expert (SME) support to numerous working groups, task forces, and program offices

JUONS

Army: Formal AH-64E Advanced Threat Warner (ATW) JUONS Test

- Sponsor: Project Management Office Aircraft Survivability Equipment (PMO ASE)
- Activity: The Center provided one Multi-spectral Sea and Land Target Simulator (MSALTS) and one Joint Mobile Infrared Countermeasure (IRCM) Test System (JMITS) for simultaneous ultraviolet (UV) and infrared (IR) missile simulations and jam beam data collection. The Center provided simulators for single threat engagements against the integrated Department of the Navy (DON) Large Infrared Countermeasures (LAIRCM) Advanced Threat Warner (ATW)/Common Missile Warning System (CMWS) and Guardian Laser Turret Assembly (GLTA) as installed on the AH-64E. The PMO ASE conducted the test to collect data during dynamic clutter, degraded modes, sister/own ship flares, and sister/own ship guns and/or rockets testing for ATW Engineering Software Release 1.0. The PMO ASE conducted the test from October 1 – 19, 2016, at Test Area 1 (TA-1), Redstone Arsenal, Huntsville, Alabama.
- Benefit: Center participation in this test was in direct support of ongoing PMO ASE JUONS efforts. The Center collected data during this effort that allowed the PMO ASE to assess the integrated ATW/CMWS system declaration and threat angle-of-arrival performance and Direct Infrared Countermeasure (DIRCM) slew and pointing accuracy. The data also allowed the PMO ASE to determine if sister/own ship guns and/or rockets and flares degraded the performance of the ATW and/or GLTA.

Army: Army Special Operations Aviation JUONS Phase 1a and 1b Flight Tests

- Sponsors: U.S. Army Technology Applications Program Office (TAPO) and the 160th Special Operations Aviation Regiment (SOAR) Systems Integration and Maintenance Office (SIMO)
- Activity: The Center provided one MSALTS and one JMITS; the Center test team used the systems to emit IR missile simulations and collect jam beam data. The Center also provided missile simulator and missile warning sensor (MWS) SME support and an independent assessment of the test results. The TAPO installed the ATW (with ATW Engineering Software Release 1.0) and GLTA on the MH-60M with an upturned exhaust system (UES) and the MH-47F aircraft. The TAPO used the tests to assess the ATW system declaration and angle-of-arrival performance and the GLTA pointing accuracy.

The TAPO conducted the tests from November 7 – 15, 2016, at TA-6, Redstone Arsenal (Phase 1a MH-60 and Phase 1b MH-47F).
- Benefit: Center participation in these tests was in direct support of ongoing TAPO JUONS efforts. The data collected assisted the TAPO in its evaluation of the GLTA ability to acquire, track, and provide energy on target. The Center provided an independent assessment and collected data during this effort that allowed TAPO to investigate the use of smart dispensing for IRCM flare sequences (i.e., dispense the best pattern based off threat angle-of-arrival).

Army: Army Special Operations Aviation JUONS Software 2.5 Test
- Sponsors: TAPO and the 160th SOAR SIMO
- Activity: The Center provided one MSALTS for IR missile simulations and jam beam data collection. The Center also provided missile simulator and MWS SME support and an independent assessment of the test results. The TAPO installed the ATW and GLTA on the MH-60M UES helicopter. The TAPO conducted the test to assess the performance of the ATW Engineering Software Release 2.5 in cluttered environments. The TAPO conducted the test from January 26 – 28, 2017, at Decatur, Alabama.
- Benefit: Center participation in this test was in direct support of ongoing TAPO JUONS efforts. The Center provided an independent assessment and collected data during this effort that allowed TAPO to investigate whether the ATW 2.5 software upgrades corrected deficiencies found in the ATW Engineering Software Release 1.0.

Army: Formal AH-64E ATW JUONS Software 2.5 Test
- Sponsor: PMO ASE
- Activity: The Center provided one MSALTS for simultaneous UV and IR missile simulations and jam beam data collection. The Center provided the simulator for single threat engagements against the integrated ATW (with Engineering Software Release 2.5)/CMWS and GLTA as installed on the AH-64E. The Center test team used the UV simulations to collect data for the CMWS, the IR simulations for the ATW, and the jam beam radiometers to evaluate ATW jam return. The PMO ASE conducted the test, to assess the performance of the ATW in cluttered environments. The PMO ASE conducted the test from January 26 to February 9, 2017, at Decatur, Alabama, and from February 16 – 17, 2017, at Nashville, Tennessee.
- Benefit: Center participation in this test was in direct support of ongoing PMO ASE JUONS efforts. The Center collected data during this effort that allowed PMO ASE to assess the integrated ATW/CMWS system declaration and threat angle-of-arrival performance and DIRCM slew and pointing accuracy. The data also allowed the PMO-ASE to determine whether the ATW 2.5 software upgrade provided improved performance over the ATW 1.0 software.

Army: Army Special Operations Aviation JUONS Phase 2 Clutter Flight Tests
- Sponsors: TAPO and the 160th SOAR SIMO
- Activity: The Center provided one MSALTS and one JMITS to emit IR missile simulations and collect jam beam data. The Center also provided missile simulator and MWS SME support and an independent assessment of the test results. The TAPO installed the ATW (with Engineering Software Release 3.0) and GLTA on the MH-60M UES and MH-47F aircraft. The TAPO conducted the tests to determine the capabilities of the ATW to detect and declare the MSALTS simulations in the presence of clutter. The TAPO conducted the tests from June 5 – 13, 2017, at Houston, Texas, and from June 26 – 30, 2017, at Decatur, Alabama.
- Benefit: Center participation in these tests was in direct support of ongoing TAPO JUONS efforts. The Center collected data during this effort that helped TAPO assess the capabilities of the ATW, as installed on the MH-60M and MH-47, to declare, track, and respond when presented with simulated missiles in a clutter environment.

Army: Formal CH-47F, UH-60M, and AH-64E ATW JUONS Software 2.5 Test
- Sponsor: PMO ASE
- Activity: The Center provided one MSALTS for simultaneous UV and IR missile simulations and jam beam data collection. The Center provided the simulator for single threat engagements against the integrated ATW (with Engineering Software Release 2.5)/CMWS and GLTA as installed on the aircraft. The Center test team used the UV simulations to collect data for the CMWS, the IR simulations for the ATW, and the jam beam radiometers to evaluate ATW jam return. The PMO ASE conducted the test to assess the performance of the ATW in benign and cluttered environments. The PMO ASE conducted the test from mid-July 2017 to mid-September 2017 at Redstone Arsenal and Decatur, Alabama.
- Benefit: Center participation in this test was in direct support of ongoing PMO ASE JUONS efforts. The Center collected data during this effort that allowed PMO ASE to assess the integrated ATW/CMWS system declaration and threat angle-of-arrival performance, DIRCM slew and pointing accuracy, and ATW performance in benign and cluttered environments.

Air Force: CV-22 Air Force Special Operations Command (AFSOC) JUONS ATW Sensor Flight Test
- Sponsor: 96th Test Wing Test Squadron
- Activity: The Center provided two MSALTS missile simulators and personnel to perform two-color, IR simulations to collect system response data and three lasers (rangefinder, target designator, beamrider) to assess the ATW system as installed on the CV-22 platform. The 413th Test Squadron conducted the test in February 2017 at Hurlburt Field, Florida.

- Benefit: The Center collected the data that the 96th Test Wing Test Squadron required to assess the performance of the ATW system installed on the CV-22 aircraft.

Air Force: Medium Fixed-Wing (MFW) JUONS ATW Sensor Flight Test
- Sponsor: 645th Aerospace Systems Group (AESG)
- Activity: The Center provided one MSALTS missile simulator and personnel to perform two-color, IR simulations to collect system response data used to assess the ATW system as installed on the MFW platform. The 645th AESG tasked the U.S. Air Force 46th Test Wing Test Squadron, Defensive Systems and Mobility Directorate, Air Force Life Cycle Management Center to execute the test in April 2017 at Eglin AFB, Florida.
- Benefit: The Center collected the data that the 645th AESG required to assess the performance of the ATW system installed on the MFW platform.

Navy: DON Distributed Aperture Infrared Countermeasure (DAIRCM) JUONS HH-60G Risk Reduction Flight Test
- Sponsor: Program Executive Officer, Advanced Tactical Aircraft Protection Systems (PMA-272) on behalf of the Detachment 1 (Det 1), 413th Flight Test Squadron.
- Activity: The Center provided one MSALTS missile simulator and personnel to perform two-color, IR simulations to collect data during the risk reduction for DAIRCM missile warning algorithm development. PMA-272 did not enable the DAIRCM jammer response for this risk reduction test. The U.S. Air Force Det 1, 413th Flight Test Squadron executed the test in June 2017 at Nellis AFB, Nevada.
- Benefit: Center participation in this test was central in aiding the DAIRCM developers in their assessment of the missile warning capability at the current stage of the program. The Center collected data during this effort that PMA-272 intends to use to develop algorithms.

UUNS

Navy: DON LAIRCM ATW MV-22B UUNS IT2C Flight Testing
- Sponsor: PMA-272 and the Navy's Operational Test and Evaluation Force (OPTEVFOR)
- Activity: The Center provided one MSALTS to perform two-color, IR missile simulations, and consultation regarding test preparation, planning, and execution for the missile simulator and laser test events. The Navy conducted testing in December 2016 at the U.S. Army Yuma Proving Ground, Arizona. This test was an end-to-end, open-air T&E of the UUNS for integration of the DON LAIRCM ATW system onto the MV-22B.
- Benefit: The Center provided an independent assessment and collected data during this effort that helped PMA-272 evaluate the integration of the DON LAIRCM ATW system onto the MV-22B and test the new ATW software upgrades.

Navy: DON LAIRCM ATW CH-53E UUNS IT-D3 Flight Testing
- Sponsor: PMA-272 and OPTEVFOR
- Activity: The Center provided one MSALTS to perform two-color, IR missile simulations, and consultation regarding test preparation, planning, and execution for the missile simulator and laser test events. The Navy conducted testing in July 2017 at Ingalls Field, Hot Springs, Virginia. This test was an end-to-end, open-air T&E of the UUNS for integration of the DON LAIRCM ATW system onto the CH-53E.
- Benefit: The Center provided an independent assessment and collected data during this effort that helped PMA-272 evaluate the integration of the DON LAIRCM ATW system onto the CH-53E and test the new ATW software upgrades.

ASE ACTIVITIES

Army: Reduced Optical Signature Emissions Solution IRCM X Test
- Sponsor: TAPO and the 160th SOAR SIMO
- Activity: The Center provided SME support during the IRCM effectiveness test for the MH-60M UES and MH- 47G aircraft. The Center also assisted with the operation of IR seekers in the Missile and Space Intelligence Center (MSIC) seeker test van (STV). These tests evaluated new flare CM sequences and variations of current flare CM sequences using improved flares, different flares, and/or flare timing within the sequences. The Center provided near real-time data reduction and analysis of flare sequences as well as on-site recommendations on flare sequence timing and/or pattern adjustments. As a result, the sponsor was able to make decisions on flare sequence performance during the course of the test. After the test, the Center provided an independent assessment analysis report and a briefing of test results to TAPO leadership. The TAPO conducted the test in October and November 2016 at Redstone Arsenal.
- Benefit: The Center provided an independent assessment and collected data during this effort that allowed TAPO to determine a final IRCM flare solution for the MH-60M UES and MH-47G, thus providing better protection for those aircraft against MANPADS. This test also resulted in the modification and procurement of flares needed for the next phase of testing; these new flares should help enhance the protection of the MH-60M UES and MH-47G aircraft against MANPADS.

Army: Seeker Bowl XII IRCM Test

- Sponsor: Armament Research, Development and Engineering Center (ARDEC), Pyrotechnics Division, Countermeasure Flare Branch
- Activity: The Center provided SME support during the IRCM effectiveness test for the CH-47F Infrared Suppression System (IRSS), RC-12, Foxhound, Saturn Arch, and UH-60L Hover Infrared Suppression System (HIRSS) aircraft. The Center also assisted with the operation of IR seekers in the MSIC STV. These tests evaluated the fielded flare IRCM sequences and variations of the sequence with timing and/or pattern adjustments. The Center provided near real-time data reduction and analysis of flare sequences as well as on-site recommendations on flare sequence timing and/or pattern adjustments. As a result, the ARDEC was able to make decisions on flare sequence performance during the course of the test. After the test, the Center provided an independent assessment analysis report. The Army conducted the test in October and November 2016 at Redstone Arsenal.
- Benefit: Center involvement in this test helped ARDEC determine the most effective IRCM flare solution for each platform and prepare its post-test briefing for its higher headquarters, PMO ASE, and each platform's Program Office. The data collected during this effort resulted in a change to the fielded flare sequence for the CH-47F IRSS and UH-60L HIRSS, thus providing better protection for those aircraft against MANPADS.

Navy: P-8A Poseidon Multi-mission Maritime Aircraft (MMA) Flight Test Large Aircraft Infrared Countermeasures (LAIRCM) Next Generation Flight Test

- Sponsor: DON Air Test and Evaluation Squadron VX-20
- Activity: The Center provided MSALTS missile plume simulations as well as personnel to perform two-color, IR simulations to collect system response data to assess the LAIRCM system, as installed on the P-8A during two separately scheduled test events. VX-20 tasked the Air Force 46th Test Wing Test Squadron, Defensive Systems and Mobility Directorate, Air Force Life Cycle Management Center to execute the two test events in November 2016 and March 2017 at Eglin AFB.
- Benefit: The Center collected the critical data that the Navy required to assess the performance of the LAIRCM Next Generation system installed on the P-8A platform.

Army: Common Infrared Countermeasure (CIRCM) Program of Record Contractor Flight Test

- Sponsor: PMO ASE
- Activity: The Center provided one MSALTS for simultaneous UV and IR missile simulations and jam beam data collection. The Center provided the simulator for single threat engagements against the CMWS and CIRCM as installed on the UH-60M. The Army conducted this test to demonstrate production configuration CIRCM end-to-end functional performance on the aircraft per the Contractor System Performance Specification. This test evaluated CIRCM end-to-end functional performance while exposed to own ship motion, vibration, and electromagnetic environments specific to the aircraft. The Army conducted the test from August 28 to September 9, 2017, at TA-6, Redstone Arsenal.
- Benefit: The Center collected data during this effort that allowed the CIRCM contractor to assess the CIRCM capabilities to acquire, track, point, and emit laser energy in both benign and cluttered environments. The test allowed the CIRCM contractor to update hardware/software as needed prior to moving into formal government testing.

Army: AN/APR-39D(V)2 Follow On Test & Evaluation (FOT&E)

- Sponsor: Aviation Test Directorate (AVTD), U.S. Army Operational Test Command (USAOTC)
- Activity: The Center provided support equipment and operators for the Portable Range Threat Simulator (PRTS), GPS event recorder, and video recording in support of the AN/APR-39D(V)2 FOT&E. The PRTS was used to engage and stimulate two AH–64D Apache helicopters equipped with the AN/APR-39D(V)2 during both day and night operational test missions. The Center supported a total of 16 successful missions. The Navy conducted the test from July 15 – 29, 2017, at Electronic Combat Range (ECR), Naval Air Weapons Station (NAWS) China Lake, California.
- Benefit: The PRTS emitted different threats that registered on the AN/APR-39D(V)2. PRTS mobility allowed threat deployment throughout the test range and was a cost-effective way to provide threat stimulations to the AN/APR-39D(V)2.

Navy: Poseidon Multi-mission Maritime Aircraft (MMA) Flight Test LAIRCM Next Generation System Processor Replacements (LSPR) P-8A Flight Test

- Sponsor: DON Air Test and Evaluation Squadron VX-20
- Activity: The Center provided MSALTS missile plume simulations, and personnel to perform two-color, IR simulations to collect system response data to assess the LAIRCM LSPR, as installed on the P-8A test platform. VX-20 tasked the Air Force 46th Test Wing Test Squadron, Defensive Systems and Mobility Directorate, Air Force Life Cycle Management Center to conduct the test event in September 2017 at Eglin AFB.
- Benefit: The Center collected critical data that the Navy required to assess the performance of the LAIRCM Next Generation system installed on the P-8A platform.

TRAINING SUPPORT FOR SERVICE MEMBER EXERCISES

- Sponsors: The Center supported the six Service member exercises listed below:
  - Red Flag 17-1 (January 23 to February 10, 2017) Nellis AFB, Nevada
  - Emerald Warrior 17 (February 27 to March 10, 2017) Hurlburt Field, Florida
  - Northern Edge 17 (May 1 – 10, 2017) Eielson AFB, Alaska
  - Joint Strike Fighter/Close Air Support (May 31 to June 2, 2017) Yuma, Arizona
  - Joint Strike Fighter/Combat Search and Rescue (July 31 to August 4, 2017) NAWS China Lake, California
  - Red Flag 17-4 (August 14 – 25, 2017) Nellis AFB, Nevada
- Activity: The Center provided personnel and equipment to simulate a MANPADS threat environment, as well as SME support, to observe aircraft ASE systems and crew reactions to this environment. Specifically, the Center simulated MANPADS threat engagements for participating aircraft. Additionally, the Center provided MANPADS capabilities and limitations briefings to pilots and crews and conducted familiarization training at the end of the briefings. The Center provided camouflage, concealment, and deception equipment in support of Northern Edge.
- Benefit: Center participation in these exercises provided realism to the training threat environment and enhanced pilot and crew understanding and use of CM equipment, especially ASE. The data the Center collected and provided to the trainers helped the units develop/refine their tactics, techniques, and procedures to enhance survivability.

PGW CM ACTIVITIES

Army: Javelin Lightweight Command Launch Unit (CLU) Testing and Javelin SP3 Flight Matrix Sandbox

- Sponsor: U.S. Army Program Executive Office Missiles and Space, Close Combat Weapon Systems, Javelin
- Activity: The Center provided aerosol obscurant CM deployment SME support for the test planning stages and assisted in the acquisition of pyrotechnics. To help meet the obscurant requirements, the Center provided 50 GG24 smoke grenades. These tests were designed to evaluate system performance in CM environments. The Army conducted testing from August 7 – 11, 2017, at Redstone Arsenal.
- Benefit: The Center provided the projects with aerosol CM environments, which were helpful in data collection used to further improve system performance and increase its effectiveness.

Army: Anti-Tank-Guided Missile (ATGM) Obscurant Testing

- Sponsor: Aberdeen Proving Ground, U.S. Army Research, Development and Engineering Command, Edgewood Chemical Biological Center
- Activity: The Center provided an aerosol obscurant CM SME in support of static pyrotechnic firing to capture repeatable data for projects and the modeling and simulation (M&S) group. The Center further assisted in supplying, shipping, and deploying the GG24 smoke grenades, and in deploying CM aerosols with the M56 E1 smoke generators. The Army conducted ATGM Obscurant Testing from August 7 – 11, 2017, at TA-3, Redstone Arsenal.
- Benefit: The Center provided the projects with aerosol CM environments, which were helpful in data collection used to further improve system performance and increase its overall effectiveness.

Army: Joint Attack Munition System (JAMS), Joint Air-to-Ground Missile (JAGM) Live Drop Testing

- Sponsor: U.S. Army Aviation and Missile Research Development and Engineering Center
- Activity: The Center provided SME support for M239 smoke grenade launcher operations. The Army used the Center's standard operating procedure CCM-053-12, "Detonating Ammunition, Explosives, and Pyrotechnics During Countermeasures Testing," for deploying and training program personnel. Training included the remote M239 smoke grenade firing setup and deployment techniques to ensure that the timing sequences produced effective CMs to meet the test objectives. The Army conducted JAMS JAGM Live Drop Testing from August 14 – 25, 2017, at the U.S. Army Yuma Proving Ground Test Range, Arizona.
- Benefit: The Center provided aerosol CM deployments in different tactical maneuvers, which the Army used to increase target discrimination accuracy and in data collection to further improve the system's performance and increase its overall effectiveness.

T&E TOOLS

The Center continues to develop tools for T&E of ASE. The Joint Standard Instrumentation Suite (JSIS) was funded by the USD(AT&L) Test Resource Management Center's Central T&E Investment Program (CTEIP). Additional investment for the remaining JSIS needs are being pursued via the T&E IR Threat Signatures M&S Roadmap activities of the Joint CM T&E Working Group, which DOT&E and DASD(DT&E) co-chair.

JSIS

JSIS is a transportable, fully integrated instrumentation suite that collects threat signatures; time, space, position information; and related threat missile and hostile fire munitions metadata. JSIS transportability is intended to allow it to be used both in the United States and abroad to reduce costs and expand the types of threat data available in the United States. The Missile and Space Intelligence Center will use the data to create threat models for use in M&S of ASE. The Navy (PMA-272), Army (PMO ASE), and Air Force (LAIRCM System Program Office) have endorsed JSIS, and it will be an integral part of each Program Office's aircraft self-protection capability development. Community SMEs formulated the JSIS' need as part of the IRCM Test Resources Roadmap activities. Near-term needs for operational testing with the Navy's ATW drove JSIS Initial Operational Capability (IOC), which was sponsored by the CTEIP Resource Enhancement Project (REP). A JSIS IOC graduation event in October 2016 exercised JSIS capabilities in an operationally realistic environment. The Center conducted the event at Dugway Proving Ground, Utah, completing over 20 free-flight live fires of MANPADS. In general, JSIS performed as expected, though the Center is addressing improvements in the Kineto Tracking Mount tracking performance in advance of FY18 free-flight live fire events in support of the PMO ASE and PMA-272.

While JSIS represents a significant step forward in fielding data collection capabilities, significant gaps and shortfalls remain. Some of these gaps and shortfalls may be mitigated by expanded missile attitude data collection and additional signature instrumentation to support emerging aircraft self-protection programs with associated M&S needs. The Center has been advocating for additional investment toward achieving the JSIS Full Operational Capability (FOC). The REP Working Group sponsorship will address the missile attitude need in FY17-20.

Threat Signature Generation

In support of the PMO ASE, the Center is generating over 12,000 threat signatures for the CIRCM program. The Center briefed its threat signature generation process to the program, Army Test and Evaluation Command, and Army Validation Working Group. The PMO ASE reviewed the Center's standard operating procedure. To date, 6,700 signatures have been generated. The PMO ASE will use these signatures in labs and open-air testing for evaluating CIRCM performance.

The Center also continually generates signatures that are used as the input signatures for JMITS and MSALTS in open-air missile simulator testing. Over 9,000 signatures have been generated for this purpose.

Additionally, the Center provides signatures to various programs upon request for use in signature model analysis and test activities not involving the Center. Over 700 signatures have been generated for this purpose.

The Center has been a key participant in an M&S Working Group that continually evaluates threat signature models with the goal of improving them and creating uniformity in model version use across the programs.

Remote Launch System Foxtrot (RLS-F) Turret Upgrade

RLS-F was designed to provide a transportable, fully instrumented remote launch capability for MANPADS and vehicle-launched surface-to-air missiles. The Center is currently evaluating bids to replace the current pedestal with a more robust version. IOC is expected during 4QFY18.

JOINT COUNTERMEASURES TEST AND EVALUATION WORKING GROUP

DOT&E and DASD(DT&E) co-chartered the Joint Countermeasures Test and Evaluation (JCMT&E) Working Group to measure, test, and assess the following:

- Aircraft self-protection, CMs, and supporting tactics
- Live fire threat weapons and open-air T&E
- System performance in operationally relevant aircraft installations and combat environments
- T&E methodologies, instrumentation, analysis, and reporting
- Overseas threat and air electronic warfare systems performance and effectiveness data collection in coalition warfare environments

DOT&E, DASD(DT&E), and all four of the U.S. Services participate in the JCMT&E Working Group. In addition, the JCMT&E Working Group works with Australia, Canada, New Zealand, the United Kingdom, and the 22-nation NATO Air Force Armaments Group, Sub-Group 2 to seek common T&E goals. The Working Group is tasked with seeking mutually beneficial T&E opportunities to measure performance and suitability data, which are necessary to provide relevant operational information to deploying joint/coalition Service members and to U.S. acquisition decision-makers. Specific efforts include:

- The JCMT&E Working Group's discussions with the U.S. European Command's Office of Defense Cooperation resulted in a plan to conduct testing and data collection in Finland, Slovenia, Sweden, and the United Kingdom in operationally relevant environments important to the Combatant Command, Warfare Centers, and Programs of Record.
- The JCMT&E Working Group is cooperating with NATO partners and Partnership for Peace nations to provide opportunities to obtain and expand operationally relevant information in order to field new capabilities rapidly and reduce cost by coordinating the T&E efforts of the Center's

Alliance partners with the data needs of the Center's ASE programs.

- The JCMT&E Working Group is building on the Center's proven record of conducting successful ASE data collection by coordinating live firings of radio frequency/electro-optical/IR surface-to-air missiles, hostile fire indication, and anti-tank guided missile firings by active duty air-defense units and test organizations in Bulgaria, Finland, Slovenia, Sweden, and the United Kingdom. These efforts will provide data on the operational performance of actual, modern, multifunction radars and integrated air defense systems that pose threats to U.S. and allied forces.
- The JCMT&E Working Group chair is the U.S. Steering Committee Chairman for bilateral and multinational Cooperative T&E Project Arrangements with Australia, Canada, and the United Kingdom. The JCMT&E Working Group is currently developing similar agreements with Finland and Sweden. These efforts have already expanded the availability of electronic warfare system performance and suitability data to improve aircraft survivability. They have also identified opportunities at U.S. testing facilities to expand the data available for U.S. and allied survivability programs.
- The JCMT&E Working Group is working with U.S. European Command's Office of Defense Cooperation, U.S. Central Command's Military Assistance Program, and the State Department's Office of Weapons Removal and Abatement to expand the availability of threat weapons for use by T&E programs while reducing the number of weapons that pose a serious threat to international security.

Index

Index

FY17 INDEX OF PROGRAMS

www.dote.osd.mil