FY 2021 Annual Report

Director, Operational Test & Evaluation

January 2022

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.

Nickolas H. Guertin
Director

Director's Foreword

On December 20, 2021, following confirmation by the Senate, it was my great privilege to be sworn in as the Director, Operational Test and Evaluation (DOT&E). After a lifetime in the national security sphere, I am deeply honored to join the dedicated women and men who serve as the independent, unbiased assessors of American warfighting capability. The DOT&E mission -- determining a system's operational effectiveness, suitability, and survivability – supports every soldier, sailor, airman, marine, and guardian, along with the strategists and decision-makers in the chain of command.

In order to fulfill congressional mandates and timelines, DOT&E staff completed this critical Annual Report, including the introduction, prior to my taking the oath of office. I deeply appreciate their initiative and diligence. I have reviewed the report's contents and fully support all programmatic findings and recommendations.

Over the next year, I intend to closely examine DOD's operational test and evaluation infrastructure, tools, processes, and workforce, then to vigorously pursue efforts that will prepare the operational T&E community for the coming decade. The mechanisms by which DOD and its industry partners develop new systems are changing rapidly and continuously, as are the capabilities ultimately produced. Test and evaluation must be responsive to these changes and carve new paths so that we can continue to inform the warfighter and perform the work that Congress has asked us to do.

I look forward to collaborating with all stakeholders in the research, development, acquisition, and testing spheres. Together, we will press to achieve maximum impact of the resources taxpayers have provided, and to position our warfighters to fulfill their solemn commitment to the American people: protect our Nation, our freedom, and our way of life.

Nickolas H. Guertin
Director

Introduction

There are three Imperatives of Combat. The first is “believe in your mission;” the second is “believe in your commanders.” For the operational test community, the third imperative holds special significance: “believe in your weapons and equipment.” Our soldiers, sailors, airmen, marines, and guardians, along with DOD leadership and the Congress, count on us to tell them when and where to place that faith. We must not let them down.

As we start the third decade of the 21st century, the United States remains the world's preeminent military power, thanks to our dedicated all-volunteer force, who are committed to their oath to support and defend the Constitution, and the civilians who stand beside and behind our women and men in uniform. Our Armed Forces' intellect, creativity, and countless hours of selfless service fuel America's successful national defense. Those unparalleled intangibles are backed by the technology the Defense Department puts in their hands, which, thus far, has given them the edge necessary to protect our homeland and our allies, and to advance the United States' strategic objectives.

The acquisition and testing communities are responsible for ensuring that this technology continues to provide American forces the decisive advantage they need. On the surface, the operational tester's job may appear simple: determine a system's operational effectiveness and suitability, and the survivability of the system and its operator, in the context of the intended mission. This succinct description belies the challenge in assessing a weapon or other technology in operationally realistic conditions – with the warfighters who will use it, in the expected physical environment, under the tactical conditions and battle plan anticipated, facing threats that accurately replicate our potential adversaries. As the operational test community knows, fulfilling that mandate was never simple and the future offers no respite. U.S. systems are growing more complex; our adversaries are becoming more sophisticated and capable; and joint multi-domain operations, encompassing land, air, sea, space, and cyberspace, are now the driving operating concept. The need to execute rigorous, credible OT&E has not lessened; in fact, it may be more critical than ever. Over the past year, competitors revealed technological advances that match and outpace our own, for instance, in hypersonic missiles. In November 2021, just prior to concluding four decades of service, then Vice Chairman of the Joint Chiefs of Staff General John Hyten remarked that "probably should create a sense of urgency." DOT&E couldn't agree more.

But where should that sense of urgency steer the operational test community? Concerns about being able to conduct proper OT&E are perennial. The Annual Report for Fiscal Year 2000 noted then that "Weapon technologies are outdistancing our ability to adequately test systems as they are developed." That statement remains accurate today. The high-volume wave of new technology in DOD's acquisition pipeline, the rapidly changing threat landscape against which we must evaluate it, and the need to field systems at the ever-quickening speed of relevance will strain or exceed our current infrastructure, tools, processes, and knowledge base.

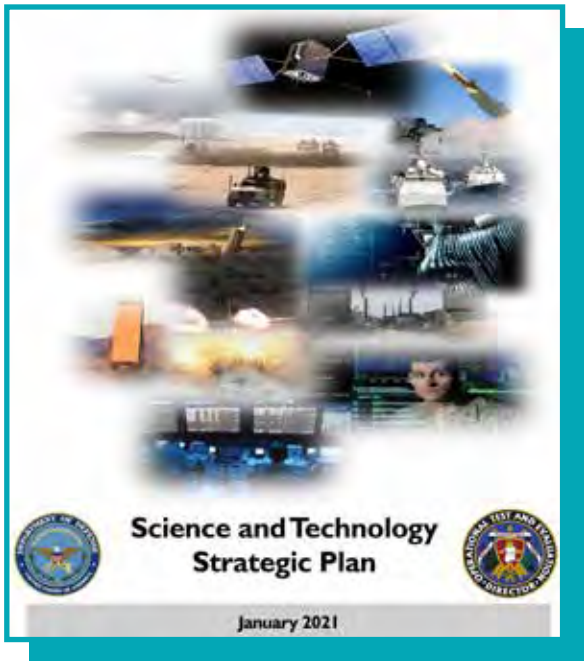
Some of the most frequently cited principles and means to improve acquisition outcomes and T&E efficacy and efficiency aren't novel, either. In 1995, then Secretary of Defense William Perry laid out five themes to guide the strategic direction for T&E. Four of them are equally valid now as they were 26 years ago: earlier involvement of operational testers in the acquisition process; more and more effective use of models and simulations; combining, where possible, different types of testing; and conducting operational testing and training exercises together. Quoting then Under Secretary of Defense (Acquisition, Technology, and Logistics) Jacques Gansler, the FY 2000 Annual Report also highlighted what is now known as the "shift left" mantra: "… serious testing with a view toward operations should be started early in the life of a program. Early testing against operational requirements will provide earlier indications of military usefulness. It is also much less expensive to correct flaws in system design, both hardware and software, if they are identified early in a program. Performance-based acquisition programs reflect our emphasis on satisfying operational requirements vice system specifications." These sentences could have been crafted today.

The nature of most organizations is to change incrementally – that is, to evolve – and the Defense Department is no exception. But the pace of evolution no longer is sufficient for national security writ large, nor operational test and evaluation in particular. Instead, to keep fulfilling our obligation to the warfighter, we need a T&E revolution.

Where the T&E Revolution Should Start

In January 2021, DOT&E released a Science and Technology Strategic Plan to help set the stage. A basic blueprint for operational T&E over the next five years, the S&T Strategic Plan has five focus areas.

Software and Cybersecurity T&E



Software and cybersecurity T&E lead the pack. The vast majority of DOD systems are extremely software-intensive. Software quality, and the system's overall cybersecurity, often are the factors that determine operational effectiveness and survivability, and sometimes lethality. The survivability aspect is especially critical. Many national security experts predict the next Pearl Harbor won't manifest as bombs destroying ships but as key strokes and hidden malware idling a fleet in home port or already at sea – an equally effective attack, with deniability, similar tactical results at lower cost for the adversary, and an unpredictable impact on public opinion due to the lack of visible carnage.

Now more than ever before, getting cybersecurity right on our weapon systems is essential to their actually being useful in the field. Warfighters, commanders, and program managers are relying on operational T&E to tell them what the cybersecurity risks, and their potential consequences, are, and to help them devise mitigation options to fight through a loss of capability. That means we must be certain that we understand the threat and can accurately emulate it during testing, and we can represent the entire attack surface, including the network and other platforms to which the system connects. The use of commercial technologies and services, such as cloud computing, adds another layer of risk to assess: are those commercial products, services, and their supply chains secure and suitable for military use?

The need for a sea change in cybersecurity OT&E is undeniable. The sheer number of systems that should undergo robust cybersecurity testing – that the Congress expects DOD to test – only intensifies that need. Cybersecurity testing must be accurate yet not endanger the operator. It must uncover whether the system is hackable and can be compromised, and what the impacts would be. Is the operator induced to make a bad choice based on spoofed system readings? Is certain offensive or defensive functionality lost, which, in turn, impedes individual or unit mission accomplishment? Or, does the platform shut down entirely?

Strengthening the engineering rigor of our testing is one place to start. We must expand cybersecurity T&E to examine whole-of-platform and systems-of-systems architectures and concepts of operations that reflect joint multi-domain operations. Broader use of automated testing methods, perhaps enhanced by artificial intelligence and machine learning, also is necessary; relying solely on people to conduct cybersecurity OT&E no longer is feasible due to the scale and scope of the testing requirement. Program schedules must accommodate an iterative approach to operationally relevant testing, with time and resources for test-fix-test cycles that begin with the minimum viable product and continue until, and perhaps beyond, a full deployment decision. The operational testing community, and DOD at large, will have to build a much larger and deeper bench of cyber expertise, both in house and outside the department to be tapped on demand, as well.

Getting cybersecurity principles right at the early stages of system design and development – long before operational testing begins – is a step the acquisition community can take to foster system resilience and posture the program for long-term success. Operational testers, and warfighters trained in offensive and defensive cyber operations, have the requisite knowledge. DOT&E is ready to assist any program office in incorporating the right cybersecurity principles that will give its platform the ability to respond to the continuously and rapidly morphing threat.

Transforming T&E to ensure cybersecurity across DOD systems and supporting supply chains will require a collaborative effort with our partners inside DOD, across the federal government, in industry and academia, and among our international allies.

Next-Generation T&E Capabilities

The quality of T&E – and ultimately warfighting capability – depends on the quality of the T&E tools, infrastructure, and processes we use. T&E must be able to handle whatever technologies are presented and it must mirror real-world environments and scenarios, to include accurate threat and countermeasure replication, in order to be thorough, operationally representative, and credible.

The T&E enterprise is not as prepared as it needs to be for the types of systems currently, or soon to be, in the development pipeline. The majority of the Department's open-air test and training ranges and laboratories are outdated and must be modernized to capture the complexities and capabilities of today's and future operational environments. We know already that artificial intelligence, autonomous and adaptive systems, space-based systems, directed energy, hypersonics, and biotechnology will challenge DOD's T&E capacity, facilities, and methodologies. To keep pace with the technological advancements expected on the modern battlefield, and to adequately test and train U.S. and coalition partner forces in complex and dynamic multi-domain operational environments, DOD requires significant and sustained investments in T&E infrastructure. The T&E Resources section of this report provides more detail regarding the critical T&E capability shortcomings that we must address to dominate the next conflict. We almost certainly will discover additional gaps as new technologies and operating concepts arise.

In late 2020, DOT&E commissioned the National Academies of Sciences, Engineering and Medicine (NASEM) to assess the ranges, infrastructure, and tools used for operational T&E. The main question was: Will the Defense Department be able to conduct the robust operational T&E our warfighters deserve on the systems and technologies anticipated in the 2025-2035 timeframe? NASEM completed and released to the public the first segment of that study in September 2021 and expects to finish the second segment, which is classified, in mid to late FY22. DOT&E will review the findings and recommendations from both portions to help inform DOD efforts to develop a holistic, enterprise-wide modernization and investment plan. With 2025 around the corner, DOT&E will press DOD stakeholders to begin implementation immediately.

DOT&E already is working on transforming one of the most important aspects of operational test and evaluation, and the acquisition process overall: data management. Capturing the right data, sharing them with the right people, and making the best data-driven decisions possible in a timely manner are fundamental to testing and fielding high-quality capabilities at the speed of need. The utility of data collected during all phases of T&E – contractor, developmental, integrated, and operational – can be much broader when analyzed as a whole, however. This vast quantity of data potentially could reveal trends in system design and performance, threat replication and emulation, test design and execution, program management, and other areas that would reshape DOD decision-making. But our ability to exploit that treasure trove is currently limited: the Defense Department lacks the means to aggregate, securely store, easily access and query, trace, and quickly analyze the cornucopia of test data it collects.

DOT&E recently engaged outside expertise to help revamp how we handle and use test data, and we would welcome information on other data analytics projects that are underway both inside and outside DOD. Our goal is to partner with other DOD stakeholders to start generating a draft data management capabilities and architecture blueprint.

Integrated T&E Lifecycle

The S&T Strategic Plan's third focus area is instituting an integrated T&E lifecycle. The concept isn't new, yet, to date, DOD has not fully implemented it. DOT&E believes that DOD's best avenue to improving T&E efficacy and efficiency is to greatly reduce, if not eliminate, the traditional contractor, developmental, and operational test silos. We need to replace that segregated, sequential approach with a process that integrates CT, DT, and OT to maximize test efficiency and effectiveness within a mission construct, whenever possible. In practical terms, that means designing test events to collect data that satisfy both DT and OT needs, when able. Additionally, program managers must involve the intended users and testers in developing system specs to ensure that

they're operationally relevant and testable; and contract language to ensure that testing requirements fulfill OT needs as early as possible and the right data are collected.

DOT&E currently is working with the Under Secretary of Defense (Research and Engineering) Developmental Test, Evaluation, and Assessments team to examine how we can expand the integrated T&E window. The goal is to enable agility, efficiency, and expediency. With that in mind, the operational test community must expand its partnership with DT and program offices to maximize integrated testing that provides operationally relevant data.

Digital Transformation

DOD is struggling to keep up with industry's and our adversaries' adoption of digital research and development and T&E capabilities. Besides the need for new tools and data management practices, perhaps the most critical shortcomings are in "digital twinning" and modeling and simulation (M&S). The test community acknowledged the need for M&S more than 20 years ago. That requirement has only become more urgent over time. For a variety of reasons, live operational testing in a threat-representative environment is not always feasible. When that occurs, we must have high-fidelity, operationally realistic M&S venues that produce enough high-confidence data to inform a determination of operational effectiveness, suitability, and survivability. These venues must be constantly refreshed and undergo continuous verification, validation, and accreditation (VV&A), particularly of the system under test and threats portrayed.

Sound VV&A, based on data collected during live (not simulated) events, is critical. The results of certain recent live operational tests diverged significantly from the outcomes predicted by M&S. Creating accurate, high-caliber M&S is a complicated endeavor but we must continue to invest in it and follow through with VV&A to ensure that our warfighters and commanders can trust operational T&E findings.

T&E Workforce: The Essential Human Element

The final focus area is the T&E workforce. T&E of complex technologies requires a tremendous amount of deep and broad cutting-edge expertise. DOD needs mechanisms both to attract more talent to government service and to obtain consistent, on-demand access to experts from academia and industry. DOT&E looks forward to working with DOD stakeholders, industry, and the Congress to improve T&E talent development, access, and management to ensure that the T&E community continues to provide outstanding support to the warfighter over the next decade.

Realigning DOT&E: Strategic Initiatives, Policy, and Emerging Technologies

To help set the conditions for T&E transformation, DOT&E initiated an internal reorganization last summer. In the spirit of integrated T&E, we folded Live Fire Test & Evaluation (LFT&E) functions and personnel into the warfighting domain divisions to better align our efforts. DOT&E's LFT&E expertise and oversight capacity remain the same; the LFT&E program will not be reduced.

To ensure that operational T&E is prepared to fulfill the warfighter's and the decision-maker's demands for credible, independent data and analysis, DOT&E has created a new division focused on the future. The Deputy Director for Strategic Initiatives, Policy, and Emerging Technologies (SIPET) will proactively look forward to identify OT&E needs, gaps, and potential solutions; craft new ways of doing business; and help Service and agency operational test organizations solve problems. Working with stakeholders across the department, SIPET also will develop and refine operational test policy guidance. The first areas SIPET will address include cybersecurity testing guidance and M&S VV&A guidance.

By dedicating personnel to the full-time mission of planning for emerging technology, digging into shared T&E challenges, and big-picture brainstorming, SIPET will foster greater agility and responsiveness in the operational

test community. The intent is that, as a result, we will create the conditions to "shift left" more often, more quickly, and with even better results than we achieve today.

DOT&E has realigned the Annual Report itself, as well. A new Executive Summary highlights major DOT&E products, contributions, and findings from this fiscal year.

Impetus and Way Ahead

Revolutionizing test and evaluation is within our grasp. It will take a concerted effort, and a steady and substantial flow of intellectual and financial resources – but we can achieve it.

Maintaining the status quo is not an option. The Defense Department's 2021 annual report to Congress on military and security developments involving the People's Republic of China noted that our primary pacing challenge "has substantially reorganized its defense-industrial sector to improve weapon system research, development, acquisition, testing, evaluation, and production." For the operational test community to fulfill its role as trusted, unbiased arbiters of a system's performance and its effect on mission accomplishment, DOD's T&E enterprise must stay ahead.

CONTENTS

Director's Foreword	1
Introduction	5
Table of Contents	11
Mission	17
Executive Summary	19
T&E Resources	29
DOD Programs	35
Army Programs	65
Navy Programs	127
Air Force Programs	189
Missile Defense System	233
Cyber Assessment Program (CAP)	241
Center for Countermeasures (CCM)	251
International Test and Evaluation Program (ITEP)	255
Joint Aircraft Survivability Program (JASP)	261
Joint Technical Coordinating Group for Mission Effectiveness (JTCG/ME)	267
Joint Test and Evaluation (JT&E)	275
T&E Threat Resource Activity (TETRA)	281
Appendix	285

CONTENTS

Director's Foreword 1

Introduction 5

Mission 17

Executive Summary 19

Test and Evaluation Resources 29

DOD Programs 35

Aerosol and Vapor Chemical Agent Detector (AVCAD) 37

Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives 39

DOD Healthcare Management System Modernization (DHMSM®) 43

F-35 Joint Strike Fighter (JSF) 45

Joint Biological Tactical Detection System 54

Joint Regional Security Stack (JRSS) 57

Key Management Infrastructure (KMI) 60

Public Key Infrastructure (PKI) Increment 2 62

Army Programs 65

120mm Advanced Multi-Purpose (AMP), XM1147 67

7.62mm Advanced Armor Piercing (ADVAP), M1158 69

Abrams M1A2 System Enhancement Package version 3 (SEPv3) Tank with Trophy Active Protection System (APS) 71

AN/TPQ-53 Counterfire Target Acquisition Radar 73

Armored Multi-Purpose Vehicle (AMPV) 75

Army Integrated Air & Missile Defense (AIAMD) 77

Assured–Positioning, Navigation, and Timing (A–PNT) 79

Bradley Family of Vehicles (BFoV) Engineering Change Proposal (ECP) 82

Command Post Computing Environment (CPCE) 84

Dark Eagle 87

Electronic Warfare Planning and Management Tool (EWPMT) 90
Extended Range Cannon Artillery (ERCA) 91
Handheld Manpack and Small-Form Fit (HMS) Programs – Leader Radio and Manpack 93
Infantry Squad Vehicle (ISV) 95
Integrated Tactical Network (ITN) 98
Integrated Visual Augmentation System (IVAS) 100
Joint Air-to-Ground Missile (JAGM) 102
Joint Assault Bridge (JAB) 104
Joint Light Tactical Vehicle (JLTV) Utility (UTL) and Fire Direction Center (FDC) 106
Long Range Fires 109
M917A3 Heavy Dump Truck (HDT) 111
Maneuver-Short Range Air Defense (M-SHORAD) Increment 1 113
Mobile Protected Firepower 115
Multi-Function Electronic Warfare – Air Large 117
RQ-7Bv2 Block III SHADOW – Tactical Unmanned Aircraft System 119
Soldier Protection System (SPS) 122
Stryker Family of Vehicles (FoV) 125

Navy Programs 127

Advanced Anti-Radiation Guided Missile - Extended Range (AARGM-ER) 129
Aegis Modernization Program 131
AIM-9X Air-to-Air Missile Upgrade Block II 134
CH-53K King Stallion 136
CMV-22B Joint Services Advanced Vertical Lift Aircraft – Osprey – Carrier Onboard Delivery 138
Conventional Prompt Strike 140
CVN 78 *Gerald R. Ford*-Class Nuclear Aircraft Carrier 142
DDG 1000 – *Zumwalt*-Class Destroyer 146
Evolved Sea Sparrow Missile Block 2 148
F/A-18 Infrared Search and Track Block II 150
F/A-18E/F Super Hornet 152
FFG 62 *Constellation* Class – Guided Missile Frigate 155
LHA 6 Flight 1 (LHA 8) Amphibious Assault Ship 157
Littoral Combat Ship (LCS) 159

Mk 48 Torpedo Modifications 162
Mk 54 Lightweight Torpedo Upgrades Including the High Altitude Anti-Submarine Warfare Weapon Capability (HAAWC) 164
MQ-4C Triton 167
MQ-8 Fire Scout Unmanned Aircraft System (UAS) 169
Next Generation Jammer Mid-Band(NGJ-MB) 171
Offensive Anti-Surface Warfare (OASuW) Increment 1 174
Over-The-Horizon Weapons System (OTH-WS) 176
Ship Self-Defense System (SSDS) Mk 2 Integrated Combat Systems 178
Surface Electronic Warfare Improvement Program (SEWIP) Block 2 181
Tactical Tomahawk Modernization 183
Unmanned Influence Sweep System (UISS) Including Unmanned Surface Vessel (USV) and Unmanned Surface Sweep System (US3) 185
VH-92A® Presidential Helicopter Replacement Program. 187

Air Force Programs. 189

AGM-183A Air-Launched Rapid Response Weapon 191
AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM) 194
Air Operations Center–Weapon System (AOC-WS) 196
B-52H Commercial Engine Replacement Program (CERP) 198
B-52 Radar Modernization Program (RMP) 200
F-15 Eagle Passive Active Warning and Survivability System (EPAWSS). 202
F-15 Eagle Integrated Infrared Search and Track 205
F-16 Radar Modernization Program 207
F-22A – Raptor Advanced Tactical Fighter Aircraft 209
Family of Advanced Beyond Line-of-Sight Terminals (FAB-T). 211
Global Positioning System (GPS) Enterprise 212
HH-60W Jolly Green II. 216
Joint Cyber Warfighting Architecture (JCWA) 218
KC-46A Pegasus 220
Massive Ordnance Penetrator Modification 223
MH-139A Grey Wolf 225
Presidential and National Voice Conferencing (PNVC) Integrator 227
Small Diameter Bomb Increment II 228

Wide Area Surveillance 230

Missile Defense System 233

Cyber Assessment Program 241

Center for Countermeasures 251

International Test and Evaluation Program 255

Joint Aircraft Survivability Program 261

Joint Technical Coordinating Group for Munitions Effectiveness 267

Joint Test and Evaluation 275

Test and Evaluation Threat Resource Activity 281

Appendix 285

Oversight List 287

DOT&E Activities 293

Acting Director Dr. Raymond O'Toole SASC Statement for the Record 299

Acting Director Dr. Raymond O'Toole HASC Statement for the Record 307

Service Secretary Comments 313

Index of Programs 321

Mission

The Director, Operational Test and Evaluation (DOT&E) is senior advisor to the Secretary of Defense on operational test and evaluation (OT&E) and live fire test and evaluation (LFT&E) in the DOD.

DOT&E's mission is to:

- Enable adequate OT&E and LFT&E of DOD weapon systems in operationally representative and relevant conditions to support credible evaluation of the operational effectiveness, suitability, survivability, and lethality of DOD weapon systems in combat. Adequate T&E enables the delivery and fielding of proven capability to warfighters, and allows them to plan and execute their missions while informed by the weapon system's demonstrated performance. Adequate T&E characterizes those portions of the operational envelope where the weapon system performs well and where deficiencies exist, so they can be fixed prior to fielding and prior to their use in conflict.
- Document weapon system performance and any vulnerabilities in an independent and objective report to Congress and the Secretary of Defense. Each DOT&E report summarizes the assessment of the adequacy of the testing executed in support of the evaluation, as well as the Director's assessment of the operational effectiveness, suitability, survivability, and lethality of the unit equipped with the system under test. The report also offers practical recommendations to fix identified deficiencies and address any gaps that precluded a complete evaluation of system performance as it would be used in combat.
- Report on the health of the T&E resources needed to adequately execute OT&E and LFT&E, including operational test facilities and equipment.
- Identify best practices, develop improved testing methodologies, and implement lessons learned through updates to T&E policy and guidance to meet the T&E and acquisition demands of today and tomorrow. Current efforts include, among others, improved cybersecurity testing, software testing, integrated testing, electromagnetic spectrum operations, modeling and simulation validation, and efficient test methodologies.

DOT&E responsibilities are detailed in the legislation codified in 1983 (Title 10, Sections 139, 2399, and 2400) and then in 1986 (Title 10, Section 2366). These responsibilities were established to support the fielding of weapon systems that work in combat regardless of the competing acquisition priorities. DOT&E responsibilities have since been augmented through a range of subsequent National Defense Authorization Acts, DOD Directives, and DOD Instructions. DOD Directive 5141.02 assigns the following, critical DOD programs and activities to DOT&E:

1. **The Joint Test & Evaluation Program** – DOD's developer of non-materiel solutions (tactics, techniques, and procedures) intended to mitigate operational deficiencies as outlined in **DoDI 5010.41**.
2. **The Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME)** and the **Joint Live Fire program (JLF)** – DOD's developer of weaponeering tools for mission planning and execution across warfare domains.
3. **Joint Aircraft Survivability Program (JASP)** – DOD's developer of T&E tools and solutions to assess and mitigate U.S. aircraft losses in combat.
4. **The Center for Countermeasures (CCM)** – enables T&E of U.S. and foreign countermeasure/counter-countermeasure systems as outlined in **DoDI 5129.47**.
5. **International Test and Evaluation (IT&E) Program** – established to enable T&E activities authorized under international agreements for reciprocal use of ranges and resources.
6. **The T&E Threat Resource Activity (TETRA)** – established to support operational and live fire T&E programs with relevant intelligence data.

Executive Summary

Operational and LFT&E is essential to demonstrate weapon system performance and provide DOD mission planners, commanders, operators, and maintainers with an understanding of true weapon system capabilities, and data to adequately plan and execute their mission in combat. In FY21, DOT&E provided oversight for 237 acquisition programs and published its first Science and Technology Strategy.

Major Products

In FY21, DOT&E provided operational and live fire test and evaluation oversight for 237 acquisition programs at various stages in their acquisition cycle.[1] Specifically, DOT&E reviewed and approved 26 Test and Evaluation Master Plans (TEMPs), 9 of which included a Live Fire Test and Evaluation (LFT&E) Strategy; 2 separate LFT&E Strategies; and 56 individual test plans.

DOT&E evaluates the adequacy of the Service test strategies and plans based on the degree that they will provide: 1) data to support credible evaluation of operational effectiveness and operational suitability, 2) coverage of the battlespace and threats, 3) adequate use of modeling and simulation (M&S), 4) complete cybersecurity and live fire assessments, including demonstration of system survivability and lethality against mission-relevant threats, 5) production-representative test articles, 6) operational realism, and 7) sufficient funding required to support test execution.

DOT&E published 26 reports, including 23 reports to Congress and the Secretary of Defense, and a classified annual report on the Ballistic Missile Defense Systems. In addition to the assessment of test adequacy, DOT&E reports summarize the Director's independent assessment of operational effectiveness, lethality, suitability, and survivability of DOD weapon systems in expected combat conditions. In instances where operational and live fire testing and evaluation have not yet been completed, DOT&E provides an interim assessment and identifies any risk to accomplishing the required operational performance in upcoming operational and live fire test, prior to fielding or the next acquisition decision review. DOT&E reports summarize practical recommendations intended to fix the identified deficiencies and improve the operational performance of the weapon system in expected operational scenarios and conditions to minimize risk to warfighters and maximize probability of mission success in conflict.

In FY21, DOT&E published its first Science and Technology Strategy focused on addressing the following T&E challenges: 1) software and cyber T&E, 2) next generation T&E capabilities, 3) needed integrated T&E lifecycle, 4) digital transformation, and 5) workforce expertise and partnerships. DOT&E intends for these strategic initiatives to inform emerging T&E policy and guidance and enable agile yet credible T&E that can adequately support acquisition reforms while responding to the emerging technology requirements and the increasingly complex and dynamic multi-domain operational environment.

In March 2021, in response to the FY21 Department of Defense Appropriations Act, DOT&E published a follow-on suitability assessment of MHS GENESIS. In April 2021, DOT&E testified before the Senate Armed Services Committee Readiness Subcommittee on the performance of the DOD acquisition, while in July 2021, DOT&E testified before the House Armed Service Committee, Tactical Air and Land Forces Subcommittee on the FY22 budget request for the DOD for fixed-wing tactical and training aircraft programs. In May 2021, in response to the Senate Appropriations Committee, Explanatory Statement for the Department of Defense Appropriations Bill, 2021, DOT&E published the Certification of Appropriateness of Services' Planned Test Strategies for Approved Middle Tier of Acquisition (804) and Accelerated Acquisition Programs report. Lastly, Table 1 provides the status of several completed and ongoing activities in response to the FY20 and FY21 National Defense Authorization Acts (NDAA).

1 The number of programs on DOT&E oversight fluctuates throughout the year; 237 is the number of programs on DOT&E oversight as of September 30, 2021.

Table 1. Summary of DOT&E NDAA Activities		
Section #	**Title**	**Status**
FY 2020 NDAA		
231	Digital Engineering Capability to Automate Testing and Evaluation	Ongoing; DOT&E in support of R&E
800	Authority for Continuous Integration and Delivery of Software Applications and Upgrades to Embedded Systems	Complete with publication of DOD Instruction 5000.89
FY 2021 NDAA		
112	Report on limitations of Integrated Visual Augmentation System (IVAS)	Ongoing
159	Documentation Related to F-35 Program	Ongoing
162	Briefings on Software Regression Testing for F-35	Ongoing; A&S develop quarterly briefings in consultation with DOT&E
222	Activities to Improve Fielding of Air Force Hypersonic Capabilities	Ongoing; R&E to deliver report in consultation with DOT&E
271	Modification to Annual Report of the Director of Operational Test and Evaluation	Adds 1 year to sunset date of DOT&E Annual Report
277	Independent Evaluation of Personal Protective and Diagnostic Testing Equipment	Complete
836	Digital Modernization of Analytical and Decision-Support Processes for Managing and Overseeing Department of Defense Acquisition Programs	DOT&E is a member of the Steering Committee

Major Contributions

Ensure Adequate Testing in Combat Representative Conditions

In FY21, DOT&E continued to highlight and correct instances where proposed test plans were not adequate. Based on the test plans that DOT&E reviewed in FY21, common shortfalls were associated with data collection plans, deficiencies with M&S fidelity or validation, test resources constraints, and insufficient coverage of the operational environment and threats, including insufficient test scope and threat realism for cyber assessments. To address these test shortfalls, DOT&E worked with program stakeholders to improve the test adequacy of plans.

In addition, because some test shortfalls result from range infrastructure challenges, DOT&E recruited the National Academies of Sciences, Engineering, and Medicine to conduct a study on the health and readiness of the DOD test ranges and associated infrastructure for future operational and live fire testing. DOT&E also established a T&E resources and infrastructure working group responsible for cataloging and resolving operational and LFT&E resource and infrastructure shortfalls in coordination with USD(R&E) and other DOD stakeholders.

The National Academies of Sciences, Engineering, and Medicine published their report in September 2021 offering the following five major recommendations: 1) develop the "range of the future" to test complete kill chains in Joint All Domain Operational environments, 2) restructure the range capability requirements process for continuous modernization and sustainment, 3) bootstrap a new range operating system for ubiquitous M&S throughout the weapon system development and test life cycle, 4) create the "TestDevOps" digital infrastructure for future operational testing and seamless range enterprise interoperability, and 5) reinvent the range enterprise funding model for responsiveness, effectiveness, and flexibility. DOT&E is evaluating the National Academies' recommendations and will work with DOD stakeholders to address each as appropriate, and as resources allow.

In parallel, through the newly-formed T&E resources and infrastructure working group, and in coordination with the Test Resources Management Center in USD(R&E), DOT&E initiated the development of more representative electronic warfare testing at Navy sea and land ranges, a threat torpedo capable of simulating a range of acoustic signatures, the acquisition of miniaturized instrumentation for data collection from unmanned aerial system threats, and continued the development of the next generation aerial target.

Ensure Adequate Testing Across any Acquisition Pathway

The DOD has made significant changes to its acquisition policies to support the National Defense Strategy goal of delivering performance at the speed of relevance. To support faster delivery of proven warfighting capability, in November 2020, DOT&E, in conjunction with USD(R&E), USD(A&S), and Service T&E executives, supported the publication of a DOD Instruction 5000.89, which provides T&E procedures for new acquisition pathways that include Urgent Capability Acquisition, Middle Tier Acquisition, Major Capability Acquisition, Software Acquisition, and Defense Business Systems.[2] Significant efforts are underway to provide the T&E community with the tools, architectures, and methods required to optimize the benefits of integrated testing, digital engineering tools and enable agile T&E without compromising the credibility of operational performance evaluation. Such improvements will be documented in the Enterprise T&E Guidebook that is being developed by DOT&E and USD(R&E) to provide the DOD Acquisition and T&E communities the tailorable guidance they require to ensure adequate developmental, operational, and live fire T&E for each of the acquisition pathways.

In the interim, in FY21, DOT&E assessed the appropriateness of test strategies for 86 programs approved by the Service Acquisition Executives to pursue accelerated acquisition authorities. DOT&E reviewed 47 test strategies (the remaining 35 were not made available for review) and certified 33 of those as appropriate, while observing the following: 1) test strategies frequently lack well-defined resources to plan and execute operational testing, or to train operators, maintainers, and cyber defenders, 2) test strategies lack the rigor typically required to demonstrate operational effectiveness, suitability, survivability, and lethality, 3) adoption of integrated test approaches with rapid test/fix/test cycles to enable agility has begun to stress the Service operational test agencies and developmental test organizations, which are currently not resourced, staffed, or trained for the continuous level of effort and reporting required by such approaches.

Transforming T&E Concept of Operations

The increasing complexity of U.S. weapons systems and the capabilities of our potential adversaries, compounded with the parallel, increasing complexity of the environments in which combat will be conducted, continue to underscore the importance and need for transforming T&E concept of operations. As the warfighting capability continues to evolve to support the DOD's ability to fight and dominate in a multi-domain operational environment, the T&E community will require innovative and enterprise-level approaches to enable realistic testing, both live and virtual. To support the new T&E concepts, DOT&E has emphasized the need for investments in: 1) tools to automate testing and visualize the test space and mission effects, 2) data collection, storage, and analytics improvements, 3) improved virtual environments and M&S tools that are credible and validated by live data, 4) tools and methods such as sequential testing and uncertainty quantification to optimize integrated T&E, and 5) tools and methods to test autonomous and artificial intelligence (AI) enabled systems, hypersonic weapons, directed energy weapons, space systems, and other emerging T&E challenges. To adequately focus on meeting these and similar objectives, DOT&E established a new Deputate for Strategic Initiatives, Policy, and Emerging Technologies (SIPET). Notable FY21 efforts in this domain can be grouped into five major lines of effort:

2 DOT&E and USD(R&E) are assessing the inclusion of the Acquisition of Services Pathway in the next update to DoDI 5000.89

1. Enhance Software and Cyber Testing and Evaluation

In FY21, DOT&E established a team of software and cyberspace experts from across the organization to orchestrate internal and external efforts to improve cyber T&E and DOD cyber strategic initiatives. Specific objectives include: 1) improving cyber threat representation, 2) optimizing mission-focused cyber assessments, 3) increasing the availability and integration of cyber expertise, 4) increasing the understanding and inclusion of cyber OT&E of defensive countermeasures in cyberspace, 5) enhancing OT&E of DOD's cyberspace attack and enabling capabilities, and 6) emphasizing vulnerability management in all phases of a program's lifecycle. Initiatives to improve standardization of cyber T&E data and to assess effects from the supply chain are also underway.

2. Develop Next-Generation T&E Capabilities

As AI and autonomy advance to become an integral part of the DOD mission space, DOT&E is teaming up with the Joint Artificial Intelligence Center and USD(R&E) to develop a T&E roadmap for such systems. While Industry's approaches, best practices, and technologies are informative, they do not address the suite of challenges and needs when evaluating DOD capabilities that operate in complex and degraded environments and inform strategic and tactical decisions critical to national security. The roadmap aims to ensure that the larger T&E community is developing the test strategies, practices, methods, infrastructure, data tools, workforce, and other T&E needs as AI-based systems and technologies mature.

3. Enable Optimal Integration of T&E Across the Program Lifecycle

The DoDI 5000.89 policy emphasizes the importance of integrated testing to increase the efficiency of the overall T&E program by planning test events that provide data for multiple objectives. Integrated testing provides programs with the opportunity to identify problems earlier in developmental test, improve production readiness, and shorten the acquisition timeline by leveraging more operationally relevant data across the acquisition cycle. Specifically, DOT&E has partnered with USD(R&E) to expedite the implementation of an integrated decision support key framework intended to ensure data-based acquisition decisions. This guidance will provide a more structured and standardized approach for program stakeholders to align decision points with the operational and technical evaluations and events necessary to inform decisions. Using this framework, testing could be planned in a mission context with operational end users earlier by adopting test design methodologies, such as sequential methods. Using these methods for test planning, execution, and evaluation, individual test events build upon each other and are refined based on previous test outcomes, avoiding redundancies without compromising the credibility of the evaluation.

4. Enable Digital Transformation to Advance T&E Efficiency

In partnership with USD(R&E)-TRMC, DOT&E led the selection and execution of five demonstrations showcasing applications of digital engineering paradigms as called for in the FY20 NDAA Section 231 study, "Digital Engineering Capability to Automate T&E." Demonstration results, still preliminary, suggest improvements spanning attributes such as quality, cycle time, predictability, and costs. This work spawned a number of related digital transformation initiatives, to include: FY22 NDAA Section 217, "Development and Implementation of Digital Technologies for Survivability and Lethality Testing," as well as initiatives in agile Verification, Validation, and Accreditation (VV&A), and an assessment of digital twins.

Separately, in September 2021, DOT&E kicked off an internal initiative to improve T&E data management by automating the manual processes of searching and aggregating data elements from various artifacts. An initial proof of concept will demonstrate the ability to ingest a variety of unstructured documents and automatically process them into a readable machine learning format, giving the T&E community the ability to quickly and easily identify information required to inform requirements, users, materiel developers, and acquisition decisions.

5. Prepare the T&E Workforce for the Future

In August 2021, DOT&E initiated a technical workforce assessment to better understand and develop the knowledge, skills, and abilities the T&E workforce needs to execute its mission as DOD weapon systems evolve. This effort is crucial to ensure the organization is optimally structured, organized, and postured for success. Over the coming months, DOT&E will develop a Technical Skills and Manpower Report and Strategic Workforce Plan detailing the challenges, opportunities, and actionable steps DOT&E can take to best position the T&E workforce to meet the mission of today and the future. Our greatest asset is our workforce, and this assessment will help DOT&E provide its people the support and resources they need to stay ahead of evolutions and revolutions in T&E.

In addition to the workforce assessment, DOT&E partnered with Cyber Test Teams across the Services to complete the first year of Software and Cyber Network of Excellence for Testing (SCyNET) pathfinding activities. These pathfinding initiatives are identifying requirements, defining the business case, and documenting lessons learned for institutionalizing a long-term capability, provided in the form of university-based service providers, to address strategic T&E gaps. This real-time DOD operator and university researcher connection has both solved problems and developed a DOD-university relationship for future work and collaboration.

Demonstrating the Value of T&E

T&E is essential to demonstrate weapon system performance and provide DOD mission planners, commanders, operators and maintainers with an understanding of true weapon system capabilities and data to adequately plan and execute their missions in combat. Examples of this can be found in the Joint Technical Coordinating Group for Munition Effectiveness, Joint Test and Evaluation, and Cyber Assessment Program sections of this report. Specifically, DOT&E cyber-related activities have helped the DOD characterize cyber effects on mission performance, identify network and system vulnerabilities, assess operational concepts and procedures, enhance cyber team capabilities, update guidance and methodologies, facilitate operational assessment of offensive cyber capabilities, and inform the Department on cyber considerations of initiatives and technologies such as the move to commercial cloud-based computing. DOT&E cybersecurity assessments have uncovered important vulnerabilities that, if corrected, will improve the Department's resilience against cyberattacks. T&E, in general, identifies warfighting performance shortfalls that could and should be addressed prior to weapon system fielding or the next acquisition decision. This identification permits corrective action to be taken before large quantities of a system are procured and avoids expensive retrofit of system modifications. An example includes the full ship shock trial testing on the CVN 78 that identified several CVN 78 design shortfalls that, if addressed, could improve the survivability of the CVN 78 against underwater torpedo or mine engagements. The performance trends section below provides additional detail on the value of T&E.

Major Findings

Test Adequacy Trends

Consistent with DOT&E reports from previous years, in FY21, DOT&E reported that 62 percent (13 of 21) of programs conducted adequate operational testing, as detailed in Figure 1.[3] Of the eight programs assessed as not adequate or partially adequate, five programs reported cyber testing inadequacies due to limited breadth of coverage; insufficient collection of data on mission effects and the ability to prevent,

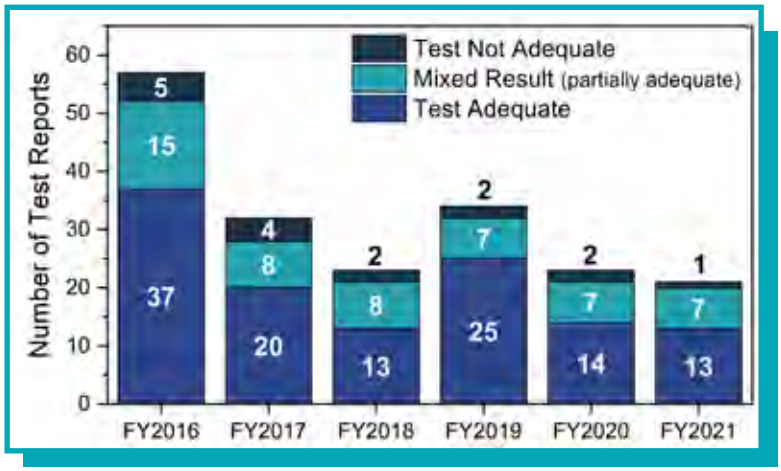


Figure 1. Test Adequacy Trends in DOT&E Reports

3 Five FY21 reports were excluded where DOT&E did not make a test adequacy assessment.

mitigate, and recover from attacks; and lack of sufficient funding. Three programs reported deficiencies with M&S fidelity or model validation. Two programs reported that the most challenging threats were not considered or the threat used was not portrayed properly. Other test adequacy issues included contractor support that is not combat representative, failure to collect or deliver all required data, and system developmental delays that led to incomplete testing.

In addition to test adequacy concerns, DOT&E reports identified other test execution limitations. Common test limitations included inadequate data collection, test range environmental restrictions that prevented a robust operational assessment, unrealistic maintenance due to overreliance on field support representatives, limited doctrinal training resources that prevented full use of new system capabilities, and operational testing being limited to one environment or not covering all required threats, such as electronic attack. For eight programs, COVID-19 hindered full test participations of all T&E stakeholders, which affected data collection and the availability of supporting assets and other resources.

DOT&E-approved test plans also provide insights into known test limitations. As shown in Figure 2, survivability was the most common type of test plan limitation, followed, in order, by limitations that affected DOT&E's assessment of effectiveness and suitability. The majority (93 percent) of survivability limitations were due to cybersecurity. Twenty-four of the 56 test plans in FY21 were focused only on cybersecurity and all but two identified cybersecurity limitations. Common cyber test limitations included lack of advanced cyberattack capabilities by cyber Red Teams, inadequate coverage of all attack vectors due to concerns with safety or the compromise of live operational networks, the need for a more robust supply chain assessment, missing test resources such as data connection cables, insufficient time for Red Teams to probe all possible threat vectors, and lack of an available full-up system. Other common test limitations included M&S or model VV&A deficiencies that were sometimes due to lack of an available full-up system.

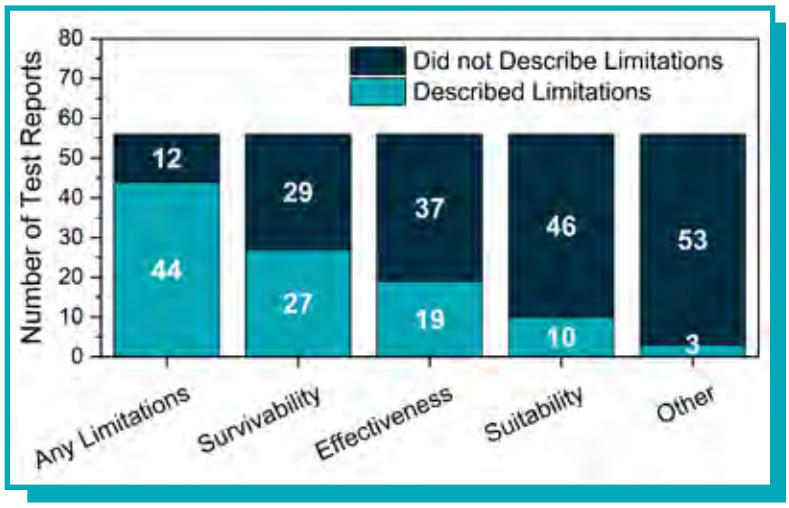


Figure 2. Limitations in DOT&E FY21 Test Plans by Area

Performance Trends

Figures 3 through 5 show the result of DOT&E assessments of operational effectiveness, operational suitability, and survivability since FY16. The figures exclude reports where DOT&E did not make an assessment because the test event was too early in the acquisition cycle, was narrow in scope, or had limitations that precluded an assessment of operational performance.

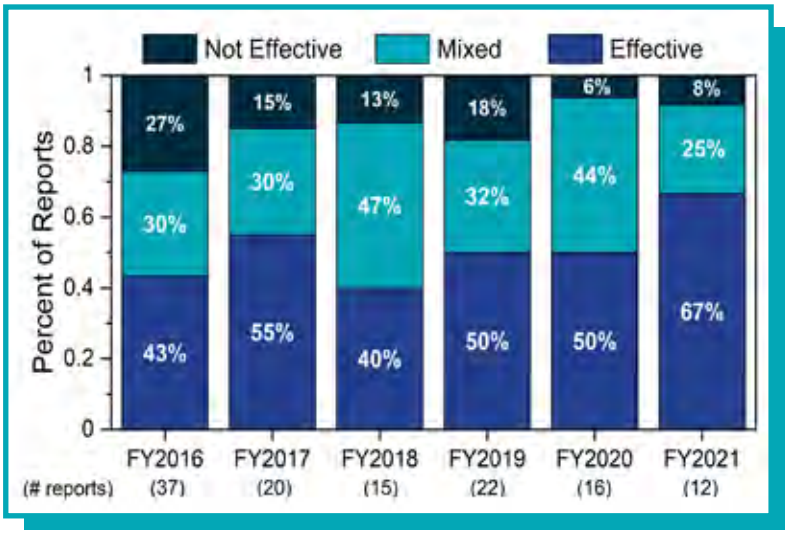


Figure 3. DOT&E Operational Effectiveness Trends

Effectiveness

In FY21, DOT&E evaluated 67 percent of programs to be operationally effective without any caveats. Reasons for systems being not operationally effective included: system, software, or integration deficiencies; training limitations that affected operator performance or unit effectiveness; and

shortcomings when operating in particular environments, mission areas, or against specific threats. Programs that conducted early user testing, including operational assessments before Milestone C, were able to identify operational problems early, providing a greater opportunity to influence the design and make corrections prior to fielding. For example, the IVAS program conducted several Solider Touch Point events in order to test system prototypes in an operational, mission-based environment, and obtain early feedback from military users to support design refinements. In contrast, DOT&E has observed the consequences of not conducting early operational assessments. The F-35 program produced and fielded aircraft, avionics changes, and software releases prior to completing operational test (OT) and analysis. As a result, the OT and user communities continue to discover significant problems with the F-35, through both testing and actual employment in the field.

Suitability

In FY21, DOT&E assessed approximately half of programs to be operationally suitable without any caveats, a trend that has been relatively consistent since FY16. Suitability shortfalls were spread across Human System Integration (HSI), reliability, availability, and safety. Most notably, 80 percent of programs that assessed human factors reported HSI deficiencies. The most common causes of degraded HSI were training deficiencies resulting from incomplete or inaccurate documentation, poor usability, and high workload. Operators and maintainers frequently reported that they would benefit from additional hands-on training. Fifty percent of reports that included a determination on reliability found that the system was reliable enough to support the mission without caveats. Reliability shortfalls resulted from both hardware and software deficiencies. A larger percentage of reports found systems to be maintainable (71 percent) and available (77 percent) without caveats.

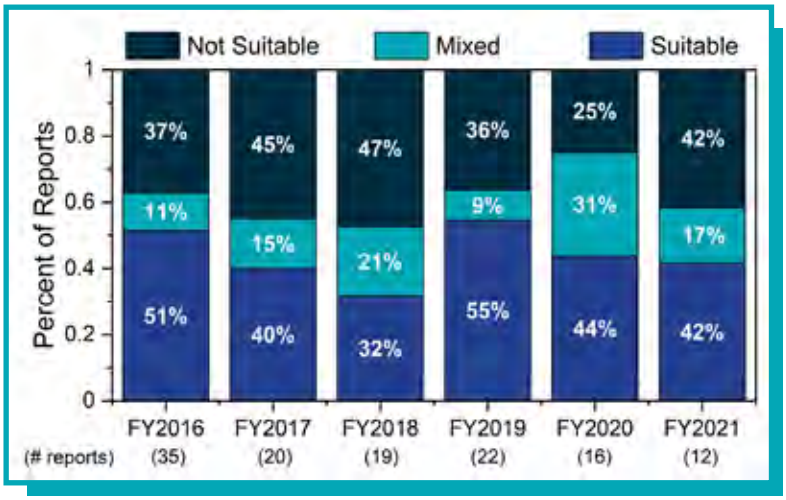


Figure 4. DOT&E Operational Suitability Trends

Survivability

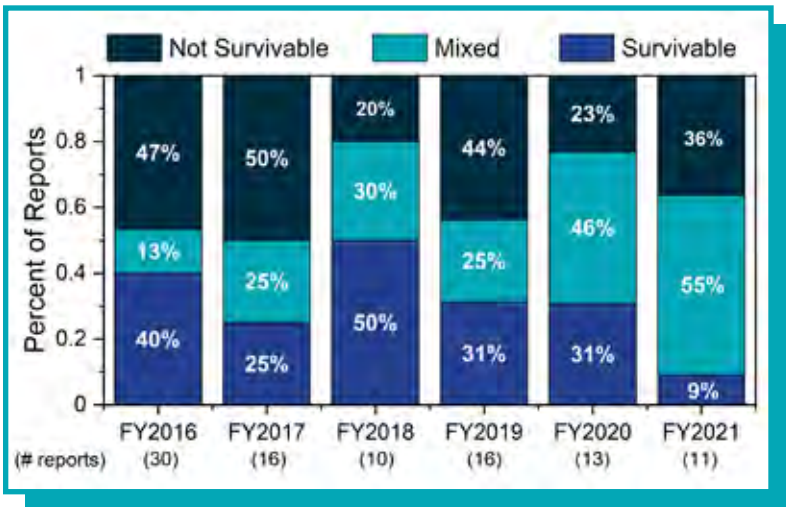


Figure 5. DOT&E Survivability Trends

In FY21, DOT&E assessed nine percent of programs to be survivable without any caveats, a significantly lower percentage than in FY16. Given the complexity of the multi-domain operational environment, the cyber threats, and the contested electromagnetic spectrum environment, survivability assessments are becoming increasingly multi-faceted, and the fraction of programs demonstrating poor survivability has increased over time. Cybersecurity was the most common survivability problem. Cybersecurity issues included supply chain vulnerabilities, unencrypted software, and system-unique vulnerabilities to a wide spectrum of cyber threats. Other survivability shortfalls included challenges with operating in a contested electronic warfare environment and vulnerabilities to specific kinetic threats unique to the system designs.

Recommendations

The following recommendations would better posture a program for success during operational testing:

1. Program managers should develop robust cybersecurity T&E strategies, which include an assessment of supply chain vulnerabilities; consideration of cybersecurity in the design phase to reduce potential attack vectors; collection of data to evaluate mission effects and the ability to prevent, mitigate, and recover from attacks; sufficient coverage of the system's attack surface; and early correction of deficiencies to improve the likelihood of being assessed as survivable during operational testing.
2. Program managers should develop adequate M&S, as a complement to live testing, supported by an independent VV&A process that uses credible and relevant data. M&S is increasingly necessary for development, integration, and mission-level evaluation due to the complexity of DOD systems, the importance and difficulty of representing complex operating environments, and the growing sophistication of our adversaries' weapon systems.
3. Program managers should ensure adequate rigor of HSI assessments by evaluating HSI early in the design phase and throughout development so that deficiencies can be discovered and addressed prior to operational testing. Program managers should also plan for sufficient operator and maintainer training commensurate with the level of system complexity. For many systems, the degree of hands-on and unit collective training should be expanded, and more attention should be paid to improving reliability and developing, refining, and validating operator and maintenance manuals prior to operational testing.
4. Program managers should conduct early, operationally realistic test events, including Operational Assessments, Limited User Tests, and Integrated Testing, where possible. When conducted early in a program's development and when adequately resourced across the acquisition cycle, operationally-realistic T&E offers a unique opportunity to identify and correct problems before the program matures. Early problem discovery allows the program manger to manage cost and schedule later in the process, and fix problems early so that they are not discovered for the first time in the final operational test, the field, or worse, in combat. For this to work, program managers must structure their contracts to require demonstration of operationally relevant, mission-level goals during early testing, instead of focusing solely on specification compliance.

Test and Evaluation Resources

T&E infrastructure must enable credible and comprehensive performance assessments of DOD weapon systems in operationally representative environments.

To keep pace with the expected technological advancements in the modern battlefield, and to adequately test and train U.S. and coalition partner forces in projected multi-domain operational environments, the DOD requires significant and sustained investments in Test and Evaluation (T&E) infrastructure. Specifically, the majority of the Department's open-air test and training ranges and laboratories are outdated and must be modernized to represent and capture the complexities and capabilities of the operational environments of today and the future.

Security regulations, spectrum and range space access constraints, safety considerations, and other limitations, in addition to the sheer cost of live system testing, inherently limit the amount of live testing that is practically achievable. The cost and complexity of hardware-in-the-loop ground-test facilities effectively preclude their development for large-force, multi-domain test and training events. Accordingly, investments are needed to enable solutions to augment the physical test infrastructure with credible digital environments and modeling and simulation (M&S) tools.

Lastly, while the Department recognizes the need to enable T&E of all-domain operations, further investments will expedite the enhancement of test productivity by leveraging and optimizing the benefits of digital engineering tools to standardize data collection and reduction management, as well as data analytics. This section details the specific shortfalls and recommendations in the areas of hypersonics, directed energy weapons, cyber security, nuclear modernization, electromagnetic warfare, space, autonomous and artificial intelligence (AI)-enabled systems, multi-domain operations, common range infrastructure, threat and target surrogates, knowledge management and big data analytics, range sustainability, and the T&E workforce.

Hypersonic Missile and Hypersonic Missile Defense

Hypersonic missiles are designed to achieve speeds between Mach 5 and 20 in the atmosphere, fly distances that can exceed 1,000 miles, and perform extensive maneuvers. The performance evaluation of such systems requires the following T&E capabilities:

- Long-range missile flight test corridors, to include overland corridors
- Range instrumentation sensors to adequately characterize critical aspects of hypersonic flight, from launch, through booster separation and hypersonic vehicle flight with cross-range maneuvers, to impact
- Representative threat targets to adequately evaluate the lethality of U.S. hypersonic missiles
- Foreign missile defense system surrogates (e.g., directed energy weapons, kinetic, countermeasures) to evaluate the survivability of U.S. hypersonic missiles
- Threat hypersonic missile surrogates to evaluate the effectiveness of U.S. defensive capabilities against incoming hypersonic missiles

More detailed shortfalls are included in the Controlled Unclassified Information edition of this report.

Directed Energy

Directed Energy Weapons (DEW) are designed to disable large numbers of adversary targets at fast rates using concentrated energy in the form of high-energy lasers (HEL) or High Power Microwaves (HPM). The DOD needs the following capabilities to safely and effectively test DEW:

- Instrumentation for laser beam diagnostics, to include atmospheric effects on beam properties
- Tools for range safety, satellite deconfliction, and predictive avoidance
- Open-air target boards for measuring laser energy on various targets
- Survivable targets and target instrumentation to evaluate HEL system effectiveness in a measurable, repeatable manner
- A vulnerability data library that includes intelligence-based information regarding target failure mechanisms

The ongoing Mobile High Energy Laser Measurement (MHELM) project is supporting the advancement of these capabilities.

HPM lethal effects focus on disrupting, degrading, or destroying targeted electronic systems or circuits. Narrow-band HPM weapons have greater effective ranges, but prior knowledge of the target characteristics is required to design for optimum radio frequency energy transfer. Wideband HPM systems affect an array of electronic systems but have shorter effective ranges.

Cybersecurity

As the cyber threat continues to exponentially evolve, so must the cybersecurity T&E infrastructure and skilled workforce to adequately assess the cybersecurity posture of developing systems and keep pace with the volume of complex systems and aggressiveness of attacks. There is a need for a structured, coordinated approach for additional resources to develop tools that can automate routine processes to expedite testing, develop M&S tools to estimate cyber effects and complement testing, and work with the Intelligence Community and tool developers to adequately represent the cyber threats. Specifics are included in the Controlled Unclassified Information edition of this report.

Chemical and Biological Defense

The Department lacks a comprehensive approach to countering Weapons of Mass Destruction including Chemical, Biological, Radioactive, and Nuclear (CBRN) threats. Specific challenges continue to be present with the health of the T&E infrastructure required to adequately evaluate the operational performance of the chemical/biological threat detection systems or the survivability of DOD weapon systems against chemical and biological agents. To keep pace with rapid advances in technology, the Department should: 1) develop a long-term strategic solution for the modernization of T&E instrumentation necessary to reduce risk from predicted obsolescence in test instrumentation and data-collection systems; 2) ensure T&E infrastructure and workforce can enable credible and comprehensive performance assessments of DOD chemical/biological detection, protection, and decontamination capabilities in operationally representative environments in support of all-domain operations; and 3) ensure preparation and readiness for testing of aerosolized and vaporized non-traditional agent threats, resulting in reduced risks to force due to halting development and engineering of non-traditional agent safety, security, protection, and decontamination procedures and protocols.

Nuclear Modernization

U.S. Intercontinental Ballistic Missiles (ICBM) and long-range, high altitude ground- and sea-based interceptors are potentially subject to nuclear detonation (NUDET)-generated atmospheric and space environments as depicted in Figure 1. High-altitude NUDET environments could contain X-rays, gamma rays, neutrons, blast effects, and aerothermal heating, depending on the geometry of the operational scenario. X-rays, gamma-rays, and neutrons can kill a missile or space asset kinetically or by creating current pulses in wires that can disable electronics. High-altitude NUDET-generated X-rays and gamma-rays can ionize the upper atmosphere, disrupting radar and communications systems and generating high-altitude electromagnetic pulse (HEMP) effects. In addition, charged-particle bomb debris can be trapped in the Earth's magnetic field, potentially disabling satellites hours to years after the event.

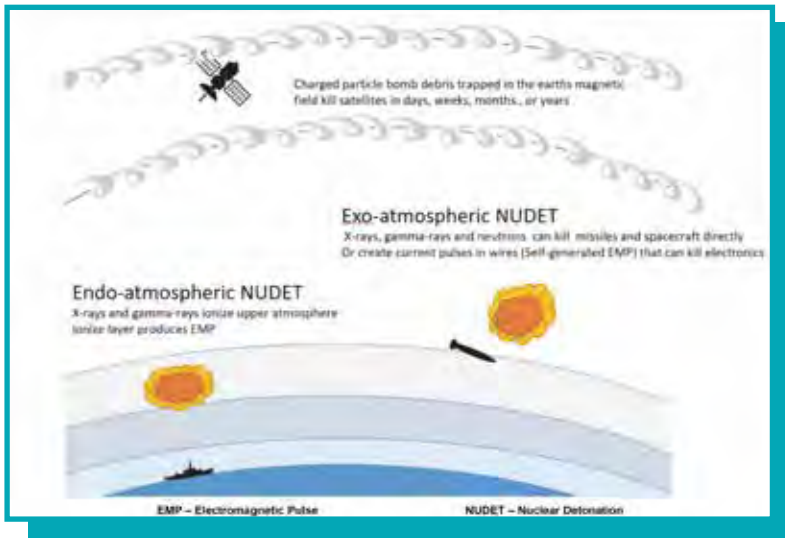


Figure 1. Nuclear Modernization

The DOD needs adequate nuclear effects, ground, and flight test T&E capabilities to collect the test data necessary for the verification and validation of M&S used to conduct nuclear weapon

effectiveness and survivability assessments in a nuclear environment. Additional details are provided in the Controlled Unclassified Information edition of this report.

Electromagnetic Spectrum Warfare

The Electromagnetic Spectrum Operational Environment is increasingly congested and contested by military and civilian systems, and constrained by national and international regulatory changes. Electromagnetic Spectrum Operations (EMSO) comprises the coordinated military actions to exploit, attack, protect, and manage the electromagnetic spectrum environment. Electromagnetic Warfare is a vital element of EMSO and includes Electromagnetic Attack, Electromagnetic Protection, and Electromagnetic Support. The DOD has recognized shortfalls in the infrastructure required to evaluate the performance of weapon systems in a contested, congested, and constrained Electromagnetic Spectrum Operational Environment. Details are included in the Controlled Unclassified Information editions of this report.

In addition, cognitive EMSO systems (incorporating AI technologies to varying degrees) beginning to be developed by the U.S. and its adversaries create unique system attributes: complex, autonomous behavior that will adapt to changing environments as the system learns. These introduce additional T&E infrastructure challenges.

Space

Critical DOD space assets are potentially subject to a range of adversarial attacks, including directed energy weapons, kinetic threats, cyberattacks, electromagnetic spectrum (EMS) fires, and nuclear weapons. To adequately evaluate the survivability of U.S. space systems against such engagements and mitigate any identified vulnerabilities, the Department requires space range infrastructure, instrumentation, and high fidelity-threat surrogates. Details are included in the Controlled Unclassified Information edition of this report.

Autonomous Systems and Artificial Intelligence

Autonomous and AI-based systems are critical enablers in delivering the warfighting capability required to achieve superiority in a multi-domain operational environment. These software-intensive and data-driven systems can learn over time and develop emergent behaviors while integrating with human operators to optimize their contribution to mission success. AI and autonomy will introduce new problems and exacerbate existing ones. T&E of systems that behave flexibly is challenging for many reasons, including covering the large operational spaces and generalizing results to untested scenarios, accounting for how evolving designs, operational use, and environments will alter system effectiveness, or difficulty in defining and measuring success in the first place. Specific challenges include:

- Non-linear, time-varying, and emergent behaviors reduce confidence in fully assessing effectiveness across a range of scenarios/environments.
- Ethical concerns related to lethal decisions may preclude warfighting capability if testing does not confirm exceptionally high confidence in its behavior. Testing for compliance with ethical constraints on behaviors is an open research issue.
- Survivability evaluation of software-intensive systems against adversarial attacks also requires additional research.

Multi-Domain Operations

The rapid proliferation of advanced technology and anti-access and area denial threats have challenged U.S. freedom of action on the battlefield and increased risks to mission effectiveness and kill-chains effects. To achieve and maintain superiority, either sustained or temporary, in an increasingly dynamic, system of systems, joint multi-domain operations environment, U.S weapons systems are being developed and/or upgraded to connect sensors and shooters effectively, efficiently, and securely across all domains using unified command and control networks.

Today's test and training environments are optimized for single-domain evaluations. T&E in multi-domain environments requires sustained investments that will be defined by scenario complexity, mission space needs, representative warfighter networks, multi-level classification, threat emulation, and a complex array of joint supporting battle management test assets. A T&E environment and corresponding tools that allow for credible assessment of combined kinetic and non-kinetic effects across all domains is critical to optimize and correctly evaluate DOD mission effectiveness in the current and future battlefield. Additional details are provided in the Controlled Unclassified Information edition of this report.

Common Range Infrastructure

To keep pace with the technological advancements expected to be found in the modern battlefield the Department should: 1) coordinate the development of credible digital environments and digital twins, 2) connect test and training ranges, 3) virtually link ground test simulation facilities and hardware-in-the-loop testing, 4) pursue common secure networks across test and training ranges in support of operational testing to leverage common live-virtual-constructive integration and real-time monitoring and control of the test, and 5) establish a common or interoperable open-air test and training range infrastructure with common data standards, models, and data collection to facilitate test and training battle shaping requirements. Additional recommendations in addressing specific shortfalls associated with testing hypersonic, directed energy weapons, space, cyber, nuclear, electromagnetic spectrum, and other emerging technologies can be found in respective subsections of this report.

Target/Threat Systems

Threat and target surrogate shortfalls required to adequately evaluate the performance of hypersonic missiles and directed energy weapons (either offensive or defensive), the survivability of our weapon systems and infrastructure against nuclear and EMS fires, and the survivability of critical space assets are discussed in the respective sections in the Controlled Unclassified Information edition of this report. This section is focused on threat and target surrogate shortfalls needed to evaluate the performance of our systems in contested air and sea domains. Details can be found in the Controlled Unclassified Information edition of this report.

Knowledge Management and Big Data Analytics

Knowledge management is a process for transforming information and intellectual assets into enduring value by connecting people with the knowledge they need to act. Creating an effective knowledge management system for meeting T&E needs requires: 1) big data analysis capability to enable efficient search and analyses of large amounts of data, 2) data architectures that make information accessible, and 3) skilled data managers to keep the data organized and accessible.

Integrated and interoperable data collection and test range instrumentation are not optimal for deployed operational testing. The DOD requires an enterprise T&E knowledge management system that securely leverages commercial big data analytic and cloud computing technologies to improve data searchability and evaluation quality, and to reduce decision timelines. It also needs an enterprise approach for T&E of knowledge management systems and implementing an effective mechanism for analyzing data at scales heretofore unimaginable.

The Department has initiated multiple pilot projects to test the capabilities of knowledge management and big data analysis systems against real test data and to inform the development of an enterprise architecture for the test community. However, additional efforts are needed to keep pace with the volume and complexity of T&E data needs.

The Department needs to continue to pursue an evaluation infrastructure, including data architecture, analytics, and skilled Operational Test Agency workforces to meet the data volume and complexity of T&E needs. The Department also needs to establish data analytics to enable data fusion and access across multiple test ranges and domains.

The Operational Test Agency Workforce

The T&E workload has increased dramatically over the last few years due to the rise of software-intensive systems, modern technologies such as autonomous/AI-enabled systems, hypersonics, and directed energy, as well as the increasingly complex and dynamic multi-domain operations environment, which includes advanced maritime, air, land, cyber, space, and electromagnetic spectrum threats. Combined with the demands of innovative, adaptive acquisition framework initiatives, these T&E complexities and changes are straining the T&E workforce. Despite these external demands and challenges, Operational Test Agency plans indicate the workforce will remain largely constant from FY20-28, with two exceptions the Air Force Operational Test and Evaluation Center, and the Defense Information Systems Agency. To address the noted workforce issues, the Operational Test Agencies should:

- Execute a detailed T&E workforce analysis to identify gaps in expertise, capacity, and recruitment needs
- Develop and sustain the execution of the training curricula in specific technical areas, with periodic refresh, to support T&E needs
- Continue to build partnerships with and create reach-back mechanisms to access subject matter experts within key universities, research organizations, and industry as a means to fill knowledge gaps for identified technical areas
- Cultivate and maintain partnerships with key federal (e.g., internal DOD partners, the Intelligence Community, non-DOD federal labs) and international/coalition partners to share lessons learned, ensure operational assessments fulfill requirements, and leverage mutual areas of interest in T&E investments

5G and Radio Frequency (RF) Spectrum for T&E

National spectrum policy supports turning over more spectrum resources to commercial users in frequency bands currently used to support testing and training. This spectrum sell-off is competing with the Department's increased need for additional spectrum as network-centric systems expand. While the Department continues to work with agency partners to develop transition plans to accommodate spectrum sales and joint use policies, there are several concerns that may limit the Department's operational test capabilities. Details are provided in the Controlled Unclassified Information edition of this report.

Wind Farms

The Department has well-established procedures to identify and mitigate any adverse effects of onshore wind turbines on test, training, and operational activities. The proliferation of offshore wind farms on both the East and West coasts, however, raise new concerns that the cumulative effects of multiple offshore wind farms may significantly affect air corridors and the performance of mission essential radars on test and training ranges, as well as surface and subsurface operating areas and transit routes. Offshore wind turbines may also introduce noise and vibration into the surrounding waters, while the cables carrying the generated power to the on-shore collection points may introduce electromagnetic interference along their paths. Noise, vibration, and electromagnetic interference could impact the accuracy of naval sensors (operational and developmental). The DOD and the Bureau of Ocean Energy Management should collect sufficient data to determine any effects of offshore wind turbine noise, vibration, and electromagnetic interference on testing, training, and operational activities to identify potential mitigation techniques.

Other Test and Evaluation Resources Concerns

In FY21, the Services have considered tradeoffs in their FY23 budget that in some cases, if implemented, would degrade their ability to execute adequate operational testing and evaluation. While the proposed budget reductions were neither officially implemented nor certified by USD(R&E) when this report was finalized, proposals like these, in the environment where adversaries continue to increase their technology and T&E capabilities, are ill-advised and should be avoided to prevent the degradation of the performance of our weapon systems in combat.

DOD Programs

Aerosol and Vapor Chemical Agent Detector (AVCAD)

At least one of the two pursued Aerosol Vapor Chemical Detector (AVCAD) systems has the potential to be operationally effective in detecting chemical vapor and aerosol threats without requiring significant design and engineering changes. At least one of the vendors needs to implement additional design and engineering changes to demonstrate the potential to meet operational suitability requirements. Both vendors have taken action to mitigate cyber-induced vulnerabilities identified during the Cooperative Vulnerability and Penetration Assessment.

System Description

The AVCAD is an aerosol and vapor chemical warfare agent and non-traditional agent detector. The Services plan to employ AVCAD as a handheld detector, a fixed site monitoring device, and on manned vehicles, ships, and aircraft to detect and alert personnel to the presence of chemical agents and support force protection decisions. The AVCAD is designed to be powered by battery or the platform on which it is integrated.

Program

The AVCAD program is a joint Acquisition Category III program in the engineering and manufacturing development phase of acquisition. DOT&E approved the Milestone B Test and Evaluation Master Plan (TEMP) in January 2019 and subsequent changes to this plan in October 2021. The Operational Assessment started in October 2021 and is expected to end in March 2022. The Milestone C acquisition decision is scheduled to occur in FY22.

Major Contractors

Smiths Detection Incorporated – Edgewood, Maryland. Chemring Sensors and Electronic Systems – Charlotte, North Carolina.

Test Adequacy

In FY21, the AVCAD Program Office, in conjunction with the Army Test and Evaluation Command, executed the following developmental test events: chemical agent detection, false alarm performance, coastal environment, reliability, and military standards compliance, as well as early user testing to identify system design and operational deficiencies. The Program Office, in conjunction with a joint Service test team, conducted integrated

developmental and operational test events to evaluate chemical warfare agent detection performance. The Program Office also executed several demonstrations to assess changes made to the systems and to the preventative maintenance and check procedures. Testing was completed in accordance with DOT&E-approved TEMP and test plans.

Performance

Effectiveness

The Smiths Detection AVCAD must address several shortfalls to mitigate its risk to meeting operational effectiveness requirements. The Smiths Detection AVCAD demonstrated the capability to meet some but not all detection requirements. The Smiths Detection AVCAD demonstrated acceptable false alarm rates.

The Chemring Sensors AVCAD will need to implement additional design and engineering changes to mitigate its risk to meeting operational effectiveness requirements. The Chemring Sensors AVCAD demonstrated the capability to meet some but not all detection requirements. The Chemring Sensors AVCAD was not able to demonstrate the acceptable false alarm rates.

Suitability

The Smiths Detection AVCAD will need to implement additional design and engineering changes to mitigate its risk to meeting operational suitability requirements. The design continues to have performance deficiencies and previous attempts to correct the problem have not proven successful. Smiths Detection is assessing other options to address the identified deficiencies.

The Chemring Sensors AVCAD may be able to meet its operational suitability requirements with the proposed design changes that need to be further verified in operational test. Chemring Sensors made changes to the initial AVCAD design to address the reliability concerns but changes negatively affected others aspect of the design. Chemring Sensors continues to assess options to address the design deficiency.

Survivability

An initial Cooperative Vulnerability and Penetration Assessment identified cyber-induced vulnerabilities affecting system survivability in a cyber-contested environment. Both vendors modified their systems to mitigate these vulnerabilities. An Adversarial Assessment was conducted in November 2021 to identify and address vulnerabilities prior to low-rate initial production.

Recommendation

1. The Program Office should continue to address the identified shortfalls to improve system performance prior to IOT&E and successfully demonstrate operational effectiveness, suitability, and survivability in support of the full-rate production and fielding decisions.

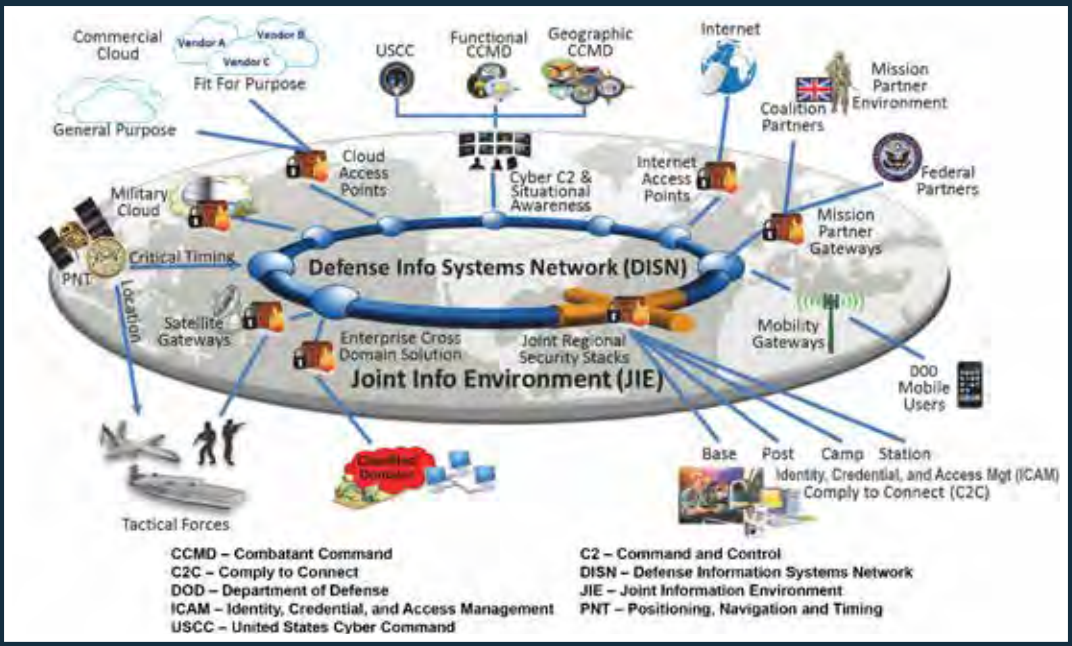
Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives

The DOD Chief Information Officer (CIO), Defense Information Systems Agency (DISA), and Services have been implementing programs, projects, and initiatives intended to achieve Digital Modernization Strategy (DMS) objectives. Many DMS initiatives use commercial cloud environments and lack an overarching systems integration process, test strategy, and program executive organization to manage cost, drive schedules, and monitor performance factors. The untested, and therefore unknown, operational performance of DMS programs, projects, and initiatives pose a significant operational risk to the DOD enterprise, particularly in a threat representative, cyber-contested environment. Future deployment decisions need to be informed by adequate OT&E.

System Description

The DOD DMS summarizes the Department's approach to information technology (IT) modernization, focused on the Joint Information Environment Framework intended to improve networking capabilities for fixed and mobile users, institute new enterprise IT services, modernize technology through coordinated refresh efforts, implement a new joint cybersecurity capability, and improve access to data. DOT&E is monitoring the DMS programs, projects, and initiatives that pose a significant operational risk to the DOD enterprise in a cyber-contested environment. These efforts align with the DMS objectives that:

- Deliver a DOD enterprise cloud environment that leverages commercial technology and innovations
- Optimize DOD office productivity and collaboration capabilities, e.g., Enterprise Collaboration and Productivity Services (ECAPS) Capability Set 1 (Defense Enterprise Office Solution (DEOS)), Microsoft Office 365 (O365), and ECAPS Capability Sets 2 and 3
- Deploy an end-to-end Identity, Credential, and Access Management (ICAM) infrastructure to support DOD systems
- Transform the DOD cybersecurity architecture, including the Joint Regional Security Stack described in this Annual Report, and initiatives to provide enterprise endpoint security for devices (e.g., desktop and mobile devices)
- Strengthen collaboration, international partnerships, and allied interoperability through a Mission Partner Environment (MPE)



Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives

Programs, Projects, and Initiatives

The DMS is not a program of record. In July 2020, the DOD CIO established the Digital Modernization Infrastructure (DMI) Executive Committee (EXCOM) chaired by the DOD CIO, U.S. Cyber Command, and Joint Staff J6 to provide guidance, direction, and oversight of the development, execution, synchronization, and utilization of DOD plans for enterprise IT programs, projects, and other funded initiatives intended to meet the DMS objectives. The DMI EXCOM does not have traditional milestone decision authorities. The DOD CIO, DISA, and Services intend to achieve DMS objectives by implementing programs, projects, and initiatives aligned under DMI EXCOM-approved and Component-funded priorities. DISA is the principal integrator for DOD information network enterprise capabilities, enabling initiatives, and testing. Current Component-funded programs, projects, and initiatives in support of the DMS include:

- **Enterprise Collaboration and Productivity Services (ECAPS)** – In FY20, the DOD established the DEOS acquisition program (ECAPS Capability Set 1) to provide NIPRNET office productivity and collaboration capabilities. In FY21, the DOD, Services, and DISA established DOD O365 commercial cloud environments as replacements for the Commercial Virtual Remote (CVR) environment rather than utilizing the DEOS contract. DISA deviated from the DEOS Phase 1 test approach and focused on fielding the DOD O365 joint tenant environment. The DEOS Program Office and Joint Interoperability Test Command (JITC) failed to update the DEOS NIPRNET Phase 1 Test and Evaluation Master Plan (TEMP) and have yet to develop a DEOS SIPRNET TEMP. DISA is coordinating a contract for ECAPS Capability Set 2 for Business Video and Voice that will be available for future DOD Component use.
- **Identity, Credential, and Access Management (ICAM)** – Based on the draft DOD Enterprise ICAM Implementation Plan, comprises 30+ enterprise capabilities managed by DOD Components intended to create a secure, trusted environment where authorized users can access IT resources. The DOD CIO is the lead for ICAM governance. The current ICAM governance is inconsistent, and the lines of authority remain unclear based on the DOD ICAM Strategy published in FY20. The DOD CIO intends to clarify the roles, responsibilities, and lines of authority for DOD enterprise ICAM capabilities, but has not yet identified a completion timeline. The DOD CIO established Global Directory as the centralized identity and authentication service for the DOD O365 environment and other cloud-based DOD systems.

DISA is developing several ICAM capabilities to support the DOD enterprise and integrating Global Directory with these capabilities. JITC is funded but has yet to conduct T&E of the DISA ICAM capabilities. A major ICAM acquisition effort is the Public Key Infrastructure, detailed in this Annual Report.

- **Endpoint Security** is an initiative to better secure endpoint devices. The DOD CIO and DISA published an Endpoint Security Strategy in 2021 that projects deployment of endpoint security capabilities by FY25 to leverage commercial innovation, support cloud adoption, and enable Zero Trust.
- **Mission Partner Environment (MPE)** – The Air Force is acquiring strategic, operational, and tactical MPE services tailored to meet mission partner information sharing needs, which will consolidate and recapitalize 28 physical Combined Enterprise Regional Information Exchange Systems across the DOD. The Air Force conducted an MPE lab-based demonstration in October and November 2021, during EXERCISE BOLD QUEST 21.
- **Enterprise Cloud Efforts** are initiatives intended to leverage commercial cloud innovation for the DOD enterprise to deliver infrastructure and services. DISA fielded military cloud (milCloud) 2.0 in FY19. Due to the unresolved Joint Enterprise Defense Infrastructure (JEDI) protest in 2020, the DOD withdrew from the JEDI contract in FY21 and is developing a Joint Warfighter Cloud Capability multi-cloud vendor contract. The DOD CIO published the DOD OCONUS Cloud Strategy in April 2021.

Test Adequacy

ECAPS – DOT&E conducted ad hoc cybersecurity assessments on DOD O365 tenant environments to inform joint DOD CIO and U.S. Cyber Command fielding decisions in 2021. Due to the accelerated fielding schedule driven by CVR disestablishment in June 2021, these were not comprehensive but still helped identify a range of significant security concerns that the DOD CIO addressed. JITC conducted functional and integration testing of the DOD O365 joint tenant environment; however, the testing was ad hoc and limited in scope.

ICAM – DOT&E conducted an ad hoc cybersecurity assessment of Global Directory in March 2021. The assessment was, however, not a comprehensive evaluation due to the accelerated fielding schedule to support cloud authentication services.

Endpoint Security – DOT&E conducted ad hoc cybersecurity assessments of pilot desktop and mobile device endpoint security solutions in 2021 to reduce risk and gain better understanding of the capabilities to inform future assessments and fielding decisions.

MPE – The Air Force has yet to coordinate with an Operational Test Agency to perform independent T&E for the MPE capabilities.

Enterprise Cloud Efforts – DISA fielded milCloud 2.0 without conducting operational testing of this capability. The milCloud 2.0 contract precludes DOD cybersecurity testing of the hosting infrastructure and some aspects of the environment. Moreover, the DOD has yet to conduct comprehensive, independent, threat-representative cybersecurity testing of any commercial cloud and its hosting infrastructure (to include DEOS and DOD O365), which will require appropriate agreements between the DOD and the commercial cloud service providers.

Performance

There has been little operationally realistic testing performed on DMS programs, projects, and initiatives, precluding an evaluation of their operational effectiveness, suitability, or cyber survivability. Many DMS efforts lack an overarching systems integration process, test strategy, and program executive organization to manage cost, drive schedules, and monitor performance factors. Many DMS initiatives also use commercial cloud environments, but threat-representative cybersecurity testing on the commercial side of cloud environments is not currently being conducted by the DOD.

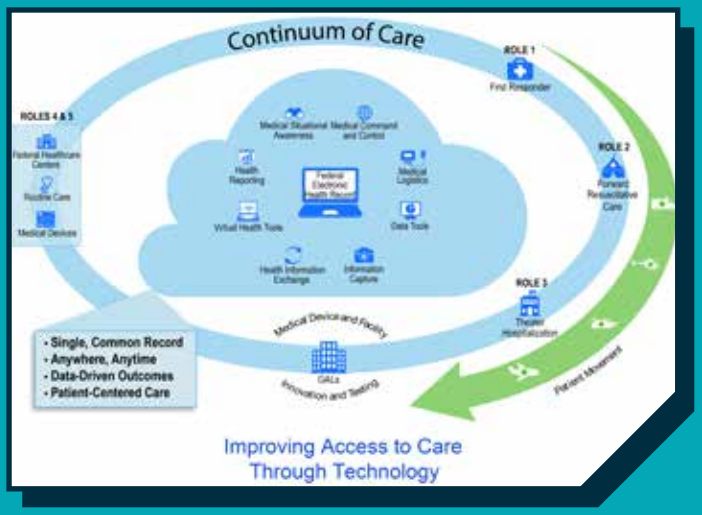
Recommendations

The DOD CIO, DMI EXCOM, Services, and Director of DISA should:

1. Conduct adequate cybersecurity testing of all DMS enterprise IT programs, projects, and initiatives in accordance with current DOD and DOT&E cybersecurity T&E guidance and policy.
2. Perform threat-representative cybersecurity testing of military and DOD commercial cloud environments, to include the commercial infrastructure operated by cloud service providers.
3. Use operational test data, analyses, and reporting to inform DMI EXCOM decisions.
4. Fund JITC to fully support DMS enterprise IT initiatives, testing, and test-related forums.
5. Develop a TEMP for ECAPS and DEOS, and more generally for each funded DMS enterprise IT initiative.
6. Continue to mature ICAM governance and establish an overarching ICAM program executive to integrate the system efforts and oversee cost, schedule, and performance.
7. Manage the key ICAM capabilities, and all other DMS initiatives, with trained program managers and supporting offices.
8. Develop an overarching ICAM test strategy that encompasses the key issues and concepts to be tested.
9. Designate an Operational Test Agency for MPE and all other DMS initiatives.

DOD Healthcare Management System Modernization (DHMSM®)

Military Health System (MHS) GENESIS is operationally effective for basic operations in conventional clinics, but not for certain specialty clinics and business areas. One of the configuration management initiatives, called "Pay It Forward," demonstrated potential for improving MHS GENESIS operational suitability. While training remains an area of major concern, with 72 percent of respondents rating it poorly, hands-on practice in a mock environment also demonstrated potential to improve MHS GENESIS operational suitability. Despite ongoing cybersecurity improvements, MHS GENESIS is not yet survivable in a cyber-contested environment.



System Description

MHS GENESIS is a modernized electronic health records system intended to create a single health care record for each patient that can be utilized by the DOD, Department of Veterans Affairs, or U.S. Coast Guard. DOD medical staff use MHS GENESIS to manage delivery of en route care, dentistry, emergency department, immunization, laboratory, radiology, operating room, pharmacy, vision, audiology, and inpatient/outpatient services, and to perform administrative support, front desk operations, logistics, billing, and business intelligence. MHS GENESIS comprises three major elements: 1) the Millennium suite of applications, which provides medical capabilities, 2) the Dentrix Enterprise, which provides dental capabilities, and 3) the Orion Rhapsody Integration Engine, which enables the majority of the external information exchanges.

Program

MHS GENESIS is an Acquisition Category I program intended to replace the legacy healthcare systems, including the Armed Forces Health Longitudinal Technology Application, Composite Health Care System, and Essentris systems. The Project Management Office (PMO) is deploying MHS GENESIS in military treatment facility "waves" in designated medical operational centers and intends to field MHS GENESIS to 205,000 MHS personnel, providing care for 9.4 million DOD beneficiaries worldwide. MHS facilities encompass 54 hospitals, 377 medical clinics, and 270 dental clinics. At the end of July 2021, MHS was fielded to about 30 percent of its intended recipients, with another deployment wave that started at the end of September 2021.

In 2020, the Joint Interoperability Test Command (JITC) conducted FOT&E on MHS GENESIS, resulting in a declaration that MHS GENESIS is partially operationally effective, but not suitable. Consequently, the FY21 Defense Appropriations Act directed a follow-on suitability assessment of MHS GENESIS change management and training and a subsequent report by March 2021.

Major Contractors

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

Test Adequacy

From February 12 through March 5, JITC conducted the congressionally mandated evaluation of MHS GENESIS change management and training, in accordance with a DOT&E-approved test plan. JITC conducted small group interviews with Defense Health Agency (DHA) and PMO personnel and with health care providers (e.g., new end users) at Nellis Air Force Base, Nevada, and Camp Pendleton, California. JITC also administered an electronic survey to users in selected clinical and business areas. The testing was adequate to evaluate current change management strategies and determine whether training had improved to a level that enabled new users to operate the system without substantial outside assistance. Testing also enabled the closure of eight previously identified incident reports, but many of them remain open. DOT&E submitted an independent assessment of the MHS GENESIS change management and training to the House and Senate Defense Appropriations Subcommittees in March 2021.

Performance

Effectiveness

Based on the FOT&E completed in 2020, MHS GENESIS is operationally effective for basic operations in conventional clinics, but not for certain specialty clinics and business areas.

Suitability

Based on the FOT&E completed in 2020, MHS GENESIS was not operationally suitable largely because training and configuration management were unsatisfactory, dissemination of system change information was inadequate, and usability problems persisted. The follow-on 2021 suitability assessment demonstrated that a new change management initiative called "Pay It Forward," designed to provide experienced military treatment facility personnel on-site to support new users during each fielding wave, proved successful, although interviews and survey results showed that this initiative was not available to many users during fielding. The 2021 follow-on assessment also demonstrated that training remains an area of major concern, with 72 percent of respondents rating it poorly. Current computer-based training remains ineffective, while a new training initiative that allows users to get hands-on practice in a mock environment demonstrated improvements.

Survivability

Despite ongoing cybersecurity improvements, MHS GENESIS is not yet survivable in a cyber-contested environment.

Recommendations

1. DOT&E's 2020 recommendations to the Under Secretary of Defense (Personnel and Readiness), the PMO, and DHA still apply.
2. JITC should continue its verification of the incident report fixes and plan for an FOT&E to verify corrective actions and resolve any outstanding incident reports.
3. DHA and the PMO should expand the "Pay It Forward" change management process.
4. DHA and the PMO should expand the new training initiative that allows users to get hands-on practice in a mock environment. The ineffective computer-based training should either be shortened, focused on more relevant skills, or discontinued.
5. DHA and the PMO should engage with vendors and JITC to conduct cybersecurity testing on vendor data storage solutions to assess the risk to mission and identify vulnerabilities that may expose sensitive protected health information and personally identifiable information.

F-35 Joint Strike Fighter (JSF)

The F-35 program made some progress in FY21 in IOT&E, but the necessary verification and validation of the Joint Simulation Environment (JSE) continued to delay readiness to conduct the 64 JSE test trials required for completing IOT&E. An official estimated date for the execution of IOT&E trials in the JSE is still to be determined.

The Program Office continues to field immature, deficient, and insufficiently tested Block 4 mission systems software to fielded units. The operational test teams identified deficiencies that required software modifications and additional time and resources, which caused delays in Block 4 capability release. The Program Office has implemented process improvements to address software development issues.

System Description

The F-35 JSF is a tri-Service, multinational, single-seat, single-engine strike fighter aircraft produced in three variants:

- F-35A Conventional Take-Off and Landing
- F-35B Short Take-Off/Vertical Landing
- F-35C Aircraft Carrier Variant

The F-35 Block 4 Modernization Capability Development Document specifies required capabilities and associated capability gaps that drive incremental improvements in capability from 2018 and beyond. Table 1 shows the linkage between development phases, hardware, block designation, mission systems software, and operational testing.

Program

The F-35 Joint Strike Fighter is an Acquisition Category ID program. DOT&E approved the F-35 Overarching Block 4 Test and Evaluation Master Plan (TEMP) and Increment 1 Annexes on May 18, 2020. The Annexes (one classified and one unclassified) cover the Block 4 developmental and operational testing of software versions 30R03 though 30R06. Increment 2 Annexes, which cover Block 4 software version 30R07 and later, are in final coordination and staffing as of the time of this report. DOT&E approved the fourth revision of the System Development and Demonstration TEMP, which governs the conduct of IOT&E, in March 2013.

Table 1. Linkage of Development Phase with Hardware, Block Designation, Mission Systems Software, and Operational Testing				
F-35 Development Phase	**Major Avionics Hardware**	**Capabilities**	**Mission Systems Software**	**Operational Testing**
SDD	TR-1	Block 2B	Block 2B Software	• Marine Corps Fielding Reports and F-35B IOC • Service and JOTT test events • Formal OUE canceled
	TR-2	Block 3i	Block 3i Software	• Air Force Fielding Reports and F-35A IOC • Service and JOTT test events
		Block 3F	Block 3F/ 3FR6**	• **Pre-IOT&E Increment 1 (Jan - Feb 2018) Cold Weather Deployment** For-score testing to evaluate the suitability of the F-35 air system and alert launch timelines in an extreme cold weather environment.
			Block 3F/30R00***	• Navy Service Fielding Reports • **Pre-IOT&E Increment 2 (Starting Mar 2018)** For-score testing of limited two-ship mission scenarios, F-35A deployment, F-35C deployment to a carrier, and weapons delivery events.
C2D2		Block 4, 30 Series	30R02.04	• **Portion of Formal IOT&E** (Dec 2018 - Sep 2019)
			30R04.52	• **Portion of Formal IOT&E: Electronic Attack (EA) trials** (Jul 2020)
			30R06.041 & .042	U.S. Operational Test Team evaluated these versions in FY21
			30R06.042	Software fix needed for **IOT&E weapons event in June 2021**
C2D2	TR-2	Block 4, 30 Series	30R07, 30R08+	Dedicated operational tests planned for each release of capability
	TR-3	Block 4, 40 Series	40R0X	Dedicated operational tests planned for each release of capability

Table 1. Linkage of Development Phase with Hardware, Block Designation, Mission Systems Software, and Operational Testing

Notes:

* For-score IOT&E events are highlighted in bold.

** The final planned version of Block 3F software was 3FR6.

*** The program changed software nomenclature for the initial increments of Block 4 from "3F" used during SDD to "30RXX" for development and "30PXX" for fielding software. The 30 series of software is compatible with the Block 3F aircraft hardware configuration and is being used to address deficiencies and add Service-prioritized capabilities.

Acronyms: C2D2 – Continuous Capability Development and Delivery; IOC – Initial Operational Capability; JOTT – JSF Operational Test Team; OUE – Operational Utility Evaluation; SDD – System Development and Demonstration; TR-X – Technical Refresh [version #], referring to the suite of core avionics processors.

Major Contractors

Lockheed Martin, Aeronautics Company – Fort Worth, Texas. Pratt & Whitney, a subsidiary of Raytheon Technologies – East Hartford, Connecticut.

Test Adequacy and Performance

IOT&E Progress

The F-35 program is nearing completion of a multi-year IOT&E. The JSF Operational Test Team (JOTT) has completed cold-weather testing; a series of weapons trials (both bombs and missiles); cybersecurity testing of the air vehicle, training systems, mission data reprogramming laboratory, and the Autonomic Logistics Information System (ALIS); deployments to ships and austere environments; and testing that compared F-35 performance to that of fourth-generation fighters against traditional and more modern surface-to-air threats currently fielded by potential adversaries. Open-air test missions evaluated the F-35 in multiple roles: offensive counter-air (OCA), defensive counter-air (DCA), cruise missile defense (CMD), suppression/destruction of enemy air defenses (S/DEAD), reconnaissance, electronic attack (EA), close air support, forward air control (airborne), strike coordination and armed reconnaissance, combat search and rescue, anti-surface warfare, and air interdiction. Test trials were conducted in varying threat environments using two-, four-, and eight-F-35 aircraft mission scenarios. During the S/DEAD and EA trials, the F-35 faced operationally representative surface-to-air threat environments represented by Radar Emulators (RE). Open air test trials were completed in June 2021, with the execution of the final AIM-120 missile trial accomplished using an F-35C aircraft. Deficiencies in earlier versions of the aircraft software prevented this event from being accomplished sooner. The program delivered software version 30R06.42 with the fixes in June 2021, enabling the operational test team to complete the trial. Suitability and cyber data collection required for the IOT&E test plan were completed by the end of CY20.

JSE Development Progress

The only remaining module of the IOT&E test plan is the 64 trials in the JSE at Naval Air Station Patuxent River, Maryland. These trials include 11 DCA, 22 CMD, and 31 combined OCA/AI/DEAD trials in operationally representative, dense, defense in-depth scenarios with the latest threat systems that are not available on open air ranges. All three F-35 variants will be involved in the execution of the trials.

Although the JSE team made steady progress in maturing the simulation and improving overall system stability, significant work remains to complete the necessary verification and validation process, which compares JSE component and system-level performance to F-35 flight test data to accredit the JSE for operational test trials. The JSE team completed a schedule review and risk analysis to

update the integrated master schedule, but an official estimated date for execution of for-score IOT&E trials in the JSE is still to be determined.

The JSE schedule has suffered multiple delays since 2015, when the Joint Program Office (JPO) transferred development and overall management of the simulation from Lockheed Martin, in an environment referred to as the Verification Simulation (VSim), to the combined JPO and Naval Air Systems Command (NAVAIR) government team at Naval Air Station Patuxent River, Maryland. Constructing and integrating the complex hardware and many software models, including Lockheed Martin's "F-35 In-A-Box" digital model of the aircraft, into the JSE has proven to be a difficult undertaking. The JPO and NAVAIR team underestimated the required level of effort to integrate and accredit a simulation of this complexity. When it was initially transferred to the government team in 2015, the JPO projected the JSE to be completed in 2017, but the schedule slipped nearly year-for-year over the following six years, despite significant progress in development. As of December 2021, significant work is required to complete the development, validate the models, and accredit the simulation before scored trials can begin.

An independent technical assessment, conducted by Johns Hopkins Applied Physics Laboratory, the Carnegie Mellon University Software Engineering Institute, and the Georgia Tech Research Institute, was completed in May 2021. The team concluded that the JSE effort needed additional financial and personnel resources, along with strong support from all stakeholders to support IOT&E requirements. DOT&E requires the JSE to complete the planned verification, validation, and accreditation process to ensure the JSE will accurately represent aircraft performance and the threat environment, so the JSE results inform an adequate effectiveness evaluation.

Block 4 Development

The JPO designed the current development process, referred to as Continuous Capability Development and Delivery (C2D2), to provide new capabilities and updates in six-month increments, but it has not worked as envisioned. The program continues to field immature, deficient, and insufficiently tested mission systems software to fielded units without adequate operational testing. Although the program designed C2D2 around commercial "agile software" development concepts, it does not adhere to the published best practices that include clear articulation of the capabilities required in the Minimum Viable Product, focused testing, comprehensive characterization of the product, and full delivery of the specified operational capabilities. The program did not deliver programmed capabilities to operational units, as defined in the Air Systems Playbook.

The program has not sufficiently funded the developmental test (DT) teams to adequately test, analyze data, or perform comprehensive regression testing to assure that unintentional deficiencies are not embedded in the software prior to delivery. In addition, integration labs must undergo a continuous verification, validation, and accreditation (VV&A) process using flight test data to provide adequate lab infrastructure. Finally, additional instrumented DT aircraft must be provided to test the wave of new capabilities, configurations, and fixes to program deficiencies from System Development and Demonstration (SDD).

The current C2D2 process has resulted in frequent shifting of priorities, discoveries of critical warfighting deficiencies after fielding to the combat units, and marginalization of meaningful operational testing and data analyses. Developmental testing of software is often truncated early, so baseline system characterization is inadequate and structured operational testing is executed simultaneously with software deliveries to the field units. The program planned to reduce flight testing with the C2D2 process by leveraging more testing in Lockheed Martin's laboratory and simulation environments, but to date that plan has not been successful due to the limitations of those test environments. The Lockheed Martin laboratories and simulations are not capable of replicating operationally representative flight conditions or target complexities and densities.

Because the current six-month C2D2 timeline has proven unsustainable, and in order to stabilize major hardware configuration changes prior to the transition to the Technical Refresh-3 configuration, the JPO is extending the development timeline to one-year increments with software version 30R08 that will begin developmental testing in December 2021.

Although designed to introduce new capabilities or fix deficiencies, the C2D2 process has often introduced stability problems and/or adversely affected other functionality. This results in the operational test units and the field units discovering deficiencies in the software. Significant operational deficiencies (classified) were identified by the operational test units and field units in CY20 that required software modifications.

The program adjusted the overall timeline and sequencing of capability development, based on an approved list of requirements, in a new Air System Playbook, version 16.1, that was presented to the JSF Executive Steering Board in September 2021.

The JSF program continues to carry a large number of deficiencies, and conducts recurring reviews with Service requirements representatives to prioritize resources to address them. Although initial development in Block 4 focused on addressing deficiencies that were identified during SDD while developing some new capabilities, the overall number of open deficiencies has not significantly decreased since the completion of SDD due to the continued discovery of new problems.

The program had to stop work on some development efforts in late CY20 and CY21 to redirect funding to the development of the new Technical Refresh (TR)-3 avionics configuration due to significant cost overruns and reductions. Further delays in the TR-3 development and integration may affect production delivery of aircraft delivered in the TR-3 configuration. Delays in Block 4 capabilities and weapons integrations activities may also limit the initial capabilities of aircraft delivered in the TR-3 configuration.

The integrated test teams at Edwards Air Force Base, California and Naval Air Station Patuxent River, Maryland, responsible for developmental flight testing of all F-35 variants, conducted testing with software versions 30R06 (eight iterations: 30R06.01, 30R06.02, 30R06.03, 30R06.031, 30R06.04, 30R06.041, 30R06.042, 30R06.043) and 30R07 (four iterations as of the end of September: 30R07.00, 30R07.01, 30R07.02, 30R07.03).

Block 4 Operational Testing

The U.S. Operational Test Team (UOTT) completed operational testing of 30R06 software in August 2020. Test missions included:

- Four Close Air Support test missions flown with F-35A and F-35B aircraft
- Four DCA test missions flown with F-35A and F-35C aircraft
- Three OCA test missions flown with F-35A and F-35C aircraft
- Two D/SEAD test missions flown with F-35A and F-35C aircraft

The UOTT completed some of these test missions by collecting limited data during large force training exercises over the test and training ranges in Alaska and off the Pacific coast. Although required by the DOT&E-approved test plan, Open Air Battle Shaping (OABS) instrumentation was not available for these training scenarios, which limited the utility of the data collected. Adequate evaluation of Block 4 capabilities against air- and surface-to-air threats continues to require the use of OABS instrumentation and threats surrogated by Radar Emulators.

Per the Block 4 TEMP and associated Annexes, operational test (OT) aircraft are required to support both developmental and operational testing. Modifications to these aircraft must be funded, scheduled, and completed just after developmental test (DT) aircraft modifications to enable integrated DT/OT, DT assist, and relevant mission-level testing of future capabilities. Without these modifications, Block 4 OT is likely to be inadequate.

U.S. Fleet Performance

In FY21, the trend in aircraft availability rates plateaued during the year and began declining in the final months of the year. Improvement in aircraft availability prior to June 2021 was a result of a program initiative to increase spare part availability and the lower percentage of aircraft needing depot modifications as more late-lot production aircraft entered the fleet. The sharp reduction in availability since June 2021 has been predominantly driven by spare parts not

being available when needed. The lack of spares inventory, and limited component-level depot repair capacity, contribute to the shortfalls in spares supply. A significant shortage of fully functional F135 engines has contributed to reduced aircraft availability. This shortage has been exacerbated by a lack of depot repair capacity. Almost all aircraft requiring an engine are F-35A variants. Although the program and the Services manage engine spares by prioritizing combat-coded units over test and training units, the shortage of spare engines has adversely affected deployed combat units as well.

The F-35 fleet remains below Joint Strike Fighter Operational Requirements Document (ORD) thresholds in some areas for overall reliability and maintainability. Maintenance data gathered through June 2021 from the U.S. fleet of all three variants show that the F-35A and F-35B are not meeting, and the F-35C is not projected to meet, the full set of ORD reliability and maintainability requirements for mature aircraft. The F-35A has accumulated the flight hours designated for maturity (75,000 hours), making it eligible for an assessment against the full ORD requirement. In June 2021, the F-35A fleet alone exceeded 200,000 flight hours, the total hours designated for the entire fleet for maturity. The F-35B fleet also reached its 75,000-hour threshold in June, making it eligible for an assessment against the full ORD requirement as well. The F-35C has not yet reached its individual variant threshold of 50,000 hours and was consequently assessed against interim goals. The tables below show reliability and maintainability trends from June 2020 to June 2021 and whether ORD requirements or imputed interim goals are being met. For the reliability metrics, higher numbers reflect better performance (a more reliable system) and for maintainability metrics, lower numbers reflect better performance (less maintenance burden). Tables 2 and 3 show trends in the reliability and maintainability metrics respectively based on data aggregated in 3-month rolling windows, where monthly reports are generated based on the last 3 months of data. This process enables trends to be observed more clearly than reports generated by only a single month of data.

Operational Suitability Testing

The UOTT conducted suitability testing per the annual DOT&E-approved suitability test plan in FY21. The test team conducted interviews with maintenance personnel and pilots on training, technical orders, the use of ALIS, software updates, maintenance of the low observable characteristics of the aircraft, support equipment and tools, and safety issues.

Table 2. F-35 Reliability Metrics (Up Arrow Represents Improving Trend)

Variant	Flight Hours for ORD or JCS Threshold	Assessment as of June 30, 2021												
		Cumulative Flight Hours	MFHBCF (hours)			MFHBR (hours)			MFHBME (hours)			MFHBF_DC (hours)		
			ORD Threshold	Change: June 2020 to June 2021	Meeting Interim Goal for ORD Threshold	ORD Threshold	Change: June 2020 to June 2021	Meeting Interim Goal for ORD Threshold	ORD Threshold	Change: June 2020 to June 2021	Meeting Interim Goal for ORD Threshold	JCS Requirement	Change: June 2020 to June 2021	Meeting Interim Goal for JCS Threshold
F-35A	75,000	202,172	20	↓	No	6.5	↓	No	2.0	↓	Yes	6.0	↓	Yes
F-35B	75,000	75,141	12	↓	No	6.0	↑	No	1.5	↑	Yes	4.0	↓	Yes
F-35C	50,000	42,449	14	↑	Yes	6.0	↓	No	1.5	↓	No	4.0	↑	Yes

Table 3. F-35 Maintainability Metrics (Down Arrow Represents Improving Trend)								
Variant	Flight Hours for ORD Threshold	Assessment as of June 30, 2020						
		Cumulative Flight Hours	MCMTCF (hours)			MTTR (hours)		
			ORD Threshold	Change: June 2020 to June 2021	Meeting Interim Goal for ORD Threshold	ORD Threshold	Change: June 2020 to June 2021	Meeting Interim Goal for ORD Threshold
F-35A	75,000	202,172	4.0	↓	No	2.5	–	No
F-35B	75,000	75,141	4.5	↑	No	3.0	↑	No
F-35C	50,000	42,449	4.0	↓	No	2.5	↓	No

The UOTT continued developing plans to conduct a 30-day demonstration of flight operations without ALIS connectivity. As required by DOT&E, the demonstration and corresponding results must be scheduled for completion prior to the approval of the next increment of TEMP annexes.

ALIS and Operational Data Integrated Network (ODIN)

The program continued making plans to transition from ALIS to ODIN, but progress stagnated due to program funding constraints and the need to address pressing ALIS obsolescence and cyber challenges. The JPO altered the ALIS-to-ODIN (A2O) strategy in early 2021 to a phased approach, replacing the previous strategy of a rapid transition to and fielding of ODIN. The result was a significant delay to the planned ODIN development timeline and a merger of the ALIS and ODIN organizations into one. The key to A2O success lies in the definition of the new data architecture, fixing cybersecurity deficiencies in ALIS, and ensuring that any new ODIN hardware and software solutions build in cybersecurity from the start of development.

In June 2021, the JPO elected to down-select one ODIN hardware solution to address urgent obsolescence needs, choosing the Lockheed Martin-produced ODIN Base Kit (OBK). Thirty-four OBKs were procured in FY21 and are currently being fielded. Fourteen are replacing the oldest ALIS Standard Operating Unit (SOU) v1, sixteen support future site stand-ups, and four are spares for the fleet. Initial performance measurements indicate the OBK runs ALIS significantly faster than existing the SOU v1 and v2 hardware. Additionally, the OBK is significantly smaller and lighter than the legacy SOU hardware. The OBK alone weighs 65 pounds. It requires an uninterruptible power supply, which weighs an additional 69 pounds. An optional battery expansion can be included, which weighs 68 pounds. The total OBK hardware weighs between 134 and 202 pounds, much less than the 891-pound SOU. The size of the OBK is significantly less than the SOU as well, roughly a 75 percent reduction in volume. The path forward is to make all new ALIS or ODIN software compatible with minimal retrofit to the OBK hardware. ALIS will be required to be compatible with both the existing SOU and OBK hardware until all of the SOUs are replaced, which is currently expected in late 2023.

Quarterly ALIS software development in FY21 focused primarily on cybersecurity improvements, software stabilization, improved processing times, and some usability improvements. The cybersecurity authorizing officials are closely monitoring progress on cyber risk reduction. Although no formal

operational test occurred apart from cybersecurity testing of the Mission Planning Support Environment described below, testing of ALIS software updates took place at the Integrated Test Force facility at Pauxent River, Maryland and the Operationally Representative Environment at Edwards Air Force Base, California. The Quarter 1 (Q1) approval for fleet release was granted in June 2021 and fielding is ongoing. The Q2 release was delayed due to issues found in flight test. It was subsequently loaded into the U.S. Central Point of Entry and Nellis Air Force Base OBK to begin an operational assessment prior to release to the fleet. The Q3 development is complete and ORE/Flight Test will be done in November. The Q4 release is in development. Both developmental and operational testing for ALIS and ODIN continue to be under-resourced, increasing risk to fielding and support. While the quarterly software development cycle that started in 2019 will continue into 2022, the program plans to transition the software release cycle to two releases per year.

The rate of spare parts with Electronic Equipment Logbooks arriving at warehouses ready for issue has historically been lower than the JPO goal of 90 percent. Recent JPO data show that this rate increased to between 80 and 90 percent.

Cybersecurity vulnerabilities and attack vectors found during testing of ALIS will need to be addressed by the program as data structures transition from ALIS to ODIN. Rigorous testing of data integrity will also be necessary to ensure a secure transition, testing that needs to be planned and documented for DOT&E approval. These steps will be critical to the success of A2O while also supporting operational unit day-to-day activities.

Cyber

While some cybersecurity-related system discrepancies have been resolved, cybersecurity testing during FY21 continued to demonstrate that some vulnerabilities identified during earlier testing periods remain in the system.

The UOTT cyber test teams conducted a Cooperative Vulnerability and Penetration Assessment on the Mission Planning Support Environment (MPSE) at Marine Corps Air Station Yuma, Arizona in July 2021 and an Adversarial Assessment on the MPSE at Eglin Air Force Base, Florida in September 2021. Both were conducted in accordance with DOT&E-approved test plans.

The UOTT worked with the JPO and stakeholders across the DOD to identify relevant scenarios, qualified test personnel, and adequate resources for conducting cybersecurity testing on AV components and support systems.

More testing is needed to assess the cybersecurity of the AV. Actual aircraft, as well as appropriate hardware- and software-in-the-loop facilities, must be used to facilitate operationally representative air vehicle cyber testing. To this end, the F-35 JPO arranged for an operationally representative F-35B AV at Naval Air Station Patuxent River, Maryland to facilitate testing.

The F-35 JPO intends to use a Security Development Operations and agile software construct with frequent software updates to the field in support of the ODIN path forward. The Block 4 construct of 30 and 40 series operational flight program software is also providing more frequent updates to the combat forces than SDD. An increased frequency of new software deployments may further stress the capacity of cybersecurity test teams to thoroughly evaluate each update. Under these new constructs, the importance of cybersecurity testing of the software development environments will increase.

In light of current cybersecurity threats and vulnerabilities, along with peer and near-peer threats to bases and communications, DOT&E required the F-35 program and Services to conduct testing of aircraft operations without access to the ALIS SOU for extended periods of time, with an objective of demonstrating the SOU-specified 30 days of operations. The program is currently planning for a test of the ALIS Contingency Operations Plan in late 2021 or early 2022, which will test standardized procedures for lack of connectivity scenarios.

Recommendations

The F-35 JPO, Services, and Lockheed Martin as appropriate should:

1. Complete the remaining development and VV&A of the JSE as soon as possible to enable timely completion of the required IOT&E trials.
2. Fully fund new threat air defense radar simulators and upgrades to existing REs, the JSE, and OABS systems to meet test requirements for each C2D2 release of capability.
3. Adequately fund the development and sustainment of robust laboratory and simulation environments, data management and analysis architecture, and adequate VV&A plans that include the use of data from representative open-air missions in support of developmental and operational testing.
4. Complete development of the requirements for the Block 4 USRL while ensuring adequate lab infrastructure to meet the aggressive development timelines of C2D2 and the operational requirements of both 30 and 40 series Block 4 F-35 aircraft.
5. Per the DOT&E TEMP, Increment 1 approval memo:
    - Fully fund, develop and update the detailed plan to modify all OT aircraft with the capabilities, life limit, and instrumentation, including OABS requirements.
    - Complete a 30-day demonstration of flight operations without ALIS connectivity.
    - Align the components of the F-35 air system delivery framework for each increment of capability to allow enough time for adequate testing of the fully representative system that is planned to be fielded.
6. Continue to pursue maintenance system improvements, especially for common processes distributed among many different Non-Mission Capable Maintenance drivers, such as low observable repairs and adhesive cure times.
7. Improve spare posturing, especially for F135 engines, to reduce down-time for aircraft waiting spare parts by developing alternate sources of repair (including organic repair).
8. Continue to expedite fixes to Electronic Equipment Lists.
9. Accomplish rigorous testing of data integrity while the transition from ALIS to ODIN continues, as this will be critical to the success of A2O while also supporting operational unit day to day activities.
10. Ensure both developmental and operational testing for ALIS and ODIN are adequately resourced to reduce the high risk associated with fielding an immature and inadequately tested replacement.
11. Conduct more in-depth cyber testing of the AV and provide a dedicated AV cyber-test asset.
12. Correct program-wide deficiencies identified during cybersecurity testing in a timely manner.
13. Develop and routinely report software sustainment and stability metrics that show how well the program's overall software development capability for the air vehicle and logistics sustainment system is progressing.

Joint Biological Tactical Detection System

The Joint Biological Tactical Detection System (JBTDS) must overcome major challenges to meet the operational effectiveness requirement to detect and identify biological warfare agents in the air. JBTDS requires improvements to detector and identifier reliability, battery power indicator accuracy, and the transit load configuration to meet operational suitability requirements. The IOT&E planned to support the final operational effectiveness and suitability assessment is scheduled for 4QFY23.

System Description

The Services intend for JBTDS to detect biological warfare agents in the air, by utilizing either a trigger when a biological warfare agent is detected, or through on-demand collection initiated by the operator. The system consists of an integrated man-portable biological warfare agent detector and sample collector, base station, meteorological station, GPS, sample extraction kit, and a handheld biological warfare agent identifier with consumable cartridges. The detector and sample collector can be connected to the base station using a Service-provided, closed, or restricted local area wired or wireless network to enable remote monitoring and reporting.

Program

The JBTDS is a joint Service Acquisition Category II program. DOT&E approved a revision to the Milestone B Test and Evaluation Master Plan in November 2020. The Milestone C low-rate initial production decision is scheduled for 4QFY22. The IOT&E is planned for 4QFY23.

Major Contractors

Chemring Sensors and Electronic Systems – Charlotte, North Carolina. Biomeme – Philadelphia, Pennsylvania.

Test Adequacy

In FY21, the Army conducted JBTDS test events to assess the readiness for low-rate initial production. These included detection limits tests for 6 of 10 agents, identification limit tests for 7 of 10 agents, environmental and military standards compliance tests, false alarm rejection and reliability tests, the first of two operational assessments to support Service biological surveillance and site exploitation missions, and an Adversarial

Assessment. These tests, conducted in accordance with the DOT&E-approved test plans, were adequate to characterize the intended aspects of system performance and identify areas for additional development.

Performance

Effectiveness

The JBTDS program will need to address identified performance shortfalls to mitigate its risk to meeting operational effectiveness requirements. During the operational assessment, military personnel were able to employ JBTDS to detect simulated biological threats and trigger the automatic collection of a sample for analysis. Operators were able to manually trigger the collection of an air sample and employ the sample collection/extraction kit to transfer the sample to the identifier for analysis in the field. Poor performance of identifier cartridge lots significantly affected the capability to support force protection decisions. In certain environments, the detector false alarm rate did not meet the requirement, which could lead to lost confidence in the system.

Suitability

The JBTDS program will need to successfully address identified shortfalls to mitigate the risk to meeting operational suitability requirements. During the operational assessment, the JBTDS detector collector demonstrated improved reliability while the identifier demonstrated poor reliability. The Army test unit expressed concern over their current JBTDS load configuration due to the time required to pack and load the systems for transport and due to its transport and storage footprint. The identifier requires improvements to accurately detect and indicate remaining battery life during operation, which, if not addressed, will continue to drive the need for more frequent battery changes and additional spare batteries. One of the test units noted that the packaging associated with system consumables generates burdensome waste that needs be collected, stored, and properly disposed.

Survivability

Data analysis is ongoing precluding a survivability assessment of JBTDS in a cyber-contested environment at this time.

Recommendations

The contractors should:

1. Improve the performance of the identifier cartridges to accurately identify biological warfare agents and enable appropriate force protection decisions.
2. Reduce the system false alarm rate to meet operational requirements.

JBTDS base station and handheld biological warfare agent identifier with consumable cartridges

3. Improve system reliability to meet operational requirements.
4. Fix the battery life indicator for system components to accurately estimate the remaining battery life.
5. Modify system consumable packaging to minimize waste.

Joint Regional Security Stack (JRSS)

Previous assessments demonstrated that the Joint Regional Security Stack (JRSS) was not effective in helping cyber defenders detect and respond to operationally realistic cyber threats. Pursuant to the FY21 National Defense Authorization Act (NDAA), in July 2021, the DOD Chief Information Officer (CIO) decided not to deploy JRSS on SIPRNET and sunset NIPRNET JRSS within the next five years while pursuing a Zero Trust cybersecurity architecture.

System Description

JRSS is a suite of cybersecurity capabilities intended to protect the Department of Defense Information Network (DODIN). The DOD intends to use JRSS to enable DOD cyber defenders to continuously monitor and analyze DODIN traffic to minimize the effects of cyberattacks while ensuring the integrity, availability, confidentiality, and non-repudiation of data. The suite of capabilities integrated as part of JRSS are to support both defensive cyber operations and network operations for bases, posts, camps, and stations.

Program

JRSS is not a program of record and does not have a Test and Evaluation Master Plan. The Defense Information Systems Agency (DISA) manages the technical implementation of JRSS, while the DOD CIO chairs the JRSS Senior Advisory Group (SAG) that governs programmatic aspects of the system. The Services jointly fund JRSS and manage their own use of its capabilities. JRSS is currently operational on NIPRNET. A SIPRNET version was planned, with several being installed in 2016, but not used operationally. Pursuant to the 2021 NDAA, the DOD CIO elected to sunset JRSS within five years rather than transition it to a program of record.

Major Contractors

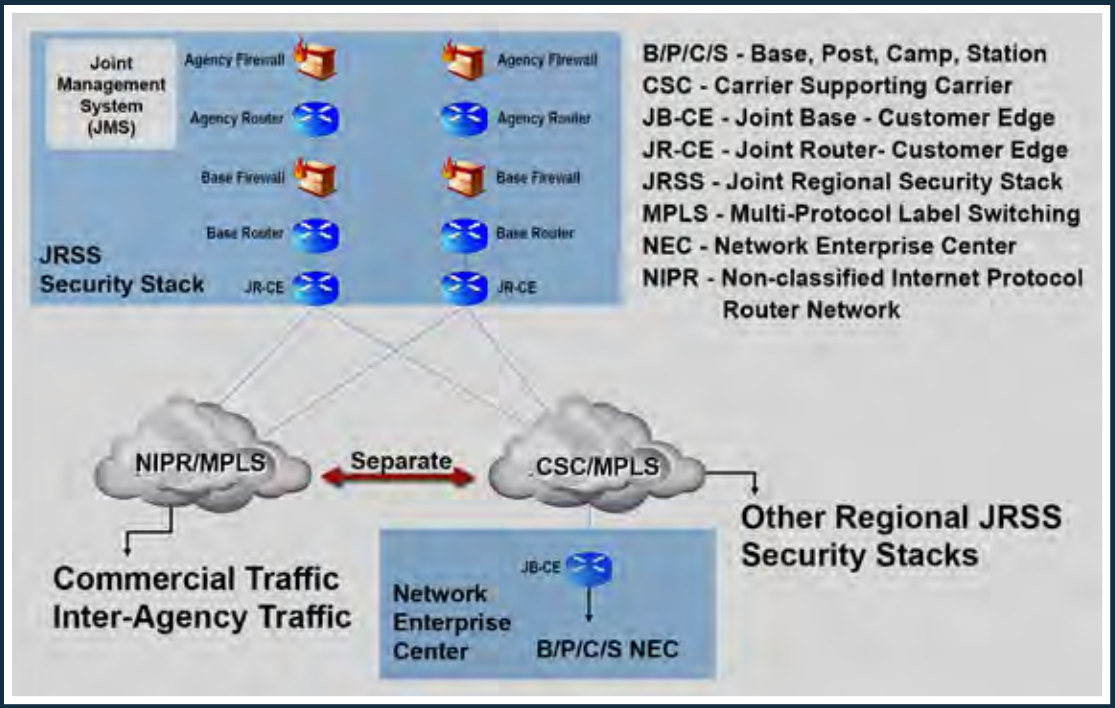
DISA is the lead integrator for JRSS. The paragraph below lists the current Original Equipment Manufacturers (OEMs) of the JRSS capabilities.

- A10 – San Jose, California.
- Ansible – Durham, North Carolina.
- Axway – Phoenix, Arizona.
- BMC – Houston, Texas.
- Cisco – San Jose, California.

- Citrix – Fort Lauderdale, Florida.
- Corelight (Zeek) – San Francisco, California.
- Confluent (Kafka) – Mountain View, California.
- CSG International – Alexandria, Virginia.
- Dell – Round Rock, Texas.
- Elastic – Mountain View, California.
- 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.
- InQuest – Arlington, Virginia.
- ITIPIE – Springfield, Virginia.
- Juniper – Sunnyvale, California.
- 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.

Test Adequacy

In September 2020, the JRSS SAG implemented an updated test strategy that relies on the Joint Interoperability Test Command (JITC) to continuously monitor the live system and produce risk assessments of new capabilities to determine the necessary level of test. These monitoring and risk assessment processes are still maturing, causing new challenges for JITC and the test community. JRSS upgrade schedules have not been made available to assist in planning risk assessments, and the JRSS Program Management Office (PMO) has not committed to considering operational test data in deployment or migration decisions. JITC is also working to identify



Joint Regional Security Stack (JRSS)

additional measures to include in their continuous monitoring reports.

In October 2020, JITC and the Army Combat Capabilities Development Command Data and Analysis Center conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) of selected JRSS stacks. This event was adequate to inform the PMO of findings to help improve system security, but did not support a decision.

Performance

Effectiveness

Previous operational assessments of JRSS have demonstrated that JRSS capabilities do not help cyber defenders thwart operationally realistic cyber threats. No operational test events were conducted in 2021 that provided data on JRSS operational effectiveness.

Suitability

Previous operational assessments of JRSS have shown that operator proficiency is a persistent shortfall, indicating the JRSS training processes and system usability need improvement. JITC has produced two quarterly reports on some aspects of JRSS for the continuous monitoring approach, which have not indicated problems with stack availability. No operational test events were conducted in 2021 that provided data on JRSS operational suitability.

Survivability

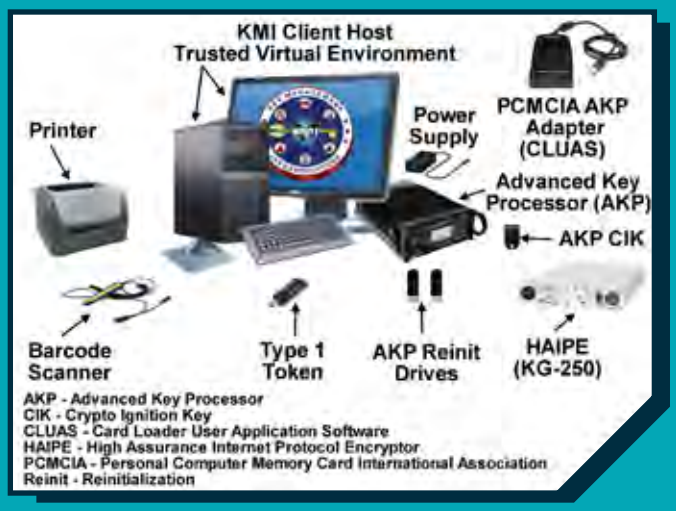
The October 2020 CVPA yielded findings that the PMO could use to improve system security. A follow-on Adversarial Assessment has not yet occurred due to Red Team availability and the pending migration to System Integration and Event Management (SIEM) 2.0.

Recommendations

1. The DOD CIO and the DOD Components should transition from JRSS to a Zero Trust cybersecurity architecture, involving layered and data-centric security as quickly as possible.
2. The JRSS PMO should generate, maintain, and make available a master schedule, which shows the final capability developments currently anticipated, as well as major strategic milestones for sun-setting JRSS. The schedule should be reconciled with progress and milestones for the incoming replacement capability. As updates are available to this schedule, the PMO should share and coordinate directly with JITC and JRSS stakeholders to support risk assessments and continuous monitoring activities, as well as DOD Component planning, until the incoming capability is fully adopted.
3. JITC and the DOD Components should collaborate to identify and implement meaningful metrics in JITC's continuous monitoring reports.
4. The JRSS PMO and JITC should implement a method to ensure that any new capabilities and upgrades are evaluated via risk-based analyses to support the continuous monitoring test strategy.
5. The JRSS PMO, DOD Components, and JITC should proceed with the planning of an Adversarial Assessment against JRSS, inclusive of the new SIEM 2.0 capability.
6. DISA should assure adequate test funding to support a successful operational transition from JRSS to the incoming replacement capability.

Key Management Infrastructure (KMI)

The National Security Agency (NSA) Senior Acquisition Executive approved the Key Management Infrastructure (KMI) Increment 3 Milestone B in November 2020. The NSA awarded the KMI Increment 3 development contract in January 2021. The Joint Interoperability Test Command (JITC) intends to conduct early KMI Increment 3 release testing scheduled in late 2022.



System Description

KMI replaces the legacy Electronic Key Management System (EKMS) to provide a means for securely ordering, generating, producing, distributing, managing, and auditing cryptographic products, to include encryption keys, cryptographic applications, and account management tools. KMI consists of core nodes that provide web operations at sites operated by the 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, which include a client host computer with monitor and peripherals, printer, and barcode scanner.

Program

The NSA is delivering KMI Increment 3 in eight planned Agile releases that will enhance existing capabilities and subsume EKMS Tier 0 and Tier 1 cryptographic product delivery into the infrastructure. The KMI Program Management Office (PMO) produced an initial draft test and deployment schedule for the Increment 3 acquisition in September 2021 that supports Release 0 infrastructure and initial capability enhancements; however, the schedule has yet to be updated with the Tier 0 and Tier 1 infrastructure requirements. The KMI PMO began Increment 3 capability development in July 2021.

Major Contractor

Leidos – Columbia, Maryland (Prime).

Test Adequacy

The KMI Increment 3 Test and Evaluation Master Plan, approved by DOT&E in August 2020, defines an adequate operational test strategy for the KMI program release testing through IOT&E scheduled for late FY25. JITC is developing the operational test plan in late 2021 to support early KMI Increment 3 release testing that will commence in late 2022.

Performance

The preliminary performance assessment will be available after the completion of the early KMI Increment 3 release testing in late 2022. The KMI test community is concerned about the overly aggressive KMI Increment 3 schedule and concurrency with test planning, execution, and reporting. In addition, while the KMI Test Infrastructure provides a safe laboratory for evaluating KMI software builds, it is currently not maintained in the same configuration as the operational KMI. This may limit the KMI Test Infrastructure users' ability to identify problems prior to deploying a new KMI release to the operational system; however, the PMO intends to refresh the KMI Test Infrastructure and the production system to be the same in Increment 3.

Recommendations

1. The KMI PMO should reassess the release cadence to reduce delivery and test concurrency to make the schedule more achievable.
2. JITC should employ a multi-release test plan that would cover up to four releases over two years, since the test team will not know what KMI capabilities will be in each release until 45-60 days prior to testing.
3. The NSA should maintain the KMI Test Infrastructure configuration to be the same as the operational environment.

Public Key Infrastructure (PKI) Increment 2

The DOD Public Key Infrastructure (PKI) Increment 2 is operationally effective, demonstrating the capability to facilitate secure electronic information exchanges between DOD users and network devices. PKI's Token Management System (TMS) is not operationally suitable due to significant problems with SIPRNET token ordering processes and accountability, with over 143,000 unaccounted for tokens worth over $1.4 million. The NIPRNET Enterprise Alternate Token System (NEATS) is not secure against moderate cyber threats.

System Description

PKI Increment 2 provides the hardware, software, and services to generate, publish, revoke, and validate NIPRNET and SIPRNET public and private key certificates. Specifically, PKI Increment 2 delivers the NEATS, Non-person Entity (NPE), and TMS capabilities. Commanders at all levels use DOD PKI to provide authenticated identity management via personal identification number-protected Common Access Cards or SIPRNET or NEATS tokens to enable DOD members, coalition partners, and other authorized users to access restricted websites, enroll in online services, and encrypt/decrypt and digitally sign email. Military operators, communities of interest, and other authorized users use DOD PKI to securely access, process, store, transport, and use information, applications, and networks. Military network operators use NPE certificates for workstations, web servers, and devices to create secure network domains, which facilitate intrusion protection and detection.

Program

The National Security Agency (NSA) has developed and is deploying PKI Increment 2 in four spirals on SIPRNET and NIPRNET. The NSA delivered the SIPRNET TMS in Spirals 1, 2, and 3 prior to late August 2018. Spiral 4 is intended to deliver NEATS and NPE NIPRNET and SIPRNET capabilities. DOT&E approved the PKI Spiral 4 Test and Evaluation Master Plan Addendum in October 2017. The NSA developed the NEATS with the Defense Manpower Data Center (DMDC), and NPE with operational support from the Defense Information Systems Agency (DISA), which provide PKI support for the DOD. NPE and NEATS use commercial and government off-the-shelf hardware and software hosted at DISA and DMDC operational sites. DOT&E approved the PKI Increment 2 FOT&E plan in October 2020 and Cybersecurity Annex in November 2020. DOT&E published the PKI Increment 2 Report in September 2021 in support of a full deployment decision projected in mid-2023.

Major Contractors

- General Dynamics Mission Systems – Dedham, Massachusetts (Prime for TMS and NPE).
- Global Connections to Employment – Lorton, Virginia (Prime for NEATS).
- SafeNet Assured Technologies – Abingdon, Maryland.
- Giesecke and Devrient America – Twinsburg, Ohio.

Test Adequacy

The Joint Interoperability Test Command (JITC) conducted the PKI Increment 2 FOT&E from late November 2020 through March 2021, in accordance with a DOT&E-approved test plan. Testing was adequate to verify system fixes, assess operational effectiveness and suitability of PKI capabilities for long-term sustainment and transition, and inform a full deployment decision for PKI Increment 2.

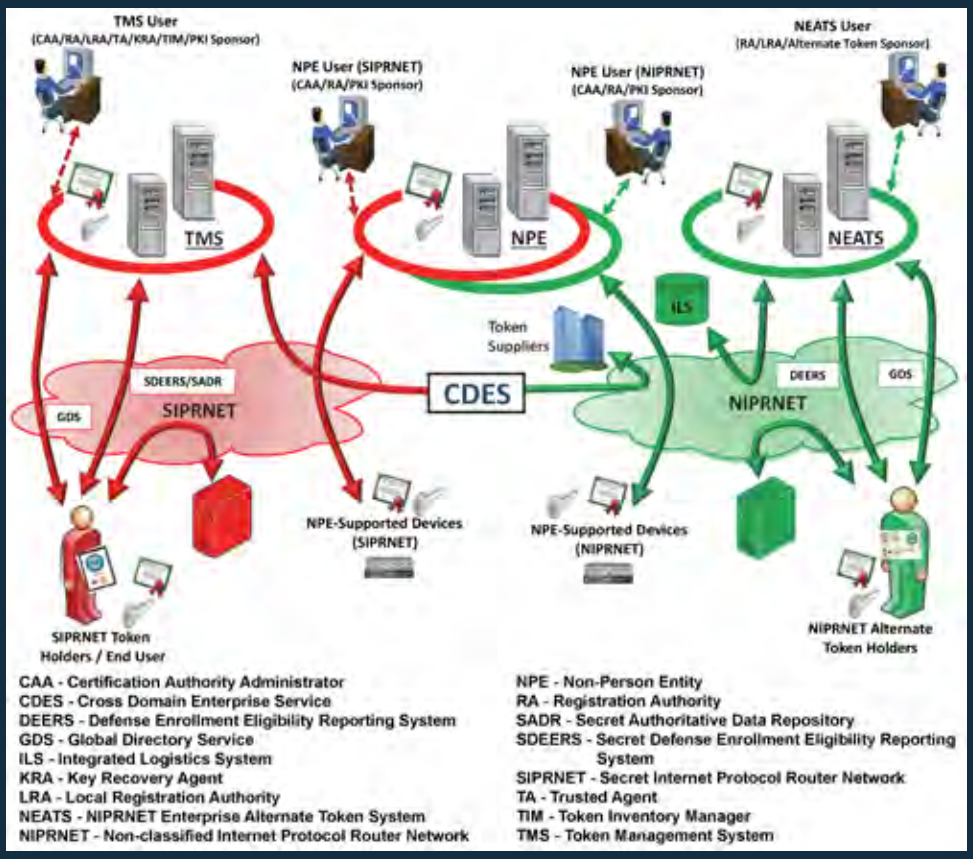
The PKI Program Management Office (PMO) interfered with test data collection and investigative processes, which is antithetical to the DOD's independent operational testing approach. While such actions did not ultimately affect DOT&E's and JITC's ability to assess the system, PMO test interference is a problem that DOT&E addressed in a separate memorandum to NSA leadership to prevent such actions from happening in the future.

Performance

Effectiveness

NEATS, NPE, and TMS are operationally effective, with a caveat that all three systems experienced problems accessing the Certificate Revocation List using the Robust Certificate Validation System within the required timelines, which potentially allows users to access restricted systems using revoked certificates. Additionally, the NPE auto-rekey functionality on devices using the Enrollment over Secure Transport

PKI Increment 2 delivers the NEATS, NPE, and TMS capabilities.



(EST) protocol performed inconsistently and remains not operationally effective as an enterprise capability.

Suitability

NEATS and NPE are operationally suitable, with a caveat that the DMDC NEATS help desk responsiveness is not satisfactory and the application experienced unexplained brief outages on the client that affected token processing. TMS is not operationally suitable because the Central Management of Tokens system and processes resulted in a lack of token accountability, with over 143,000 unaccounted for tokens worth over $1.4 million. JITC also uncovered critical token ordering and logistics problems with TMS. The PKI DISA Integration Lab (DIL) designed to test new token variants and device certificates does not support user needs. The PKI lifecycle sustainment plan and transition plan remained not finalized or ready for assessment five months after the test. TMS capabilities are not ready for long-term sustainment and transition.

Survivability

NEATS is not secure against moderate capability nearsider and advanced capability outsider threats. JITC conducted NPE and TMS cyber survivability testing in July 2021; however, the systems' cyber survivability status remains undetermined, pending completion of operational cybersecurity test analyses and classified reporting in late 2021.

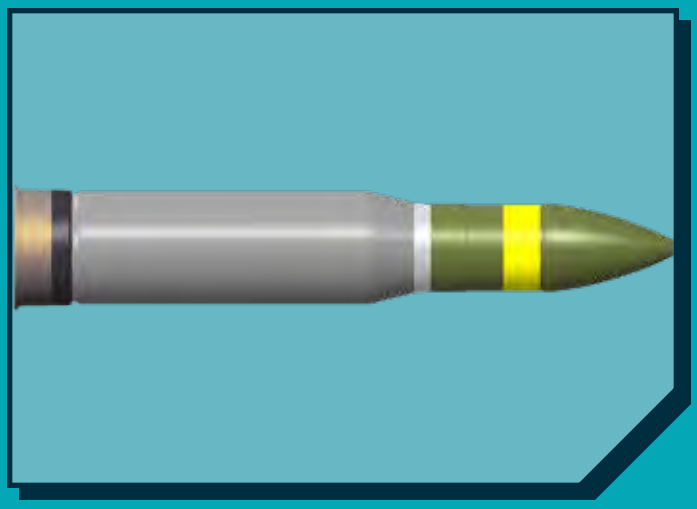
Recommendations

1. The PKI PMO, DMDC, and DISA should establish a reproducible and accurate token ordering and accountability process for TMS, correct software compatibility and long-term sustainment problems, and improve training and help desk support.
2. The PKI PMO and DMDC should remediate the identified NEATS vulnerabilities found during cyber assessments over the past two years to secure this system and supporting environment.
3. The NSA and JITC should conduct comprehensive, independent, operational capability testing with advanced threat-representative cybersecurity cooperative and adversarial assessments of NEATS to improve cyber survivability prior to full deployment in mid-2023.
4. The PKI PMO should fix EST protocol-related auto-rekey problems before fielding and coordinate with other device manufacturers to assist with NPE EST protocol configuration to improve usefulness and reliability.
5. The PKI PMO and DISA should ensure the PKI DIL supports Service and Agency TMS and NPE functional testing and remote access.

Army Programs

120mm Advanced Multi-Purpose (AMP), XM1147

Preliminary analysis of the 120mm Advanced Multi-Purpose (AMP) round IOT&E, completed in September 2021, indicates that the Abrams tank unit can effectively employ the 120mm AMP round to destroy or degrade intended targets at operationally realistic ranges. Preliminary analysis suggests that the AMP round is reliable and survivable in a cyber-contested environment. A final assessment will be summarized in the 120mm AMP IOT&E and LFT&E report in 3QFY22 to support the Army's full-rate production decision scheduled for 4QFY22.



System Description

The 120mm AMP round, termed XM1147, is a line of sight, full-bore multipurpose munition employed by Abrams tanks. The AMP round consolidates the capabilities of four rounds: the M830 High Explosive Anti-Tank round, M830A1 Multi-Purpose Anti-Tank round, M1028 Canister round, and M908 Obstacle Reduction round, into one round, intended to add new capabilities for breaching walls and against dismounted Anti-Tank Guided Missile (ATGM) teams at extended ranges.

Program

The 120mm AMP is an Acquisition Category III program. The program entered Milestone C in December 2020. DOT&E approved the 120mm AMP Test and Evaluation Master Plan to include the LFT&E Strategy in December 2020, and the IOT&E plan in August 2021. The Joint Program Executive expects to make a full-rate production decision in 4QFY22.

Major Contractor

Northrop Grumman Defense Systems – Minneapolis, Minnesota.

Test Adequacy

The Army Test and Evaluation Command (ATEC) conducted an IOT&E in accordance with a DOT&E-approved test plan from September 7-26, 2021 at Yuma Proving Grounds, Arizona. Testing was adequate to evaluate the 120mm AMP operational effectiveness and suitability. In FY21, ATEC continued the 120mm AMP live fire lethality testing to evaluate its lethal effects against hard targets, to include bunkers and walls, and light and heavy armored vehicle targets. Live fire lethality testing also supported the evaluation of the 120mm

AMP sensitivity to kinetic threat impact and crew vulnerability to consequent onboard, 120mm AMP energetic reaction. Live fire testing was conducted in accordance with the DOT&E-approved test plan.

Performance

Effectiveness

IOT&E data analysis is ongoing, precluding a final assessment of the 120mm AMP round operational effectiveness. Live fire testing and modeling is ongoing, precluding a final assessment of the 120mm AMP lethality. Preliminary assessments indicate that the Abrams tank unit can effectively engage and destroy or degrade intended targets with the 120mm AMP at operationally realistic ranges. Required 120mm AMP lethal effects against ATGM teams at extended ranges are dependent on the capabilities and limitations of the laser range finder and second generation forward-looking infrared sight system. Final operational effectiveness and lethality assessment will be summarized in the 120mm AMP IOT&E and LFT&E report to be published in 3QFY22.

Suitability

IOT&E data analysis is ongoing, precluding a final assessment of the 120mm AMP round operational suitability. Preliminary analysis suggests that the 120mm AMP round is reliable. Final assessment of operational suitability will be summarized in the 120mm AMP IOT&E and LFT&E report to be published in 3QFY22.

Survivability

The 120mm AMP round is survivable in a cyber-contested environment. The fuze cannot be programmed in advance, even with access to the round, and the only means for communicating with the 120mm AMP round is via the Ammunition Data Link when the round is chambered on the Abrams platform.

Recommendation

1. Recommendations will be detailed in the 120mm AMP IOT&E and LFT&E report in 3QFY22 after the completion of IOT&E and LFT&E data analysis.

7.62mm Advanced Armor Piercing (ADVAP), M1158

The M1158 Advanced Armor Piercing (ADVAP) ammunition is lethal demonstrating increased lethal effects as compared to the currently fielded M80A1 and M993 rounds. The M1158 LFT&E was adequate to support the full-rate production scheduled for September 2025.

System Description

The M1158 Advanced Armor Piercing (ADVAP) is a new 7.62mm round designed to provide dismounted infantry with an overmatch capability against a broad spectrum of targets as compared to the legacy M993 armor piercing (AP) and M80A1 Enhanced Performance Rounds. The M1158 round is compatible with the M240 series of machine guns; the Mk 48 machine gun; and the M110, Mk 17, Mk 14, and M14 series rifles.

Program

The M1158 ADVAP is an Acquisition Category III program. The Army began low-rate initial production in May 2019 to support an urgent material release in October 2019. The Army approved the M1158 Milestone C and Type Classification Standard in January 2020. DOT&E approved the Milestone C Test and Evaluation Master Plan in May 2020. In December 2020, the Army completed lethality testing to support the full material release decision in March 2021 and the full-rate production decision planned for September 2025.

Test Adequacy

The Army completed LFT&E in December 2020 in accordance with DOT&E-approved test plans. Testing was adequate to evaluate M1158 lethality in support of the full material release decision.

Performance

The M1158 round is lethal. Additional details including target descriptions, lethality performance, and limitations as well as comparison to the legacy M993 and M80A1 rounds are available in the classified LFT&E report, published in October 2021. Specifically, the report summarizes the ability of a shooter equipped with M1158 and an M240 series machine gun to incapacitate an armed adversary in a wide array of operationally representative conditions.

Recommendation

1. The Army should update the small arms warfighter training based on the recommendation detailed in the classified report.

Abrams M1A2 System Enhancement Package version 3 (SEPv3) Tank with Trophy Active Protection System (APS)

In FY21, the Army initiated testing of the Trophy Active Protection System (APS) installed on Abrams M1A2 System Enhancement Package version 3 (SEPv3) tanks to inform the urgent materiel release. Preliminary analysis indicates that the Trophy APS effectively detects, identifies, tracks, and intercepts most of the incoming threats in basic range conditions and engagements. The Army needs to address the identified Trophy APS-equipped Abrams' operational suitability concerns. Abrams tank base armor configurations have the potential to provide adequate force protection against the debris generated by a successful intercept.

M1A2 Abrams System Enhancement Package version 2 With Trophy Active Protection System

System Description

The Abrams M1A2 is a tracked, land combat, assault vehicle equipped with a 120mm main gun, enabling maneuverability across the full range of military operations to destroy the enemy by fire. The Army intends to equip the Abrams M1A2 with a 5,000 pound Trophy APS to offer additional defense and improved survivability against anti-tank guided missiles and rocket-propelled grenades. The Trophy APS is designed to search, detect, identify, track, and then intercept such threats with its inherent kinetic countermeasures.

Program

The Abrams M1A2 is an Acquisition Category IC program. In response to directed requirements from the Army G-8 issued in October 2016 and again in March 2018, the Army is installing the non-developmental Trophy APS on the Abrams M1A2. The Army has not documented any Trophy APS operational requirements, which has affected the test planning process and the assessment of adequate warfighting capability.

Software upgrade delays from General Dynamics Land Systems caused the Army to reschedule the urgent materiel release from December 2021 to June 2022.

Major Contractors

General Dynamics Land Systems – Sterling Heights, Michigan. DRS/Rafael – St. Louis, Missouri.

Test Adequacy

The Army Test and Evaluation Command is currently testing the Abrams M1A2 SEPv3 equipped with Trophy APS in accordance with the DOT&E-approved test plan. Test results will inform an update to the DOT&E classified report published in June 2020 to support the urgent materiel release scheduled for June 2022.

Performance

Effectiveness

Preliminary analysis indicates that the Trophy APS effectively detects, identifies, tracks, and intercepts most of the incoming threats in basic range conditions and engagements. The system as installed on SEPv3 appears to retain operational effectiveness limitations noted in the Abrams SEPv2 APS test report published in June 2020. Final assessment of the performance of the Trophy APS equipped Abrams SEPv3 tank will be detailed in a classified report in 2QFY22, after the completion of live fire testing, to support the urgent materiel release scheduled for June 2022.

Suitability

Preliminary analysis indicates that Army has to overcome several challenges to demonstrate the operational suitability of the Trophy APS-equipped tanks. The M1A2 SEP v2 and v3 overall weight growth with full combat load and Trophy APS has introduced transportability and recovery challenges. The Army intends to restore the ability to recover a Trophy APS equipped Abrams with an upgrade to the M88 recovery vehicle.

Survivability

The survivability of the Trophy APS equipped Abrams SEPv3 tank is largely proportional to the operational effectiveness of the Trophy APS to search, detect, identify, track, and intercept the incoming threats. Survivability is also dependent on the capability of the Abrams base armor to absorb the threat by-products generated after a successful intercept. Preliminary analysis indicates that Abrams SEP v2 and v3 base armor configurations have the potential to provide adequate force protection against the threat and countermeasure debris generated by a successful intercept.

Recommendation

1. The Army should develop a requirements document for the Abrams M1A2 tank with Trophy APS.

AN/TPQ-53 Counterfire Target Acquisition Radar

The Army intends to extend the range for the currently fielded Q-53 target acquisition radars using hardware and software upgrades. Preliminary developmental test data demonstrate an improved Q-53 performance compared to the legacy variant. The Army plans additional Q-53 upgrades to further improve its performance in a contested environment and is scheduled to conduct operational testing to evaluate its operational effectiveness, suitability and survivability.

System Description

The Q-53 is a mobile, counterfire target acquisition radar designed to detect, classify, and track projectiles fired from mortar, artillery, and rocket systems. The Q-53 radar is fielded to the target acquisition platoons in Brigade Combat Teams, target acquisition batteries in Field Artillery Brigades, and Division Artillery headquarters. Field Artillery units employ the Q-53 to locate and suppress, neutralize, or destroy adversary rocket, artillery, and mortar systems through effective counterfire engagements. Air Defense Artillery units integrate the Q-53 radar to warn friendly forces and engage incoming threat indirect fires. The Q-53 is transportable by C-17 aircraft.

Program

The Q-53 is an Acquisition Category IC program that entered full-rate production in December 2015. The Army has since implemented hardware and software upgrades to improve reliability and address parts obsolescence to extend the range over which the radar can acquire rockets, artillery, and mortars. The Army plans additional upgrades using a Distributed Digital Receiver Exciter (DDREX) to further improve the Q-53 performance.

Major Contractor

Lockheed Martin Missile Systems and Training – Syracuse, New York.

Test Adequacy

The Army conducted a Customer Test 5 from July 12 to August 6, 2021 of the extended range radar using civilian operators to provide a baseline performance for comparison with the future DDREX radar. The Army conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) on the Q-53 extended range radar in October 2020 and again in February 2021 given the software upgrades. Using the CVPA findings, the Army

planned and executed an Adversarial Assessment in July 2021. Tests were conducted in accordance with DOT&E-approved test plans. The Army also executed a Soldier Touchpoint using two systems. The Army has not yet started developing the Q-53 DDREX Test and Evaluation Master Plan.

Performance

Effectiveness

The operational effectiveness of the Q-53 extended range radar using hardware and software upgrades cannot yet be evaluated. Preliminary developmental test results demonstrate an improved Q-53 performance compared to the previous Q-53 variant evaluated in 2015.

Suitability

The operational suitability of the Q-53 extended range radar using hardware and software upgrades cannot yet be evaluated. Preliminary developmental test results demonstrated an improved Q-53 performance compared to the previous variant evaluated in 2015 that also exceeded the reliability requirement.

Survivability

The survivability of the Q-53 in a cyber-contested environment has not yet been evaluated.

Recommendations

The Army should:

1. Execute an operational assessment on the extended range Q-53 radar as part of the DDREX upgrade.
2. Continue to improve and assess the radar's reliability.
3. Develop the Test and Evaluation Master Plan for the planned DDREX upgrade.
4. Plan and execute an IOT&E, CVPA, and Adversarial Assessment for the DDREX upgrade and associated software and hardware upgrades in an operationally relevant and stressing environment with threat munitions and countermeasures.

Armored Multi-Purpose Vehicle (AMPV)

The 2018 Limited User Test (LUT) did not reveal any significant risks to demonstrating Armored Multi-Purpose Vehicle (AMPV) operational effectiveness as it proceeds to IOT&E scheduled to begin in March 2022. The Army needs to continue to address several deficiencies to mitigate the risk to demonstrating AMPV operational suitability as it proceeds to IOT&E. Final assessment of AMPV operational effectiveness, suitability, and survivability will be provided after the completion of IOT&E and LFT&E to inform the full-rate production scheduled in 1QFY23.

System Description

AMPV is a tracked, ground combat vehicle that provides logistical resupply, casualty evacuation and treatment, command post operations, and heavy mortar fire support. There are five variants: the General Purpose (GP), Mission Command (CD), Medical Treatment (MT), Medical Evacuation (ME), and Mortar Carrier (MC). The Army intends for the AMPV to address the M113 Family of Vehicles (FoV) shortcomings in survivability and force protection; size, weight, power, and cooling; and the ability to incorporate future technologies, such as the Army Network.

Program

AMPV is an Acquisition IC program that entered Milestone C in January 2019. The Army conducted a LUT in September 2018 in accordance with the DOT&E-approved test plan. In January 2021, the Program Office re-baselined the program schedule due to BAE System's production start-up issues and the impact of COVID-19. Based on BAE System's recovery plans, the program manager anticipates delivering the vehicles required for operational testing no later than November 2021. IOT&E is scheduled to begin in March 2022 to support the Army's full-rate production decision scheduled for 1QFY23.

In May 2021, DOT&E approved changes to the Milestone C Test and Evaluation Master Plan to efficiently leverage previous live fire testing data, reducing the number of vehicles from 10 to 7 to support the Full-up System Level (FUSL) LFT&E program.

Major Contractor

BAE Systems – York, Pennsylvania.

Test Adequacy

In January 2021, the Army completed system-level live fire testing on prototype vehicles in accordance with DOT&E-approved test plans. FUSL testing started in May 2021 and is expected to be completed in March 2022. The Army executed FUSL events using production vehicles to evaluate system and crew vulnerability to kinetic threat engagements. The Army is planning a test to evaluate the effectiveness of the Automated Fire Extinguishing System.

The planning of IOT&E, scheduled for March 2022, is ongoing. The Army conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) in September 2021 in accordance with the DOT&E-approved test plan. DOT&E intends to publish a combined IOT&E and LFT&E Report in 4QFY22.

Performance

Effectiveness

The 2018 LUT did not reveal any significant risks to demonstrating AMPV operational effectiveness as it proceeds to IOT&E scheduled to begin in March 2022. During the 2018 LUT, the AMPV demonstrated increased capability over the MI113 FoV. All elements of the test unit equipped with the AMPV variants demonstrated the ability to successfully accomplish their required tasks and purposes. AMPV mobility is comparable to the mobility of the Abrams tank and Bradley Fighting Vehicle, which enables it to maintain its position in the tactical formation. Of note, the GP variant increased the first sergeant's ability to conduct logistical resupply with its increased mobility and interior space. The medical treatment and ambulance variants provided a level of medical treatment capability currently not available to the brigade combat team.

Suitability

The Army needs to address several deficiencies to mitigate the risk to demonstrating AMPV operational suitability as it proceeds to IOT&E. The Program Office is addressing reliability failures identified during the 2018 LUT and is subsequently upgrading production qualification and initial operational test vehicles. While the mean time between system aborts continues to improve, the mean time between effective function failures is below the Army required threshold. The program manager has been working with BAE Systems to understand and mitigate these failure modes prior to IOT&E. The program manager has also been working on addressing several failure modes noted at the LUT that have been reoccurring during production testing.

Survivability

The AMPV demonstrated the potential to meet force protection and vehicle survivability requirements against specified kinetic threats. Coordination with the Army has enabled the test team to potentially conduct remote access threat vectors against the platform during both the CVPA and during the IOT&E. Final survivability assessment of the AMPV in a cyber-contested environment will be provided after the completion of IOT&E.

Recommendations

The Army should:

1. Continue to validate through FUSL testing design changes intended to mitigate vehicle and crew vulnerabilities found in live fire testing.
2. Continue to apply corrective actions and identify the root cause for the observed failure modes.

Army Integrated Air & Missile Defense (AIAMD)

The Army Integrated Air and Missile Defense (AIAMD) program will enter IOT&E in January 2022. Final assessment of AIAMD operational effectiveness, suitability, and survivability will be published in a classified report, after the completion of IOT&E, to inform the full-rate production decision scheduled for December 2022.

System Description

AIAMD is a command and control system that integrates Engagement Operations Centers (EOCs), Sentinel air surveillance radars, and Patriot missile system radars and launchers across an integrated fire control network (IFCN). The EOCs provide the operating environment for soldiers to monitor and direct sensor employment and the engagement of air threats. Hardware interface kits connect adapted Patriot and Sentinel components to the IFCN, either through an EOC or through an IFCN Relay. IFCN Relays also provide mobile communications nodes to extend fire control connectivity and distributed operations. Air Defense Artillery forces will use the AIAMD system to provide the timely detection, identification, monitoring, and (if required) engagement of air threats in support of active defense of the homeland, critical assets and locations, and forces.

Program

AIAMD is an Acquisition Category ID program. DOT&E approved the Milestone C Test and Evaluation Master Plan in April 2019 and the IOT&E test plan in October 2021. The Army intends to enter full-rate production in December 2022.

Major Contractors

- Northrop Grumman Systems Corporation – Huntsville, Alabama.
- Raytheon Missiles and Defense – Huntsville, Alabama and Andover, Massachusetts.
- Lockheed Martin Corporation – Dallas, Texas.

Test Adequacy

The Army Test and Evaluation Command (ATEC) completed a DOT&E-approved cybersecurity Cooperative Vulnerability and Penetration Assessment in August 2021 and an Adversarial Assessment in November 2021. The remaining phases of IOT&E consist of a sustained live air phase, a sustained software/hardware-in-the-loop phase, and missile flight tests. ATEC will accredit the modeling and simulation tools required for the software/hardware-in-the-loop phase.

Performance

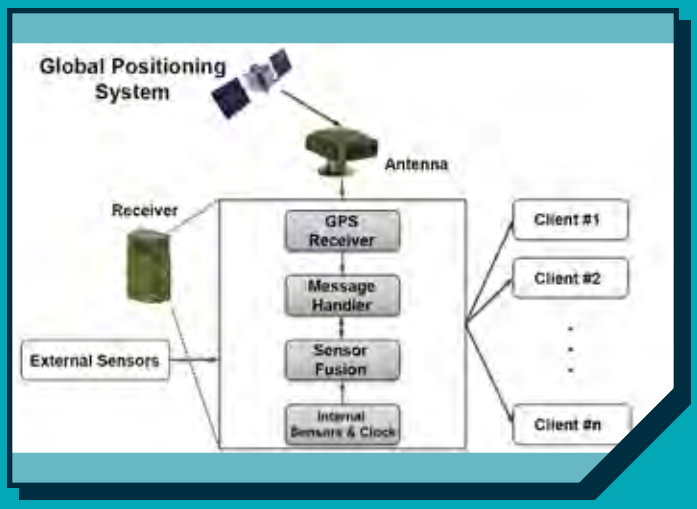
Deficiencies in some critical capabilities identified during software testing caused the Army to delay the start of IOT&E from September 2021 to January 2022. The program remains on track to complete IOT&E per the Milestone C Acquisition Program Baseline. Final assessment of AIAMD operational effectiveness, suitability, and survivability will be detailed in a classified report after IOT&E to support the full-rate production decision scheduled for December 2022.

Recommendation

1. The Army should continue to improve the modeling and simulation tools as well as validation processes.

Assured–Positioning, Navigation, and Timing (A–PNT)

Assured-Positioning, Navigation, and Timing (A-PNT) products, including the Dismounted A-PNT System (DAPS) and Mounted A-PNT System (MAPS), continued with prototyping efforts and conducted early operational testing in FY21. MAPS and DAPS will enter Program of Record status as Major Capability Acquisition programs in FY22 and FY23 respectively. In early testing, A-PNT products performed better than legacy PNT systems in GPS-degraded or denied environments.



System Description

A-PNT products are intended to provide ground maneuver forces with access to trusted PNT information in GPS-degraded or denied environments, such as operations in dense vegetation, built-up urban and mountainous terrain, and in the presence of electromagnetic spectrum interference or enemy GPS jamming and spoofing. The four primary product families include:

- MAPS – Vehicle-mounted system providing PNT to multiple onboard client systems.
- DAPS – Soldier-worn system providing PNT for dismounted operations.
- Resiliency and Software Assurance Measures – Software upgrades to legacy military GPS receivers.
- PNT Modernization – Alternative solutions and complementary PNT technologies for integration into MAPS and DAPS systems.

MAPS GEN II, DAPS GEN 1.0, and GEN 1.2 are all Military Code (M-Code) GPS-enabled systems and support the Army's transition to M-Code GPS.

Program

In 2019, the Commanding General, Army Futures Command issued individual Directed Requirements for the DAPS and MAPS efforts directing the rapid prototyping, operational assessment, and limited fielding of advanced PNT technologies. The Directed Requirements outlined a "buy, try, and decide" process to inform an enduring requirement and follow-on programs of record. The PNT Program Manager is utilizing several Other Transaction Authority contracts and a phased prototyping approach to satisfy the Army Futures Command Directed Requirements.

DAPS GEN 1.0 and DAPS GEN 1.2 are following the Urgent Capability Acquisition pathway and will result in a limited equipping of two Infantry Brigade Combat Teams in FY22. In early FY22, DAPS will enter Program

of Record status at Milestone C as an Acquisition Category II, Major Capability Acquisition program. A DAPS Test and Evaluation Master Plan (TEMP) is currently in draft and expected to be approved by DOT&E ahead of the planned Milestone-C decision in FY23.

MAPS GEN II will replace the existing GPS receivers and antennas in most of the Army's ground vehicle variants. MAPS GEN II will enter Program of Record status at Milestone C as an Acquisition Category II, Major Capability Acquisition program. A MAPS MS-C TEMP is currently in Army staffing and expected to be approved by DOT&E in early FY22.

Major Contractors:

- DAPS GEN 1.0 – Integrated Solutions for Systems, Inc., Auburn, Alabama.
- DAPS GEN 1.2 – TRX Systems, Inc., Greenbelt, Maryland.
- MAPS GEN II – Collins Aerospace subsidiary of Raytheon Technologies, Cedar Rapids, Iowa.

Test Adequacy

Throughout FY21, the Army Test and Evaluation Command and PNT Program Manager conducted several test-fix-test cycles with each of the MAPS and DAPS solutions to complete prototyping efforts and prepare for entry into Program of Record status. This testing included chamber, systems integration lab, and open-air range testing.

In FY21, the Army conducted an operational assessment of the DAPS GEN 1.0 and GEN 1.2 systems in accordance with a DOT&E-approved test plan. The operational assessment was scoped to determine the performance capabilities and limitations of the GEN 1.0 and GEN 1.2 systems and support limited equipping decisions in accordance with their respective Directed Requirements. Results from the operational assessment will also inform a vendor selection to enter Program of Record status at Milestone C.

In FY21, the Army conducted a Limited User Test (LUT) of the MAPS GEN II system in accordance with a DOT&E-approved test plan. The MAPS LUT will support entry into Program of Record status at Milestone C as an Acquisition Category II, Major Capability Acquisition program.

Cybersecurity testing of DAPS GEN 1.0 and GEN 1.2 systems, and the MAPS GEN II, is scheduled to begin in FY22.

Performance

Effectiveness

Not enough data are yet available to provide an operational effectiveness assessment of either DAPS or MAPS. Early operational testing of the DAPS GEN 1.0 and 1.2 systems and the MAPS GEN II system indicates that both systems performed better than the legacy PNT system in GPS-degraded environments.

Suitability

Not enough data are yet available to provide an operational suitability assessment of either DAPS or MAPS. Early operational testing indicates that with additional development and testing, the DAPS GEN 1.0 and GEN 1.2 systems should be able to achieve their reliability requirement. GEN 1.0 users indicated the desire for the DAPS to have a stand-alone capability and user interface separate from the Nett Warrior ensemble. GEN 1.2 users indicated the need for longer internal battery life when disconnected from the conformal battery.

Early operational testing indicates that the MAPS GEN II system should be able to achieve its reliability requirement. Integration testing revealed that adhering to the GPS interface standard does not guarantee compatibility and software updates to the client systems will be necessary. Significant integration effort remains with complex armored vehicles such as the Stryker Fire Support Vehicle, Bradley Fire Support Team Vehicle and Infantry Fighting Vehicle, Abrams Tank, and Paladin self-propelled howitzer. Extensive integration engineering and testing is planned for FY22-23.

Survivability

No data are currently available to provide a survivability assessment of either DAPS or MAPS in a cyber-contested environment.

Recommendation

1. The Army should start identifying and securing MAPS and DAPS IOT&E locations that will allow for GPS-disrupted and denied testing, as well as sufficient maneuver space for a Battalion-sized combat formation to conduct operationally realistic missions in accordance with their Mission Essential Task List.

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

The Army corrected the Bradley M2A4/M7A4 deficiency identified in the October 2020 FOT&E. Units equipped with the M2A/M7A4 are operationally effective, demonstrating improved capability over the M2A3 in mechanized infantry platoons and companies. The M2/M7A4 Bradley is operationally suitable. The survivability of the M2/M7A4 in a contested environment to include a cyber-contested environment is detailed in the classified survivability annex of the Bradley M2A4/M7A4 FOT&E report published in June 2021.

System Description

Bradley Family of Vehicles (FoV) is a tracked fighting vehicle designed to provide protected transport of soldiers and direct fires to support dismounted infantry, disrupt or destroy enemy military forces, and control land areas. The Bradley FoV Engineering Change Proposal (ECP), termed M2/M7A4, includes changes intended to restore ground clearance, suspension reliability, and lost mobility, and to improve situational awareness. The M2/M7A4 maintains the survivability enhancement features found on legacy vehicles, to include the 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.

Program

The Bradley FoV program is an Acquisition Category IC program. The Army delegated the acquisition decision authority to the Program Executive Officer, Ground Combat Systems. A successful materiel release decision will result in the conversion of existing M2A3, M3A3, and Operation Desert Storm – Situational Awareness versions of Bradley Fighting Vehicles into the M2A4 version, and the conversion of M7A3 Bradley Fire Support Team vehicles into the M7A4 version. The current plan is to field the M2A4 and M7A4 to four brigades. DOT&E approved an updated a Test and Evaluation Master Plan, including an LFT&E Strategy for the ECP, in July 2020, and the Bradley FoV ECP FOT&E plan in September 2020.

Major Contractor

BAE Systems Land and Armaments – Sterling Heights, Michigan.

Test Adequacy

In October 2020, the Army Operational Test Command conducted the FOT&E. The Army Operational Test Command suspended the FOT&E two days early due to an identified design deficiency.

The Army Test and Evaluation Command was still able to collect sufficient data by using data from the pilot test. Testing was adequate to inform the program manager's decision to delay a materiel release decision and work with the vendor to develop and test a solution to resolve the turret battery deficiency.

Later in FY21, the Army conducted a Gunnery Soldier Touch Point with an M2A4 and M7A4 to determine if the ECP affected the Bradley Fire Control Systems and if the vendor corrected the identified deficiency.

The M2A4 LFT&E program, conducted in two phases from 2018 to 2021 to evaluate force protection and survivability against kinetic threat engagements, was adequate and conducted in accordance with DOT&E-approved plans.

Performance

Effectiveness

Units equipped with the M2/M7A4 are operationally effective, demonstrating improved capability over the M2A3 in mechanized infantry platoons and companies. The M2/M7A4 improves leader situational awareness, allows the unit to maintain tempo while moving over restrictive and complex terrain, and allows crews to react to enemy direct fire contact. The units equipped with the M2/M7A4 are also operationally effective at engaging and hitting targets in offensive and defensive engagements.

Suitability

The Army corrected Bradley's deficiency identified in the October 2020 FOT&E. Given also the improved reliability demonstrated in Production Verification Testing, the M2/M7A4 Bradley is operationally suitable. The heat generated in the crew and troop compartments by the vehicle engine, exhaust, and electronics is still a concern that needs to be resolved.

Survivability

The survivability of the M2/M7A4 in a contested environment to include a cyber-contested environment is detailed in the classified survivability annex of the Bradley M2A4/M7A4 FOT&E report published in June 2021.

Recommendations

The Army should address the two remaining recommendations identified in the Bradley M2A4/M7A4 FOT&E report published in June 2021:

1. Continue efforts to mitigate the excessive heating in the crew, troop, and engine compartments to improve the soldiers' physical readiness to fight.
2. Mitigate the identified vulnerabilities to kinetic and cyber threats.

Command Post Computing Environment (CPCE)

Preliminary analysis of the operational test data indicate that the Command Post Computing Environment (CPCE) Increment 1 is operationally effective in supporting commanders and staff with improved situational awareness and mission command, and provides corrections for deficiencies fielded with CPCE Increment 0. CPCE Increment 1 is not operationally suitable, demonstrating problems with reliability, training, and usability. CPCE Increment 1 is survivable, and demonstrated an enhanced defensive posture within a cyber-contested environment. The Army intends to conduct a CPCE Increment 1 full deployment decision in 1QFY22.

System Description

CPCE Increment 1 is a server-based software system that provides server hardware and mission command software to support commanders and staff using general purpose client computers, located within battalion, through corps Tactical Operations Centers. CPCE Increment 1 is the Army's planned evolution of the fielded CPCE Increment 0, and is intended to improve the soldier's user experience, interface with more data sources, and corrected fielded deficiencies. The CPCE Increment 1-supporting server hardware consists of two variants: a Tactical Server Infrastructure (TSI) Large, a full server stack designed to support headquarters at brigade level and above, and the TSI Small, a laptop-based server designed to support battalion headquarters and provide back-up capabilities for higher echelons. The CPCE Increment 1 software provides a common operational picture, a suite of web-based collaboration tools and messaging capabilities to facilitate the commander and staff to plan, prepare, execute, and assess Army operations. The Army designed CPCE Increment 1 to share information with joint and coalition partners utilizing the Multilateral Interoperability Programme standard.

Program

The Army designated the CPCE program as an Acquisition Category II program and delegated Milestone Decision Authority to the Program Executive Officer, Command Control Communications – Tactical. The Army conducted a CPCE Increment 0 IOT&E in November 2018. On June 13, 2019, DOT&E published a CPCE Increment 0 IOT&E report, which assessed the system as not effective, not suitable, and not survivable. The Army conducted a full deployment decision and approved a CPCE Increment 0 software fielding in July of 2019. In accordance with the CPCE Increment 0 Full Deployment Decision Acquisition Decision Memorandum, the Army conducted a developmental test in November 2019 and demonstrated correction of several IOT&E deficiencies.

DOT&E approved the CPCE Increment 1 Test and Evaluation Master Plan in November 2019 and approved the CPCE Increment 1 Operational Test Plan in June 2021. The Army completed a June 2021 CPCE Increment 1 Operational Test in accordance with the DOT&E approved test plan, and intends to conduct a full deployment decision in 1QFY22. DOT&E is completing a CPCE Increment 1 Operational Test report to support this fielding decision.

Major Contractors

Weapons Software Engineering Center – Picatinny Arsenal, New Jersey. Systematic USA/Systematic AS – Centreville, Virginia/Aarhus, Denmark.

Test Adequacy

The Army conducted a CPCE Increment 1 Operational Test, which included an Adversarial Assessment, at Fort Carson, Colorado from June 7-24, 2021, and a Cooperative Vulnerability and Penetration Assessment, at Fort Bragg, North Carolina from April 5-9, 2021. Operational testing, executed by elements of the 4th Infantry Division and allied partners operating within a command post exercise environment, was adequate to evaluate the CPCE Increment 1 operational effectiveness, suitability, and survivability. The Army conducted the operational test in accordance with a DOT&E-approved test plan and intends to use the results to support the planned 1QFY22 CPCE Increment 1 full deployment decision.

Since the discontinuation of Network Integration Evaluations, the Army has shifted operational testing of mission command systems to larger events, vice dedicated operational tests. In this case, the Army combined the CPCE Increment 1 Operational Test with the Joint Warfighter Assessment 21. The operational test included several limitations, mostly related to the command post exercise environment of the test. These limitations included collocated servers for all headquarters, reduced manning of system administrators, and employment of a fiber optic network instead of tactical communications. The full description of adequacy and limitations will be included in the pending CPCE Increment 1 Operational Test report intended to support the Army's 1QFY22 full deployment decision.

The Army completed a partial verification and validation of data instrumentation prior to the CPCE Increment 1 Operational Test due to problems with their data collection, reduction, and assessment process. DOT&E approved the operational test plan with the condition that the Army would complete the verification and validation effort following testing, and that during testing, data instrumentation would collect useful operational test data to support an adequate assessment.

Performance

Effectiveness

Preliminary analyses indicate that CPCE Increment 1 is operationally effective, enabling commanders and staff to share a single common operational picture and common operations data across staff elements, and experience an improved ability to share information with joint and coalition partners. Commanders and staff experienced improved mission execution and situational awareness, but also experienced difficulties in using CPCE Increment 1 to execute the full Army operations process. Soldiers' problems were related to poor collective and individual training, software functions requiring improvements, and troubleshooting. Soldiers were not able to share plans between current and future operations cells, and had difficulty sharing plans between different servers supporting staff elements. When staffs could not employ CPCE Increment 1, they reverted to previous methods, such as collaboration using paper maps, to complete their mission.

Suitability

Preliminary analyses indicate CPCE Increment 1 is not operationally suitable, demonstrating the following problems with reliability, training, and usability:

- CPCE Increment 1 did not meet its derived reliability requirement. CPCE Increment 1's lack of reliability reduces its support of mission command and increases the unit requirements for maintenance support and field service representatives.
- Training afforded to soldiers did not prepare them to make full use of advanced features,

troubleshooting, and employment of CPCE Increment 1 in a collaborative manner. Soldiers recognized CPCE Increment 1 as intuitive for basic features, but struggled to execute advanced capabilities to complete complicated actions, such as troubleshooting and working with CPCE Increment 1 knowledge managers to share information across servers with other staff elements. CPCE Increment 1 new equipment training offered two levels of soldier training, but did not include a collaborative staff exercise as provided during CPCE Increment 0 training.

- Soldier system administrators experienced difficulty using CPCE Increment 1 tools provided to configure and maintain CPCE software and hardware. These maintainers found CPCE Increment 1 difficult to troubleshoot and viewed CPCE Increment 1 as more manpower intensive than their previous version of servers. Soldier system administrators did not receive formal new equipment training, but were provided over-the-shoulder training from contract field service representatives.

Survivability

The CPCE Increment 1 demonstrated enhanced survivability in a cyber-contested environment as compared to CPCE Increment 0. CPCE Increment 1 maintained a strong cybersecurity defense posture when employed with trained Army cyber defense soldiers using integrated cyber defense tools. The full description of CPCE Increment 1 cybersecurity survivability against an operationally realistic cyber threat will be included in a classified annex to the pending CPCE Increment 1 Operational Test report intended to support the Army's 1QFY22 full deployment decision.

Recommendations

The Army should:

1. Correct the deficiencies identified in the CPCE Increment 1 Operational Test.
2. Improve training afforded to soldiers to allow full use of CPCE Increment 1 advanced capabilities and improve the system administrator's ability to install, operate, and maintain CPCE Increment 1 hardware and software. This training should include a capstone staff exercise to reinforce the collaborative use of CPCE Increment 1.
3. Conduct a complete review of instrumented data collection intended to support mission command and network systems. This review should lead to a set of best practices and an enduring set of data instrumentation that provides flexible and responsive support of both developmental and operational test requirements.

Dark Eagle

The Army, in coordination with the Navy and industry, is currently using rapid prototyping authorities to deliver a prototype ground-launched long range hypersonic weapon, termed Dark Eagle. Not enough data are yet available to evaluate the residual combat capabilities of the Dark Eagle. Testing must incorporate operationally representative targets and environments to support this evaluation and the fielding of one battery with the Dark Eagle system.

System Description

Dark Eagle is a prototype surface-to-surface, long range hypersonic weapon system composed of one launcher and two missiles with canisters. The missile is composed of the Common Hypersonic Glide Body (C-HGB) and a two-stage rocket booster developed by the Navy. The initial Dark Eagle Battery will include a Battery Operations Center and four Transporter Erector Launchers (TELs), each including two missiles.

Program

The Dark Eagle is a rapid prototyping program. In March 2019, the Secretary and Chief of Staff of the Army directed the accelerated delivery of a prototype ground-launched hypersonic weapon with residual combat capability. In developing the Dark Eagle, the Army is working with other Services through a Joint Service Memorandum of Agreement on hypersonic design, development, testing, and production. The Navy program is the Conventional Prompt Strike program. The Army program is the Dark Eagle ground launch capability. The Navy is the design authority for the two-stage rocket booster and the C-HGB, while the Army is responsible for C-HGB production and the design of the ground-launch capability. STRATCOM will identify targets and develop missions for strategic deployment of the joint hypersonic capabilities.

The Army Rapid Capabilities and Critical Technologies Office selected two prime contractors to build and integrate components of the Dark Eagle prototype. In FY19, the Army awarded an Other Transaction Authority (OTA) agreement to Dynetics to produce the first commercially manufactured set of prototype C-HGB systems. The Army awarded a second OTA agreement to Lockheed Martin as the Dark Eagle prototype system integrator.

The Army plans to field the first battery with four TELs and a Battery Operations Center with an inert training canister by FY21. New equipment training (NET) and soldier handling and familiarization with the system began in FY21. In addition, the Army and Navy plan to conduct three Joint Flight Campaign (JFC) test shots. JFC-1 will consist of a missile fired from a launch pad, JFC-2 will consist of a missile fired from a launcher with soldier

involvement, and JFC-3 will consist of a missile fired from a launcher by soldiers.

The Army plans to achieve a residual combat capability when the Army fields one battery with the Dark Eagle system, the updated technical and tactical Fire Control System is available, and the unit is trained. The Army intends to achieve an initial operational capability with the delivery of the second battery.

Major Contractor

Lockheed Martin and Dynetics Technical Solutions – Huntsville, Alabama.

Test Adequacy

The Dark Eagle has not yet developed a Test and Evaluation Master Plan or equivalent document to define the T&E strategy needed to support the determination of either residual combat capability or initial operational capability. The Dark Eagle program has thus far been relying on the Navy and their Conventional Prompt Strike program to evaluate weapon lethality. In FY20, the Navy performed a sled test of the Conventional Prompt Strike warhead, also used by the Dark Eagle, at the Holloman Air Force Base High Speed Test Track, which provided data for validating the lethality modeling and simulation (M&S) tools against materials and targets of interest. The value of the data acquired was limited, as it focused on data for lethality model validation, and did not test against operationally representative targets. Similarly, in March 2020 the Navy conducted a Flight Experiment-2, in which a Conventional Prompt Strike missile was fired from the Pacific Missile Range Facility Barking Sands. The flight test provided warhead performance data, but also lacked operationally representative targets. Neither program has yet performed arena testing on the operationally representative warhead, which is fundamental to the development of the lethality model.

Performance

Effectiveness

Not enough data are yet available to evaluate the effectiveness of the Dark Eagle residual combat capability. Lethality testing to date has not provided direct evidence of the weapon's lethal effects against intended targets due to lack of operationally representative targets in sled and flight tests. Incorporating representative targets into the Joint Flight Campaign tests would provide both lethality and effectiveness data and support validation of weaponeering models.

Suitability

Not enough data are yet available to evaluate the Dark Eagle suitability of the residual combat capability.

Survivability

No data are currently available to evaluate the survivability of Dark Eagle in a contested environment. In coordination with the Navy, the Army intends to evaluate the survivability of Dark Eagle by M&S only increasing the risk to the survivability assessment unless the modeling and simulation tools are adequately verified, validated, and accredited.

Recommendations

The Army should consider the following recommendations as the program transitions to a program of record:

1. Develop a plan for effectively transitioning prototypes for production, fielding, operations, and sustainment under the Middle Tier Acquisition rapid fielding pathway to facilitate development of an adequate Dark Eagle T&E strategy.
2. Develop a T&E strategy that includes integrated testing, operational testing, live fire testing, and cybersecurity assessments to credibly demonstrate the required Dark Eagle effectiveness, suitability, lethality, and survivability.
3. Incorporate operationally representative targets and environments into Conventional Prompt Strike/Dark Eagle flight tests and other lethality and survivability tests.
4. Collaborate with the Navy to develop and execute the LFT&E strategy that adequately verifies and validates required M&S tools to create credible weaponeering and mission planning tools in support of the proposed operational fielding dates.

5. Collaborate with the Navy and Air Force to identify and leverage common practices, test corridors and infrastructure, test data, and M&S capability across the family of hypersonic weapon systems.

Electronic Warfare Planning and Management Tool (EWPMT)

The Electronic Warfare Planning and Management Tool (EWPMT) is a software application used by the Commander, Electronic Warfare Officers, and Electromagnetic Spectrum Managers to plan, coordinate, integrate, and synchronize Cyber Electromagnetic Activities (CEMA) from battalion to theater level. The Army intends for EWPMT to provide local and remote operational control and management of organic and assigned electronic warfare assets and integrate with the Terrestrial Layer System (TLS) and Multi-Function Electronic Warfare - Air Large (MFEW-AL) to execute electronic support and electronic attack. In FY21, the Army conducted an IOT&E in accordance with the DOT&E-approved test plan. In accordance with the EWPMT Security Classification Guide, the details on the EWPMT test adequacy and operational effectiveness, suitability and survivability are provided in the Controlled Unclassified Information edition of this report. The report assesses the ability of the operators to plan electronic warfare missions and provide situational awareness of the electromagnetic environment.

Major Contractor

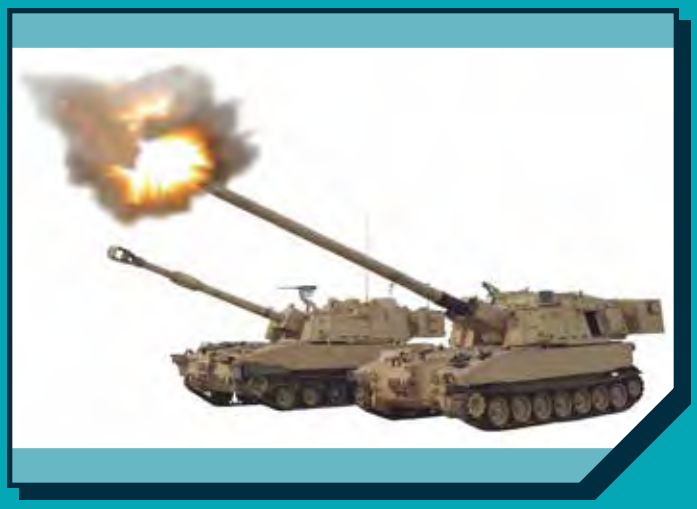
Raytheon Space and Airborne Systems – Fort Wayne, Indiana.

Recommendation

1. The Army should continue coordination with the MFEW-AL and TLS programs to demonstrate control and management of these systems during EWPMT's FOT&E.

Extended Range Cannon Artillery (ERCA)

The Extended Range Cannon Artillery (ERCA) is a Middle Tier of Acquisition program intended to integrate new cannon and projectile technologies with previously developed M109A7 artillery systems. Soldier Touchpoints with hardware, software, and ammunition sub-systems are planned to inform modifications to the current design. Early operational assessment is planned to inform the transition to a Major Defense Acquisition program at Milestone C.



System Description

The ERCA system is an upgraded self-propelled howitzer that leverages the base platform of the fielded M109A7 and includes a new cannon, breech assembly, and turret enhancements. The ERCA upgrades are intended to increase its lethal range.

Program

ERCA is Middle Tier of Acquisition program intended to integrate new cannon and projectile technologies with previously developed M109A7 artillery systems in an effort to reduce ERCA acquisition costs of building a new platform. The Program Executive Officer, Ground Combat Systems approved the Simplified Acquisition Master Plan in 2018. The test plan includes integrated testing of two Soldier Touchpoint events, an Operational Tempo event, and an Operational Demonstration/Soldier Touchpoint. The Army will use these test data to inform the transition to a Major Defense Acquisition program at Milestone C. The Army plans to execute an operational assessment after the Milestone C decision, which will be followed by IOT&E and LFT&E.

Major Contractor

To be determined. Defense Industrial Base for the prototype developmental efforts.

Test Adequacy

There have been no operational test or live fire activities in FY21. The Army is still developing the Operational Mode Summary/Mission Profile. The planned Soldier Touchpoints will be limited to scale soldier-led events in realistic operational environments executed without the full unit size and command and control architecture seen in full operational testing. Operational Tempo events will be civilian-led events conducted in an operational

manner to assess the system's ability to perform key capabilities. The subsequent Operational Demonstration will integrate soldier crews in an operationally realistic environment.

Performance

Effectiveness

The operational effectiveness of the ERCA system in providing timely and accurate artillery fires cannot yet be evaluated.

Suitability

The operational suitability of ERCA cannot yet be evaluated.

Survivability

The survivability of ERCA in contested environment, to include a cyber-contested environment, cannot yet be evaluated. Software upgrades, as well as space, weight, and power changes support the need to conduct both cyber security assessments and live fire testing. The ERCA LFT&E strategy will focus on new and modified components to the PIM program while leveraging previously captured PIM data when appropriate.

Recommendation

1. The Army should update the approved 2018 acquisition strategy for the upcoming program of record, to include an adequate ERCA T&E strategy that includes an operational assessment with soldiers, an initial operational test with soldiers using the Operational Mode Summary, an LFT&E strategy, and cybersecurity assessments.

Handheld Manpack and Small-Form Fit (HMS) Programs – Leader Radio and Manpack

Light infantry companies equipped with the Leader Radio and Manpack are not operationally effective when operating the voice and data network in dense vegetation, the primary area of operations. The system of systems that comprise the tactical network are not operationally suitable due to the increased logistics burden levied on the unit. The Leader Radio is vulnerable in a cyber-contested environment, while the Manpack is survivable against some cyber threats. Both are vulnerable in an electromagnetic spectrum-contested environment. In August 2021, the Army approved the full-rate production for the Leader Radio and Manpack.

System Description

The Handheld, Manpack, and Small Form Fit (HMS) program consists of the Leader and Manpack radios intended to equip infantry companies with a capability to send and receive voice and data to command and control the unit and execute the commander's intent. The Leader Radio is a two-channel, handheld, software-defined radio providing SECRET and CUI tactical voice and data communications. The Manpack is a two-channel, software-defined radio employed by general purpose radio users to operate two simultaneous waveforms. The Atom network management software configures the networks formed by the waveforms running on the Leader Radio and Manpack.

Program

The Leader Radio and Manpack are Acquisition Category IC programs under the Product Manager HMS and Program Executive Officer (PEO) Command Control Communications – Tactical (C3T). DOT&E approved the Leader Radio Test and Evaluation Master Plan (TEMP) and the Manpack TEMP in 2020. The Army approved the Leader Radio and Manpack for full-rate production in August 2021.

Major Contractors

- L3Harris Technologies – Melbourne, Florida.
- Collins Aerospace – Charlotte, North Carolina.
- Thales Group – Clarksburg, Maryland.

Test Adequacy

The Army conducted an IOT&E and an Adversarial Assessment (AA) of the HMS Leader Radio and Manpack at Fort Bragg, North Carolina to support the full-rate production decision. The IOT&E and AA were not conducted in accordance with the DOT&E-approved test plans. The HMS IOT&E was adequate to evaluate the operational effectiveness of the Leader Radio and Manpack but not reliability, availability, maintainability, training, and the ability of a unit to install the tactical network using Atom. The HMS IOT&E and AA were not adequate to address the cybersecurity of HMS radios against an outsider threat or the ability of the unit to prevent, mitigate, and recover from a cyberattack. The IOT&E and AA consisted of 21 force-on-force missions conducted over three, 72-hour scenarios. Additional details are provided in the HMS IOT&E report published in July 2021.

Performance

Effectiveness

Infantry companies equipped with the Leader Radio and Manpack are not operationally effective when operating the Tactical Scalable Mobile ad-hoc network (TSM) voice and data network provided by the HMS equipment. The TSM network demonstrated limited connectivity and range in dense vegetation, diminishing this operational capability. Platoons and squads may have more connectivity and use of TSM due to shorter range requirements. When connected, the TSM provided enhanced situational awareness by providing soldier position location information and clear voice communication. The radios' legacy communications worked well for company-level communications and reach-back to battalion for most missions.

The Leader Radio provided TSM at short ranges that did not meet distance requirements and had a battery life that did not support mission lengths. The Manpack also had TSM range limitations and short battery life but did provide Mobile User Objective System satellite communications that worked well. The HMS IOT&E report published in July 2021 details the ability of the unit to conduct their mission command using the HMS products as well as the performance of the individual systems. The Atom software was operationally effective for network management planning.

Suitability

The system of systems that comprise the tactical network are not operationally suitable due to the increased logistics burden levied on the unit. The dismounted infantry companies were not able to keep the Leader Radios, Manpacks, and conformal wearable batteries charged with their organic equipment. The Leader Radio did not integrate well into soldier combat equipment. Cables disconnected in vegetation, leading to battery disconnects and a loss of situational awareness. The Manpack was difficult to carry due to its weight, size, and heat. Signal soldiers scored Atom usability as marginal due to software immaturity, which the Army is working to correct. The HMS IOT&E did not provide adequate data to evaluate the reliability of the Leader Radio and Manpack.

Survivability

The survivability of the Leader Radio and the Manpack in a contested cyber and electromagnetic spectrum operational environments is detailed in the classified annex of the HMS IOT&E report published in July 2021.

Recommendations

The Army should:

1. Design a tactical network that prioritizes range for voice and position location information.
2. Develop a tactical power management plan.
3. Continue to improve integration with combat gear for both the Leader Radio and Manpack.
4. Conduct follow-on operational testing to evaluate the areas where the HMS IOT&E did not provide the data for an adequate evaluation of operational performance.

Infantry Squad Vehicle (ISV)

The Infantry Squad Vehicle (ISV) is operationally effective for employment as a troop carrier and can accomplish air assault missions in a permissive environment. The ISV is not operationally effective for employment in combat and engagement, security cooperation and deterrence (ESD) missions against a near-peer threat. The ISV is not operationally suitable because of poor developmental test reliability and deficiencies in training, maintenance, safety, and human system integration identified in IOT&E. The program has a corrective action plan to address failures identified in testing that should be verified prior to the full-rate production decision scheduled for May 2022.

An ISV-equipped unit is susceptible to enemy threats and actions but the ISV does not have a survivability requirement to protect the unit against kinetic threats defined in the Validated Online Lifecycle Threat report.

System Description

The ISV is designed to provide mobility on the battlefield for a nine-soldier light infantry squad with their associated equipment. The vehicle is required to be external and internal transportable by a CH-47F helicopter and airdropped by C-17 and C-130 aircraft. Airborne and air assault Brigade Combat Teams intend to employ the ISV during austere and offset entry operations to provide rapid cross-country mobility to conduct initial entry and offensive operations. Infantry Brigade Combat Teams require the ISV to conduct engagement, security, deterrence, and decisive action missions.

Program

The ISV is an Acquisition Category III program. The full-rate production decision is planned for May 2022 intended to support program objective of 649 vehicles.

Major Contractor

General Motors Defense – Detroit, Michigan.

Test Adequacy

DOT&E approved the ISV IOT&E operational test plan in July 2021. The Army Test and Evaluation Command conducted the IOT&E in August 2021 at Fort Bragg, North Carolina in accordance with the DOT&E-approved test plan.

The test unit did not complete 2 of 10 missions because the unit deployed to support a real world mission. Pilot test missions supplemented the evaluation. The Army will conduct an Airborne IOT&E Phase II operational test in 2QFY22.

Performance

Effectiveness

The ISV is operationally effective as a troop carrier for tactical transport. During IOT&E, a rifle company successfully employed ISVs over wooded and cross-country terrain to maneuver to their objectives and complete missions. The ISV is quiet, agile, and provides an enhanced off-road mobility capability for a nine-man infantry squad with their personal weapons and equipment. The ISV allows an infantry unit to move over extended distances rapidly, reducing fatigue.

Infantry Brigade Combat Teams equipped with the ISV demonstrated the ability to accomplish air assault missions in permissive environments. ISVs can be internally transported by CH-47F, and sling loaded with the UH-60 and CH-47F helicopters. The ISV is easy to rig, derig, and can rapidly move soldiers and equipment off the landing zone to support follow-on objectives. The ISV does not have ballistic armor, a major consideration for employment into non-secure locations, rendering the unit susceptible to threats at landing zones.

The ISV is not operationally effective for employment in combat and ESD missions against a near-peer threat, as identified in the Validated Online Lifecycle Threat report. The vehicle lacks the capability to deliver effective fires, provide reliable communication, and force protection. The rifle company equipped with the ISVs did not successfully avoid enemy detection, ambushes, and engagements during a majority of their missions. In order to traverse cross country routes and wooded terrain, the unit was forced to reduce their speed, resulting in slowed movement, or maneuvered on improved routes, negating any element of surprise. During missions, the unit experienced numerous casualties, delaying mission accomplishment and degrading its combat power for follow-on missions. The unit concealed their ISVs and drivers close to the objective and dismounted eight soldiers per vehicle to accomplish missions before recovering their ISVs. This action reduced their combat force, exposed the ISVs and drivers to opposing force attacks, and increased the risk of additional combat losses.

During missions, personal weapons were not easily accessible on the move, degrading the ability of the squad to quickly react to enemy actions and ambushes. While the ISV can mount a swing arm for an M240 machine gun, the ability for the soldier to efficiently employ the weapon on the move was a challenge because the soldier's field of fire was hindered by trees, foliage, and other obstructions when extending the swing mount. Protracting the swing mount also interfered with seated soldier egress from vehicle.

Communication between soldiers, squad leaders, and platoon leader were intermittent and not reliable on the move, degrading their ability to gain and maintain situational awareness at extended range mission between 62 to 300 miles. The ISV does not have a requirement for a mounted communication capability, so each platoon depended on their manpack and leader radios.

The ISV lacks the capability to carry the required mission equipment, supplies, and water for a unit to sustain itself within a 72-hour period. Units operating for longer durations will need to conduct mission planning, cross level-equipment across the unit, or may require additional ISVs to sustain operations.

Suitability

The ISV is not operationally suitable because of poor developmental test reliability and deficiencies in training, maintenance, safety, and human system integration identified in IOT&E. In developmental testing to date, the majority of failures were exposed in the rugged, hilly terrain of Yuma Proving Ground, Arizona. The program terminated the reliability testing because the ISV demonstrated Mean Miles Between Operational Mission Failure (MMBOMF)

was far below its required 1,200 MMBOMF. The major failures included loss of steering capability, cracked and bent seat frames, and engine cracks and overheating. The ISV was more reliable in the less challenging flat, wooded, terrain of Fort Bragg, North Carolina. The program has developed a corrective action plan to address failures in testing and verify fixes in FY22.

While ISV operator training was sufficient for the drivers to operate the vehicle, ISV maintainer training was limited due to incomplete maintenance manuals and training material. The program plans to provide contractor logistics support and improve maintainer manuals and training prior to transitioning to organic support in FY23. Because of the open design and handling characteristics of the ISV, additional training time is needed for drivers to operate the vehicle in a variety of terrain conditions, as well as night driving, and to prevent roll-overs. Unit leaders assessed collective training as lacking tactics, techniques, and procedures to employ the ISV in their combat formations. While soldiers performed diagnostic and maintenance tasks within their capability, most maintenance was performed by contractor field service representatives.

The ability of the soldier to egress from center and rear seated positions in the ISV was hindered by the limited space and interference from stored mission equipment during missions. The seating positions for the soldiers are cramped and uncomfortable. During IOT&E, over 60 percent of the soldiers expressed dissatisfaction with the ISV ride comfort. The vehicle rear seats contributed to lower back discomfort. When the company used the ISVs in wooded terrain, the ISV open design exposed soldiers to potential injuries from trees, branches, sticks, and other debris.

Survivability

An ISV-equipped unit is susceptible to enemy threats and actions. The ISV has some design features to reduce units' susceptibility to enemy detection, such as speed and small visual and aural signatures. The ISV does not have a survivability requirement to protect the unit against kinetic threats defined in the Validated Online Lifecycle Threat report. Units employing the ISV may need to consider integrating organic reconnaissance and firepower assets to enhance their survivability to threats.

The ISV is vulnerable in a cyber-contested environment through the commercial supply chain impacting the ability of a unit equipped with the ISV to accomplish its mission.

Recommendation

1. The Army should develop a plan to address recommendations identified in the ISV IOT&E report published in FY22 prior to the ISV full-rate production decision scheduled for May 2022.

Integrated Tactical Network (ITN)

The Army needs to overcome several challenges to demonstrate the operational effectiveness, suitability, and survivability of the Integrated Tactical Network (ITN). The Army should continue to develop and rapidly prototype the ITN to address problems identified in testing and conduct a Brigade-level exercise, in a contested environment, with a unit fully trained and equipped with the full complement of Capability Set (CS) 21 ITN equipment.

System Description

The ITN is an effort to rapidly prototype and field equipment to modernize Army tactical communications. The ITN is an integration effort that combines program of record (traditional acquisition) and commercial off-the-shelf systems to create network connections that add layers of data and voice capabilities to a Brigade. The ITN will field in four, two-year capability sets, starting with CS21. The Army plans for the ITN to change and evolve as new capabilities become available for future capability sets.

Program

The ITN is a Middle Tier of Acquisition program in the rapid prototyping and fielding phases. Starting in FY22, Product Line Capability Set Development will be the office of primary responsibility to integrate the systems identified by the Army's Network-Cross Functional Team into the ITN. The Army drafted a T&E strategy for CS21 in 2019, but did not submit it to DOT&E for approval. The ITN CS23 had a preliminary design review in April 2021 and plans to have a critical design review in 3QFY22. The T&E strategy for CS23 is in draft.

Major Contractors

- 4K Solutions: MBK – Midland, Georgia.
- GATR: T2C2 – Huntsville, Alabama.
- General Dynamics Mission Systems: TACDS – Fairfax, Virginia.
- Hoverfly Technologies Company: VHA – Orlando, Florida.
- Lockheed Martin: VHA – Bethesda, Maryland.
- FLIR Systems: VHA – Wilsonville, Oregon.
- KLAS Telecom: TRIK – Herndon, Virginia.

- Pacstar: Baseband Terminals – Portland, Oregon.
- PAR Government: WINTAK and ATAK software – Raleigh, North Carolina (U.S. Government-owned software).
- Samsung: EUD (Galaxy S7) – San Jose, California.
- Sierra Nevada Corporation Integrated Mission Systems: TRAX – Hagerstown, Maryland.
- Silvus: Streamcaster 4400, Streamcaster 4200 – Los Angeles, California.
- Tampa Microwave: Scout Terminals – Tampa, Florida.
- Trellisware: TW-950, TW-875 – San Diego, California.
- Verizon: Cellular plan for MBK – New York, New York.
- L3Harris Technologies: SFF 9820S – Melbourne, Florida.
- Thales Group: AN/PRC-170 – Clarksburg, Maryland.
- ViaSat: AN/PRC-161 – Carlsbad, California.

Test Adequacy

The Army intended to use a combination of test events to serve as the operational demonstration supporting rapid fielding. The CS21 T&E strategy planned for Soldier Touchpoint in January 2020 but real world events for the 1st Brigade/82nd Airborne Division (1/82) prevented the Army from conducting that event. The Army conducted a technical test in November 2020 and the Handheld, Manpack, and Small Form Fit IOT&E in January 2021. In March 2021, 1/82 conducted the Brigade Capstone event during a Joint Readiness Training Center rotation to demonstrate the CS21 ITN in an operationally realistic environment. The Capstone event did not have a DOT&E-approved test plan and did not provide adequate data to evaluate the use of the ITN at the Battalion or Brigade echelons. Several key pieces of equipment were not used in the Brigade exercise, precluding an assessment of their utility. The Army did not collect objective data during the Capstone to make up for the cancelled Soldier Touchpoint. Capstone data consisted of unit observations and surveys. The Army has not conducted an Adversarial Assessment or an assessment of the ITN in a contested electromagnetic spectrum environment. The Army is developing a T&E strategy to address these limitations.

Performance

Effectiveness

The Army needs to overcome several challenges to demonstrate ITN operational effectiveness and suitability. Brigade leaders indicated that having multiple communication paths provided redundancy they had not had previously but the battalions could not extend the Tactical Scalable Mobile ad-hoc network to the companies and brigade. This highlights the complexity of the ITN, as the Tactical Scalable Mobile network is not intended to extend from battalion to brigade. The ITN-equipped unit was not able to maintain the ITN equipment due to their lack of training and experience. The training of the ITN equipment was interrupted by real-world deployments and COVID-19 restrictions.

Suitability

In accordance with the ITN Security Classification Guide, additional details are provided in the Controlled Unclassified Information edition of this report.

Survivability

The survivability of the ITN in a cyber- and electromagnetic spectrum-contested environment cannot be assessed until the development and execution of an adequate T&E strategy.

Recommendations

The Army should:

1. Conduct a fully-trained Brigade level exercise in a contested environment, equipped with the full complement of CS21 ITN equipment.
2. Study the manpower needed to operate and maintain the ITN equipment.
3. Continue to develop and rapidly prototype the ITN to address identified problems.
4. Develop a T&E strategy for CS23 ITN designed to enable an assessment of operational effectiveness, operational suitability, and survivability.

Integrated Visual Augmentation System (IVAS)

The Integrated Visual Augmentation System (IVAS) prototyping effort demonstrated growth in capabilities with a first militarized design for Capability Set (CS) 3 and CS 4 but a few challenges remain to be addressed to demonstrate the IVAS operational effectiveness, suitability and survivability in combat. The Army should develop an adequate T&E strategy that quantifies improvements to CS 4 deficiencies prior to IOT&E and fielding.

System Description

The Army intends for the IVAS to increase close combat lethality by providing improved communication, mobility, situational awareness, and marksmanship. The IVAS includes a heads-up display (HUD), body-worn computer (puck), networked data radio, and three conformal batteries for each soldier. The IVAS HUD provides a see-through display and augmented reality capability with integrated thermal and low-light imaging sensors, a built-in compass for navigation, and Tactical Assault Kit situational awareness software. The Intra-Soldier Wireless provides Rapid Target Acquisition capabilities connecting the Family of Weapon Sights – Individual mounted on a soldier's weapon to the sight picture in the HUD. The IVAS radio enables all IVAS-equipped soldiers to pass data within the Company.

Program

IVAS is a Middle Tier of Acquisition program in the rapid prototyping and fielding phases intended to equip over 100,000 soldiers with the system, using an iterative approach of four Capability Sets. In December 2020, after the completion of CS 3 testing, the USD(A&S) approved the IVAS program to transition from rapid prototyping to rapid fielding, authorizing the Army to procure up to 10,000 CS 4 systems while also requiring that correction of problems noted during CS 3 testing be verified prior to IOT&E and CS 4 fielding. The Army employs the rapid prototyping effort to continue system development.

The Army split the IVAS CS 4 into two increments (CS 4a and CS 4b) and completed the testing of both increments in July 2021. The IVAS Program Manager has not yet developed an adequate T&E strategy that quantifies improvements to CS 4 deficiencies, a prerequisite for IOT&E and fielding.

Major Contractor

Microsoft – software development in Redmond, Washington and hardware developed in Mountain View, California.

Test Adequacy

Between October 2020 and November 2020, the Army conducted Soldier Touch Point (STP) 3 at Fort Pickett, Virginia with CS 3 to support the rapid fielding decision. Details are provided in the IVAS CS 3 Operational Assessment report published in March 2021. In April 2021, the Army conducted STP 4 at Fort Bragg, North Carolina with CS 4a prototypes. STP 4 included a 48-hour company mission scenario and multiple comparative events to compare performance of soldiers equipped with the IVAS to soldiers equipped with their current equipment. Following additional fixes, the Army demonstrated CS 4b in User Jury 4.3 at Fort Bragg, North Carolina in July 2021. The Army conducted a Cooperative Vulnerability and Penetration Assessment on hardened CS 4 systems at White Sands Missile Range, New Mexico in May 2021, followed by a developmental test with soldiers focused on discovering IVAS CS 4 cyber and electronic warfare vulnerabilities. CS 4 testing informed the Army decision about IVAS readiness for IOT&E.

Performance

Effectiveness and Suitability

To comply with the IVAS Security Classification Guide, the details of the IVAS operational effectiveness and suitability are provided in the Controlled Unclassified Information edition of this report. The report assesses the contribution of the IVAS CS 3 to navigation and mission planning and the ability of the IVAS-equipped units to distinguish enemy from friendly forces and reliably engage the enemy. It provides additional details on IVAS sensors and display, Rapid Target Acquisition integration, reliability, availability, human factors/comfort, field of vision, and user acceptance.

Survivability

The survivability of IVAS in cyber- and electromagnetic spectrum-contested environments will be assessed during the IOT&E.

Recommendations

The Army should:

1. Develop an adequate T&E strategy to quantify improvements to CS 4 deficiencies prior to IOT&E.
2. Continue to mitigate deficiencies identified in test.
3. In coordination with Microsoft, develop a reliability growth plan to continue to correct failure modes.
4. Complete a battery and power management plan to determine how soldiers will charge batteries to ensure adequate power to complete a 72-hour mission scenario.

Joint Air-to-Ground Missile (JAGM)

The Joint Air-to-Ground Missile (JAGM) is operationally effective, suitable, and lethal against a wide array of operationally representative targets when launched from the AH-64E Apache attack helicopter. To support the full-rate production decision in 3QFY22, the Navy needs to complete the second phase of operational testing intended to demonstrate JAGM operational effectiveness, suitability, and lethality as fired from the Marine's AH-1Z Viper attack helicopter.

System Description

JAGM is an air-to-ground, precision-guided missile with two new seekers that replicate and combine the capabilities of the existing laser-guided HELLFIRE Romeo and radar-guided Longbow HELLFIRE missiles. Army and Marine Corps commanders intend to employ the JAGM from helicopters 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.

Program

The JAGM is an Acquisition Category IC joint program led by the Army's Program Executive Office Missile and Space, Redstone Arsenal, Alabama. DOT&E approved the updated Test and Evaluation Master Plan on September 9, 2020. The Army completed IOT&E I in 3QFY20 but did not make a production decision due to a delay in IOT&E II required for the evaluation of the JAGM when launched from the Navy's threshold platform. The Navy is scheduled to complete IOT&E II in 1QFY22 to support a full-rate production decision in 3QFY22.

Major Contractor

Lockheed Martin Corporation, Missiles and Fire Control Division – Orlando, Florida.

Test Adequacy

The JAGM IOT&E I was adequate to assess operational effectiveness, suitability, and survivability of JAGM when launched from the AH-64E Apache attack helicopter, the Army's threshold platform. The Army Test and Evaluation Command conducted testing in accordance with a DOT&E-approved test plan. The IOT&E I included new equipment training, force-on-force missions, and live fire engagements.

LFT&E, conducted in accordance with DOT&E-approved test plans, was adequate to evaluate JAGM lethality against all required ground and maritime targets.

The JAGM IOT&E II, intended to assess JAGM performance when launched from the Marine's AH-1Z Viper attack helicopter, has been delayed due to platform software performance challenges. The Navy is continuing to address interoperability concerns and is scheduled to conduct IOT&E II in 1QFY22.

Performance

Effectiveness

The AH-64E Apache attack helicopter units firing the JAGM are operationally effective, exceeding required hit performance requirements against a wide array of operationally representative targets. The Army developed an effective and intuitive pilot-vehicle interface for aircrews. The flexibility of the JAGM's dual seeker provides aircrews a greater ability to adapt to the changing battlefield environment. The dual guidance capability mitigates the effects of battlefield obscurants such as smoke, dust, and foliage that limit the performance of legacy semi-active laser HELLFIRE missiles.

The Navy has not yet completed operational testing of the JAGM launched from the Marine's AH-1Z Viper attack helicopter, the Navy's threshold platform. There have been numerous software issues with the integration of the JAGM onto the AH-1Z's platform systems. The JAGM software has remained stable. The Navy believes integration faults are limited to the AH-1Z platform.

The JAGM demonstrated adequate lethality against heavy and light armor, structures, personnel in the open, maritime targets, and classified counterinsurgency targets. The height of burst is higher than expected when engaging personnel in the open and appears unrelated to surrounding objects or vehicles.

Suitability

The JAGM fired from the AH-64E Apache attack helicopter is operationally suitable, exceeding prelaunch and inflight reliability requirements. The Army continues to conduct reliability test engagements as part of their lot acceptance process. The Army has conducted environmental testing in a controlled chamber environment but has not completed live fire testing in an extreme cold weather environment, such as Alaska. Live fire testing in an Arctic environment may reveal reliability concerns that are masked in a static chamber test environment.

The program has completed some developmental and integrated testing on the AH-1Z. The Navy has not completed operational testing needed to verify the JAGM's operational suitability.

Survivability

The survivability assessment of JAGM against insider and nearsider cyber threats is available in the classified JAGM IOT&E report, published in August 2020. The Army has not assessed the JAGM's survivability against an outsider threat or the survivability of the JAGM's supply chain.

The Navy is scheduled to conduct additional cybersecurity testing in 2QFY22 to assess the survivability of the JAGM as integrated on the AH-1Z Viper. Cybersecurity test plans are in development and have not yet been submitted to DOT&E for review and approval.

Recommendations

The Army should:

1. Conduct cybersecurity testing to assess the survivability of the JAGM supply chain and potential vulnerabilities to an outsider threat.
2. Correct deficiencies with the height of the burst sensor and adjust tactics, techniques, and procedures to ensure lethality against personnel in the open.
3. Demonstrate JAGM effectiveness and lethality against emerging threats, including those with countermeasure systems.
4. Continue to improve reliability through lot acceptance and reliability testing.
5. Conduct missile flight testing in the Arctic to assess performance of sustained extreme cold temperatures.

Joint Assault Bridge (JAB)

The Joint Assault Bridge (JAB) is operationally effective and suitable, and designed to protect the crew against operationally relevant kinetic threat engagements. Some mission critical systems are vulnerable to direct and indirect fires, preventing the crew from launching and retrieving the bridge after such engagements. To mitigate these vulnerabilities, the Program Office implemented vehicle survivability upgrades that will be verified through testing. The Army entered the JAB full-rate production with an intent to retrofit all vehicles with these survivability upgrades, if proven effective.

System Description

The JAB is an M1A1 Abrams chassis-based, armored vehicle-launched, bridge system intended to provide Armored Brigade Combat Teams (ABCT) with a wet or dry gap-crossing capability to enable freedom of maneuver on the battlefield. The JAB replaces the M104 Wolverine and M48/M60 in the ABCT Brigade Engineer Battalions and Mobility Augmentation Companies. The JAB design, based on the M1A1 Abrams chassis with M1A2 heavy suspension, heavy assault scissor hydraulic bridge, and additional armor kits, intends to provide enhanced mobility, supportability, and crew survivability, as well as the use of common battlefield communication suites.

Program

The JAB is an Acquisition Category II program. The Army delegated the acquisition decision authority to the Program Executive Officer, Combat Support and Combat Service Support. The Army entered full-rate production in FY21.

Major Contractors

Leonardo DRS Technologies, Inc. – St. Louis, Missouri. Anniston Army Depot – Anniston, Alabama.

Test Adequacy

The Army conducted the second IOT&E at Fort Riley, Kansas from November 13-23, 2020 and the LFT&E at Aberdeen Test Center, Maryland from November 2017 through March 2018 in accordance with DOT&E-approved test plans.

To mitigate the vulnerabilities identified in LFT&E, the Army implemented survivability upgrades to the bridge launching mechanism and hydraulic power unit and will verify those through testing in accordance with the DOT&E- approved test plan.

Performance

Effectiveness

The JAB is operationally effective. Engineer units equipped with the JAB demonstrated the ability to provide ABCT wet or dry gap-crossing capability, supporting the accomplishment of doctrinal combat missions. JAB crews launched and retrieved bridges within the time requirements and kept pace with maneuver forces on roads and cross-country.

Suitability

The JAB is operationally suitable, demonstrating adequate availability to the maneuver commander for every planned operation. The JAB exceeded the mean cycles between operational mission failures requirement as well as the mean miles between operational mission failures requirement. On rough terrain, JAB crews had difficulty reconnecting the launcher tongue to the bridge.

Survivability

The JAB is designed to protect the crew from operationally relevant kinetic threat engagements. Some mission critical systems are vulnerable to kinetic threats preventing the crew from launching and retrieving the bridge after an engagement. The Program Office implemented vehicle survivability upgrades to mitigate some of those vulnerabilities. The effect of those upgrades on JAB survivability will be detailed in an update to the JAB IOT&E 2 and LFT&E report that was published in March 2021, after the Army completes the live fire verification testing.

The JAB is vulnerable in a cyber-contested environment. Specific vulnerabilities and their effect on mission accomplishment are described in the classified survivability annex of the JAB IOT&E 2 and LFT&E report published in March 2021.

Recommendations

The Army should:

1. Verify through testing that the JAB survivability design changes mitigate the identified vulnerabilities.
2. Improve JAB usability by developing a way to allow the launcher tongue to reconnect on rough ground.

Joint Light Tactical Vehicle (JLTV) Utility (UTL) and Fire Direction Center (FDC)

A field artillery unit equipped with the JLTV Fire Detection Center (FDC) with companion trailer and JLTV Utility (UTL) towing the M119A3 Howitzer can support fire support for a maneuver unit. During the developmental and operational testing (DT/OT), the JLTV FDC and UTL towing the Howitzer were reliable for the unit to accomplish fire missions. The JLTV UTL and FDC experienced suitability shortcomings in training, safety, and human factors. The program is developing a plan to address these challenges prior to fielding to artillery units. The program intends to re-compete the JLTV contract and make a production decision for the FDC Integration Kit and Howitzer interface in FY22.

System Description

The JLTV Family of Vehicles is the partial replacement for the High Mobility Multipurpose Wheeled Vehicle (HMMWV) fleet for the Army, Marine Corps, and Air Force. The Services intend for the JLTV to provide increased crew protection against improvised explosive devices and underbody attacks, improved mobility, and higher reliability than the HMMWV to support various military operations. The JLTV Family of Vehicles consists of the Combat Tactical Vehicle, with three mission package configurations (General Purpose Variant, Heavy Guns Carrier Variant, and Close Combat Weapon Carrier Variant) and the Combat Support Vehicle, with one mission package configuration (UTL Prime Mover Variant).

Program

The JLTV is an Acquisition Category IC program. The program is in full-rate production and fielding vehicles to Army, Marine Corps, and Air Force units. The program developed a JLTV FDC Integration Kit and an M119A3 Howitzer interface for the UTL variant in FY20. This engineering change proposal will allow artillery units to employ the UTL, in lieu of the HMMWV, as an FDC, the prime mover, and ammunition carrier for the towed M119A3 Howitzer. The program intends to make a production decision for the FDC Integration Kit and Howitzer interface in FY22.

Major Contractor

Oshkosh Corporation – Oshkosh, Wisconsin.

Test Adequacy

The Army Test and Evaluation Command executed the Fires DT/OT in August 2021 at Fort Campbell, Kentucky. The integrated testing was conducted in accordance with the DOT&E-approved test plan.

Performance

Effectiveness

A field artillery unit equipped with the JLTV FDC and JLTV UTL towing the M119A3 Howitzer can support fire support operations for a maneuver unit. During the DT/OT, the platoon used the JLTV FDC to perform tactical fire direction and employ the UTL to emplace the M119A3 to execute 75 fire missions. The JLTV demonstrated similar mobility as shown during the 2018 JLTV Multi-Service Operational Test and Evaluation. The vehicle provided good acceleration, enhanced off-road mobility for the platoon to successfully complete 31 tactical moves over 1,273 miles. The M119A3 Howitzer has less mobility than the JLTV UTL, resulting in the platoon reducing the operational tempo to prevent damage to their Howitzers.

During the DT/OT, the platoon employed the JLTV's adjustable suspension to lower the height of the vehicle to facilitate loading/unloading ammunition and reduce the egress height from the vehicle during emplacement. Adjusting the suspension was time-consuming, increasing emplacement and displacement times, and delaying movement. The platoon considered suspension adjustments during operations and modified their tactics, techniques, and procedures to account for the additional time. Delays in movement can affect the ability of an artillery unit to quickly react to changes in the tactical situation, and increase units' susceptibility to threats.

The JLTV UTL lacks sufficient storage for all mission equipment. The tarp and bow structure of the cargo cover does not have the capability to safely stow equipment on top of the cargo cover while moving. The platoon stored their camouflage nets and force protection equipment inside the cargo area of the JLTV, reducing the available space for other supplies and soldiers. This deficiency increased the time for the unit to erect camouflage netting and degraded the unit's ability to establish a security perimeter during the DT/OT.

The unit recommended the communication speakers be relocated to the rear of the JLTV UTL to improve audibility of firing commands and communication with the FDC. The JLTV UTL had sufficient ammunition carry capability and good ride quality. The tailgate had ample space for use as a ready rack for projectiles and fuses in preparation for firing.

Suitability

The JLTV FDC and JLTV UTL towing the Howitzer were reliable for the unit to accomplish fire missions during the DT/OT. The JLTV experienced one operational mission failure due to a fuel draw problem. The JLTV FDC and UTL demonstrated suitability shortcomings in training, safety, and human factors.

Based on soldier feedback, more hands-on time training is needed for emplacing and displacing the Howitzer with the JLTV UTL. Soldier egress from the rear of the JLTV ULT using the vehicle steps is a safety hazard because the steps failed to stay in the stowed position; the location of the steps made their use difficult and interfered with Howitzer's tow bar.

The location of the peer-to-peer communication speakers needs to be improved for soldiers to hear and understand information communicated from the crew in the cab to the rear of vehicle. The JLTV UTL provides poor visibility for the crew in the rear of vehicle to observe their surroundings and react quickly to tactical situation changes.

The cargo cover height of the JLTV trailer is low and lacks an opening in front for ease of access for erecting camouflage netting, loading/unloading cargo, and operating as a secondary FDC for chart operations.

Survivability

The JLTV survivability assessment in a contested kinetic threat environment is detailed in the 2018 classified LFT&E report. JLTV artillery units are vulnerable in a cyber-contested environment.

Recommendation

1. The Joint Program Office should develop a plan to address recommendations identified in the JLTV UTL and FDC Operational Assessment report published in December 2021, before the fielding of the JLTV to artillery units.

Long Range Fires

The Army continues to pursue the development of the Precision Strike Missile (PrSM) and advances to the Guided Multiple Launch Rocket System (GLMRS) to improve precision fires range and maneuverability, and enable a higher height-of-burst capability. Test planning is ongoing, precluding a preliminary evaluation of the performance of either system. To mitigate the risk to IOT&E and facilitate an adequate evaluation of the operational effectiveness of precision-guided missiles, the Army should continue exploring long-range flight corridors.

System Description

The long range precision fires modernization portfolio currently includes the PrSM and the GLMRS, both surface-to-surface missiles that will provide commanders with options in an all-weather, cluster-munition-compliant capability to attack critical and time-sensitive area and point targets. The PrSM will complement the current suite of GMLRS rockets and replace the Army Tactical Missile System. The GMLRS includes three fielded variants: Dual-Purpose Improved Conventional Munitions, Unitary, and Alternative Warhead (AW). Army units will fire the PrSM and ER-GMLRS rockets from the wheeled Ml42 High Mobility Artillery Rocket System and M270A2 launcher.

Program

The PrSM is a Pre-Major Defense Acquisition IB Program. The Army plans to field four increments of the PrSM missile, Increment 1 being the baseline capability. Future increments will focus on increasing range and engagement against additional targets of interest.

In June 2021, DOT&E approved the Milestone B Test and Evaluation Master Plan (TEMP) supporting the Milestone B decision on 27 September, 2021. The Army expects to have the production-representative missile design completed prior to Production Qualification Test flights. The Army plans to execute a Limited User Test to support an urgent materiel release decision and the fielding of an early operational capability, followed by IOT&E in support of a full materiel release.

The ER-GMLRS is an engineering change proposal to the GMLRS Unitary and AW rockets. DOT&E approved the ER-GMLRS TEMP Annex in August, 2020. The Army plans to conduct IOT&E in support of an engineering change proposal, full-rate production decision.

Major Contractor

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

Test Adequacy

In FY21, the PrSM program executed one engineering developmental test shot, while the ER-GLMRS conducted four. In June 2021, DOT&E approved the PrSM Milestone B TEMP with the following recommendations:

- The Army should execute a maximum range, sensor to shooter, surface-to-surface shot as soon as the DOD establishes a long-range flight corridor in the Continental United States to adequately evaluate the operational effectiveness and lethality of long range precision fires against operationally representative targets.
- With the exception of the maximum range shot, the Army should execute the operational test shots in the presence of operationally representative countermeasures using the most updated missile and firing platform software to evaluate the PrSM operational effectiveness and lethality in a contested environment.
- Given the anticipated software changes between limited user testing and IOT&E, and to ensure the Cooperative Vulnerability and Penetration Assessment (CVPA) adequately informs the Adversarial Assessment (AA), the Army should conduct both assessments in support of the limited user testing and IOT&E to enable early identification of any vulnerabilities, and to validate subsequent fixes prior to IOT&E and prior to fielding.

The ER-GMLRS TEMP Annex, approved by DOT&E in August 2020, includes live fire testing with ER GMLRS rockets and modeling and simulation considered adequate to evaluate the ER-GLMRS operational effectiveness and lethality. The TEMP does not include firing of the ER-GMLRS Unitary delay mode because the flight termination system, required when firing in the continental United States, does not fit in the Unitary missile configuration. While this remains a challenge, the Army is exploring firing a Unitary delay mode. The TEMP includes a cybersecurity assessment composed of a CVPA and an AA that will leverage a system of systems architecture, including the two launchers with the updated fire control system.

Performance

Effectiveness

The testing planning for both the PrSM and ER-GMLRS is ongoing, precluding the preliminary evaluation of their operational effectiveness at this time.

Suitability

The testing planning for both the PrSM and ER-GMLRS is ongoing, precluding the preliminary evaluation of their operational suitability at this time.

Survivability

The testing planning for both the PrSM and ER-GMLRS is ongoing, precluding the preliminary evaluation of their survivability in a non-permissive environment, to include a cyber-contested and a contested electromagnetic spectrum environment. The Army has not yet executed their plan to evaluate the PrSM in a contested/denied environment, nor have they yet completed the modeling and simulation runs to evaluate the survivability of the PrSM in a non-permissive kinetic threat environment.

Recommendations

The Army should:

1. Address the recommendations included in the PrSM Milestone B TEMP DOT&E approval memo.
2. Develop a plan to test the ER-GMLRS Unitary delay mode in an operationally realistic environment.
3. Synchronize the advanced field artillery tactical data system software releases and the development of the M270A2, as well as a new fire control system, to incorporate these platforms in the integrated operational testing.
4. Consider employing additional operationally representative countermeasures in integrated testing.

M917A3 Heavy Dump Truck (HDT)

The Army will employ the M917A3 Heavy Dump Truck (HDT) to construct and maintain air and ground supply lines. The Army completed live fire testing of the armored M917A3 in November 2020 and will issue a full material release for the armored and armor-capable variants in March 2023. The armored M917A3 HDT demonstrated the expected survivability against operationally relevant kinetic threat engagements. Additional details are summarized in a classified HDT LFT&E report published in September 2021.

System Description

The M917A3 HDT is a 22.5-ton capacity dump truck that will replace the M917 and F5070 HDTs, both of which are beyond their intended economic useful life. U.S. Army Horizontal Construction Companies, Equipment Support Platoons, Asphalt Teams, and Quarry Teams employ the M917A3 HDT throughout all operational theaters to construct and maintain air and ground supply lines by hauling, spreading, and dumping materials to build roads, landing strips, logistical facilities, helipads, parking areas, and motor pools. The M917A3 will be built in two variants: armor-capable and armored to protect the crew from kinetic threat-related accelerative injuries.

Program

The M917A3 is an Acquisition Category III program in the post Milestone C stage of the acquisition cycle. DOT&E approved the Test and Evaluation Master Plan in August 2020. The full material release decision is planned for March 2023.

Major Contractor

Mack Defense – Allentown, Pennsylvania.

Test Adequacy

The Army executed live fire testing of the armored M917A3 HDT from July 2019 to November 2020 at Aberdeen Test Center in Aberdeen, Maryland. Testing included: 1) armor coupon testing to determine how well the cab armor solutions protect the crew against penetrating bullets and fragments, 2) exploitation testing of the armored cab to determine if welds, seams, gaps between armor plates, and attachments to the armor introduced

vulnerabilities, 3) fuel tank fire suppression testing to assess the fuel tank fire suppression kit's ability to extinguish fuel tank fires initiated by side Improvised Explosive Devices (IEDs), and 4) full-up system-level testing to assess force protection from side and underbody IEDs and mines. Testing was adequate and conducted in accordance with DOT&E-approved test plans. DOT&E published a classified HDT LFT&E report in September 2021.

Performance

Survivability

The armored M917A3 HDT demonstrated the expected survivability against operationally relevant kinetic threat engagements. Additional details including threat descriptions and survivability performance can be found in the classified HDT LFT&E report. Specifically, the classified report assesses test adequacy, force protection, mission functionality, and recoverability of the armored M917A3 HDT when exposed to enemy forces.

Recommendation

1. The Army should consider the recommendations identified in the classified HDT LFT&E report to improve the HDT survivability, to include force protection against operationally relevant kinetic threat engagements.

Maneuver-Short Range Air Defense (M-SHORAD) Increment 1

The Maneuver-Short Range Air Defense (M-SHORAD) Increment 1 operational assessment, conducted from October – December 2020, highlighted several challenges the Army must address to demonstrate the operational effectiveness, suitability, and survivability of M-SHORAD Increment 1 in providing supported maneuver formation with short range air defense coverage. The Army fielded one platoon of M-SHORAD Increment 1vehicles as part of an Early Fielding.

System Description

The M-SHORAD Increment 1 integrates sensor and shooter capabilities onto a Stryker Infantry Carrier Double V-Hull A1 vehicle to defend supported maneuver elements against Group 3 unmanned aircraft systems, fixed wing, and rotary wing aircraft threats. The M-SHORAD Increment also integrates a Blue Force Tracker Situational Awareness systems and displays.

Program

The M-SHORAD Increment 1 is an urgent capability developed as an Army-directed requirement. The completion of the fielding of the first battalion of M-SHORAD Increment 1 will be used to establish an early operational capability. The Army plans to conduct an expeditionary operational assessment, which is currently not scoped to demonstrate M-SHORAD Increment 1 operational effectiveness, suitability, and survivability.

Major Contractors

- General Dynamics Land Systems – Warren, Michigan.
- Leonardo DRS – Arlington, Virginia.
- Moog – Elma, New York.

Test Adequacy

In October – December 2020, the Army conducted the M-SHORAD Increment 1 operational assessment a Cooperative Vulnerability and Penetration Assessment, and an Adversarial Assessment scoped to measure capability against the Army Chief of Staff's directed requirement, and not to determine operational effectiveness,

suitability and survivability. Neither the operational assessment nor the cybersecurity assessment were executed in accordance with the DOT&E approved test plan, partially due to the COVID-restriction-induced lack of a rotary wing target. COVID restrictions were coordinated with all stakeholders.

In December 2020, the Army completed the LFT&E in accordance with DOT&E-approved test plans. Testing was adequate to assess the survivability of the platform to kinetic threats, to include any force protection implications, and the lethality of the M-SHORAD Increment 1 kinetic effectors. Testing focused on the newly integrated mission equipment package, including missile suites and internal fire control components.

Performance

Effectiveness

The Army needs to overcome several challenges to demonstrate the operational effectiveness of the M-SHORAD Increment 1. The classified Initial M-SHORAD Operational Assessment report, published in August 2021, details the known performance of the onboard radar, the electro-optical/infrared sensors, the weapons systems, and the command and control software that allow soldiers to execute air defense missions. The report also includes specifics on detection, tracking, classification, identification, and probability of kill against the required threats.

Suitability

The Army needs to overcome several challenges to demonstrate the operational suitability of the M-SHORAD Increment 1. Additional details are offered in the classified Initial M-SHORAD Operational Assessment report, published in August 2021.

Survivability

The Army needs to overcome several challenges to demonstrate M-SHORAD Increment 1 survivability in a contested environment. The Army has not yet tested the survivability of the M-SHORAD Increment 1 in a contested electromagnetic spectrum environment. While the cybersecurity testing was limited in scope, it yielded valuable information to improve the system. Additional details are offered in the classified Initial M-SHORAD Operational Assessment report, published in August 2021.

Recommendations

The Army should:

1. Address M-SHORAD Increment 1 deficiencies identified during the operational assessment documented in the classified Initial M-SHORAD Increment 1 Operational Assessment report.
2. Revise the scope of the scheduled expeditionary operational assessment to support an adequate assessment of M-SHORAD Increment 1 operational effectiveness, suitability, and survivability in an operationally representative environment, with countermeasures and accredited threat target representation.

Mobile Protected Firepower

Limited User Test (LUT) and LFT&E data analyses are ongoing, precluding an evaluation of Mobile Protected Firepower (MPF) risk to meeting operational effectiveness, suitability, and survivability requirements. The Army will use the LUT and LFT&E data to select either BAE or General Dynamics Land Systems as the major contractor for the MPF program in support of a low-rate initial production scheduled for 3QFY22. At that time, the program will transition from the Middle Tier of Acquisition phase to an Acquisition Category IB program, with the Milestone C decision scheduled for 3QFY22.

System Description

The MPF is an armored track vehicle with a 105mm main gun that provides the Infantry Brigade Combat Team (IBCT) with a mobile, protected, direct fire capability against light armored vehicles, hardened enemy fortifications, and dismounted personnel. The MPF will be able to fire a broad spectrum of currently fielded munitions that can achieve lethal effects against a variety of targets in support of IBCT missions. The MPF design includes armor, smoke grenade launchers, blow off panels, and automatic fire suppression intended to enhance survivability against direct/indirect fire, rocket-propelled grenades, and underbody threats.

Program

MPF was originally designated as an Acquisition Category IB program intended to enter the acquisition life cycle at Milestone B, but in September 2018, the Army Acquisition Executive approved MPF as a Middle Tier of Acquisition program. DOT&E approved a Milestone B Test and Evaluation Master Plan (TEMP) in August 2019. The competition for the Middle Tier of Acquisition phase of the MPF includes two vendors: BAE Systems and General Dynamics Land Systems. The Army will select one of the two vendors during a Source Selection Evaluation Board convening in 1QFY22 to support low-rate initial production. The program is developing the MPF Milestone C TEMP to describe the T&E activities for the production and deployment phase in support of the Army Acquisition Executive's Milestone C decision scheduled for 3QFY22.

Major Contractors

BAE Systems – Sterling Heights, Michigan. General Dynamics Land Systems – Sterling Heights, Michigan.

Test Adequacy

As part of the Middle Tier of Acquisition phase of the program, the Army Test and Evaluation Command conducted a two-phase LUT utilizing prototypes focusing on gunnery and maneuver. Testing was conducted from September through November 2021 in accordance with a DOT&E-approved test plan. Prior to the LUT, the Army conducted a Soldier Touchpoint event to collect early user feedback and familiarize the crew with prototype vehicles.

The Army completed LFT&E for both vendors in September 2021. Testing was adequate and conducted in accordance with the DOT&E-approved Milestone B TEMP and test plans. LFT&E included armor exploitation and ballistic hull and turret testing to inform vendor down-select, and provide early identification of potential survivability improvements prior to Milestone C.

Performance

The LUT and LFT&E data analyses are ongoing, precluding an evaluation of the MPF's preliminary operational effectiveness, suitability, and survivability. Details will be provided in the MPF Operational Assessment report expected to be published in support of a low-rate production decision in 3QFY22.

Recommendation

1. Recommendations will be detailed in the MPF Operational Assessment report in 3QFY22 after the completion of the LUT and LFT&E data analyses.

Multi-Function Electronic Warfare – Air Large

The Multi-Function Electronic Warfare – Air Large (MFEW–AL) program did not execute the operational testing needed to meet its acquisition requirements. The lack of program maturity and operational testing precludes a preliminary assessment of MFEW-AL operational effectiveness, suitability and survivability.

System Description

The MFEW-AL is an airborne electronic warfare payload, which will be mounted onto the MQ-1C Group IV Gray Eagle Unmanned Aircraft Systems to provide the Army Battlefield Commander with electronic attack and electronic warfare support capability. The MFEW-AL is part of a larger electronic warfare framework, which includes the Electronic Warfare Planning and Management Tool (EWPMT), to build a common operating picture of the electromagnetic operating environment. The MFEW-AL is designed to detect, identify, locate, deny, disrupt, and degrade enemy communications and non-communications (radars) in support of Multi-Domain Operations.

Program

The MFEW-AL is an Acquisition Category III program. The Army Program Executive Office Intelligence, Electronic Warfare, and Sensors is the milestone decision authority. The MFEW-AL budget has been reduced multiple times and is unfunded in the Army's FY22 Base Budget, submitted in May 2021.

The Army allowed the MFEW-AL program to advance through its acquisition cycle without conducting operational testing.

Major Contractor

Lockheed Martin Systems Integration – Owego, New York.

Test Adequacy

The MFEW-AL Program Office is utilizing a Simplified Acquisition Management Plan with an included T&E strategy as its primary program management document. The Army is continuing to develop the system's engineering plan and design of experiment for the MFEW-AL, but the Simplified Acquisition Management Plan has not yet been submitted to DOT&E to determine the adequacy of its T&E strategy.

The developmental and integrated testing required to mount the MFEW-AL on a field representative MQ-1C Gray Eagle has been delayed due to inconsistent funding, limiting the ability to proceed to operational testing. The program uses surrogate platforms, to include the UV-18A "Twin Otter" and a special use MQ-1C Gray Eagle, to continue developmental testing.

The MFEW-AL Program Office continues to look for opportunities to participate as an enabler in Multi-Domain Operations environment test events to reduce costs. In May 2021, the MFEW-AL participated in an exercise supporting an Infantry Brigade Combat Team operating in a simulated Multi-Domain Operations environment. This approach reduces testing cost but limits the number of accomplished test objectives because the MFEW-AL is not the focus of the testing. The MFEW-AL is currently using a surrogate ground station for developmental testing and is expected to use the EWPMT in IOT&E scheduled for FY24.

Performance

Effectiveness

The lack of program maturity and operational testing precludes a preliminary assessment of MFEW-AL operational effectiveness. The Infantry Brigade Combat Team demonstrated the capability to conduct limited electronic attack and electronic warfare support in a controlled test environment. While the preliminary testing has demonstrated some capabilities that support program requirements, the gathered data lack the operational relevance to support an assessment. For example, Soldier Touch Points, intended to assess the utility of MFEW-AL information to the ground forces, have been limited to electronic warfare officers and have not yet included the Army's MQ-1C community. In addition, tactics, techniques, and procedures have not yet been developed to ensure the MFEW-AL is operated in a profile that supports mission success.

Suitability

The lack of program maturity and operational testing precludes a preliminary assessment of MFEW-AL operational suitability. The prototype MFEW-AL design includes known reliability concerns. The lack of an EWMPT increased the user workload to analyze and produce operational relevant information from the MFEW-AL.

Survivability

The lack of program maturity and operational testing precludes a preliminary assessment of MFEW-AL survivability in a cyber- and electromagnetic spectrum-contested environment.

Recommendations

The Army should:

1. Determine funding requirements to complete the integrated testing required to prepare for operational testing.
2. Submit a Simplified Acquisition Management Plan to DOT&E for review and approval of its T&E strategy.
3. Identify the user community for the MFEW-AL system to ensure Soldier Touch Points and feedback are comprehensive.
4. Coordinate with the Army's Unmanned Aircraft System community to ensure tactics, techniques, and procedures are developed to support operational employment of the MFEW-AL.

.

RQ-7Bv2 Block III SHADOW – Tactical Unmanned Aircraft System

Units equipped with the RQ-7Bv2 Shadow Block III are operationally effective, demonstrating ability to acquire targets at greater distances and accuracy than Shadow Block I operators. The Shadow Block III is operationally suitable, demonstrating significant improvement in mean time between system abort as compared to the Shadow Block I. The Army began fielding RQ-7Bv2 Shadow Block III in September 2021.

System Description

The RQ-7Bv2 Shadow Block III is an upgrade to the RQ-7 Shadow Tactical Unmanned Aircraft Systems intended to provide commanders with increased situational awareness, improved wide-area target acquisition, and high-value target tracking to shape the operational environment. The Shadow Block III will replace 184 of 440 Shadow Block I aircraft in Shadow formations.

Program

The RQ-7Bv2 Shadow Block III is an Acquisition Category IC program. The Army Acquisition Executive is the milestone decision authority. DOT&E approved the Test and Evaluation Master Plan, which included a fielding update, on September 9, 2020. The Army completed an FOT&E and an Adversarial Assessment in 1QFY21 to support a materiel release decision in November 2021.

Major Contractors

- Unmanned Aerial System: Textron Systems – Hunt Valley, Maryland.
- Sensor Payload: L3 Harris WESCAM – Burlington, Ontario, Canada.
- Engine: UAV Engines Limited – Lichfield, England, United Kingdom.

Test Adequacy

The RQ-7Bv2 Shadow Block III FOT&E was adequate to assess operational effectiveness, suitability, and survivability in support of a materiel release decision in November 2021. The Army Test and Evaluation Command conducted testing in accordance with a DOT&E-approved test plan. The FOT&E included new equipment

training, force-on-force missions, manned-unmanned teaming (MUMT), HELLFIRE live missile engagement missions with AH-64D and AH-64E attack helicopters, and an Adversarial Assessment.

Performance

Effectiveness

Units equipped with the Shadow Block III are operationally effective. Shadow Block III operators can acquire targets at greater distances and accuracy than Shadow Block I operators. Shadow Block III target location errors are acceptable at all operational ranges. The Shadow Block III can perform MUMT with the AH-64D and AH-64E up to the ability for Apache aircrews to take control of Shadow Block III remotely. MUMT increases the survivability and lethality of Apache aircrews and the operational effectiveness of RQ-7.

The Army has not updated Shadow tactics that capitalize on the improved capabilities of the Shadow Block III. Lack of innovative tactics led the test unit to operate the Shadow Block III in the same manner as the Shadow Block I, reducing the effectiveness of the Shadow Block III. The Shadow Block III also has a higher fuel consumption rate than the Shadow Block I, which may reduce available support to commanders and increase required Shadow platoon maintenance.

Suitability

The Shadow Block III is operationally suitable, and demonstrated a mean time between system aborts of 20.0 hours, meeting its requirement of 20 hours. This is a significant improvement (130 percent increase) from the Shadow Block I mean time between system aborts of 8.7 hours during operational testing. The Shadow Block III demonstrated a mean time between essential function failure of 4.8 hours, equal to Shadow Block I. The Shadow Electro-optical Infrared Laser Designator payload demonstrated a mean time between payload system abort of 130.1, meeting its 110-hour requirement.

The Shadow Block III engines were a recurring problem, with the test unit replacing six engines during FOT&E. Engine problems included excessive sputter prior to launch, oil leaks, coolant leaks, and throttle issues. The Shadow Block III maintenance concept emphasizes engine replacement over repair, with engines returning to the English manufacturer for repair. This concept may not support sustained combat operations.

The Shadow Block III New Equipment Training was suitable in preparing operators and maintainers. More hands-on training and additional instructors could further improve unit training. MUMT workload was minimal for Shadow operators but excessive (rated as not possible) for AH-64E aircrews under some conditions.

Survivability

The Shadow Block III is vulnerable in a cyber-contested environment and in a contested electromagnetic spectrum environment. Shadow Block III is susceptible to visual and audio ground detection making it vulnerable to certain kinetic threat engagements. The effect of those vulnerabilities on the Shadow Block III survivability and residual mission capability is detailed in the classified annex of the RQ-7Bv2 Block III Shadow FOT&E II report published in May 2021.

Recommendations

The Army should:

1. Determine the cause of target location errors, even though they are acceptable at all operational ranges, to further improve the operators' understanding and confidence in the Shadow Block III's capabilities.
2. Address the operational effects of the Block III reduced on-station time due to higher fuel consumption to improve Shadow Block III availability to commanders.
3. Isolate the cause of engine sputtering observed during testing and determine an effective mitigation to avoid mission delays.
4. Evaluate the Shadow Block III maintenance concept and assess feasible repairs for maintenance personnel.
5. Develop, codify, and update TTPs in the Shadow aircrew training manual to include tasks that include mitigating the effects of electronic warfare, execution of MUMT operations, and effective use of the Shadow Block III's improvements.

6. Revise New Equipment Training to allow for more hands-on experience and increase equipment quantities and availability during such training to improve Shadow Block III units readiness following the training.

Soldier Protection System (SPS)

The Army started early fielding of the Second Generation Modular Scalable Vest (MSV Gen II) and Third Generation Vital Torso Protection (VTP Gen III) hard armor plates in 4QFY21 to a select number of soldiers. Eight of the thirteen VTP Gen III designs passed First Article Testing, proceeding to the next phase of live fire testing that is currently ongoing. The Army intends to field VTP Gen III systems to the broader Army starting in 4QFY22 through 4QFY25 after the completion of testing. The Next Generation Integrated Head Protection System (IHPS) is under development, with First Article Testing planned for 3QFY22.

System Description

The SPS is a suite of personal protection subsystems intended to, at a reduced weight, provide equal or increased levels of protection against small-arms and fragmenting threats compared to existing personal protection equipment. The SPS subsystems are designed to protect a soldier's head, eyes, and neck region; the vital torso and upper torso areas (including the extremities); and the pelvic region. The SPS is a modular system and provides soldiers the capability to configure the various components into different tiers of protection depending on the threat and the mission. The SPS consists of three major subsystems, shown in Figure 1.

Program

The SPS program is an Acquisition Category III program comprised of three major subsystems depicted in Figure 1. Each of the three major subsystems are developed, tested, and fielded independently. The Army entered the TEP full-rate production in September 2016, the IHPS in October 2018, and the VTP in December 2019. Each subsystem has follow-on engineering change proposal efforts: MSV Gen II is replacing the initial MSV in TEP; VTP Gen III is replacing previous generations of VTP; and the Next Generation IHPS is replacing the IHPS. The Army is not planning a formal acquisition decision for the VTP Gen III, despite the significant design changes from VTP Gen II. The Army started an early fielding of MSV Gen II and VTP Gen III plates in 4QFY21 to a select number of soldiers as authorized by the Army G8 on February 16, 2021.

Major Contractors

- TEP Full-Rate Production Vendors/Designs (multiple vendors to stimulate competition and achieve best price through Fair Opportunity awards):
  - Armor Express – Eden, North Carolina (MSV, BPP).
  - Bethel Industries Inc. – Jersey City, New Jersey (MSV, BPP).

- Slate Solutions – Sunrise, Florida (MSV).
- Point Blank Enterprises, Inc. (Protective Apparel & Uniform) – Pompano Beach, Florida (BCS).
- Carter Enterprises Industries Inc. – Brooklyn, New York (BCS).
- Eagle Industries Unlimited – Virginia Beach, Virginia (BCS).

- VTP Full-Rate Production Vendors:
  - Engense Armor Systems – Camarillo, California (ESBI).
  - Florida Armor Group – Miami Lakes, Florida (ESBI).
  - Leading Technology Composites – Wichita, Kansas (ESAPI, ESBI).
  - TenCate Armor – Hebron, Ohio (ESAPI, XSBI).
  - Avon Protection/Ceradyne – Irvine, California (XSAPI, ESAPI, XSBI).
- IHPS Vendor:
  - Avon Protection /Ceradyne – Irvine, California.
- NG IHPS Vendor:
  - Avon Protection /Ceradyne – Salem, New Hampshire.
  - Gentex Corporation – Carbondale, Pennsylvania.

Test Adequacy

The Army is currently executing Lot Acceptance Testing on the eight VTP Gen III plates that have passed First Article Testing. The Army completed First Article Testing on a production of a single XXL size of the IHPS in 2QFY21. Both test series were conducted at Aberdeen Test Center, Maryland in accordance with DOT&E-approved test plans. Test planning for Next Generation IHPS is ongoing and scheduled to begin in 3QFY22. The Army plans to complete additional testing in 1QFY21 to enable the comparison of legacy VTP and SPS VTP Gen III plates against nonstandard threats.

The Army's ballistic testing of the VTP Gen III plates is being performed in accordance with the DOT&E-approved strategy but does not include an assessment of potential injuries to soldiers wearing body armor. In order to adequately assess soldier protection in the future, the Army must accredit the available mannequins for evaluating injuries and fully verify, validate, and accredit the Army's modeling and simulation tools to accurately evaluate VTP as a penetrable material.

Figure 1. Soldier Protection Subsystems

Performance

Five of the thirteen VTP Gen III designs (a combination of ESAPI, ESBI, XSAPI, and XSBI designs) did not meet the ballistic First Article Testing requirements. Final assessments of the VTP performance will be published after the completion of testing in 2QFY22 to inform the SPS fielding decision to the broader Army in 4QFY22. This assessment will include a comparison between the legacy VTP and VTP Gen III performance.

The XXL IHPS design submitted for First Article Testing in FY21 met its ballistic requirements.

Recommendations

The Army should:

1. Improve modeling and simulation capabilities so that penetration, threat breakup, and fragment behavior can be assessed on ceramic hard armor plates for a range of conditions not tested.
2. Reinitiate their efforts to accredit a mannequin as an evaluation tool for assessing injuries from penetrating threats in body armor testing.

Stryker Family of Vehicles (FoV)

The Army conducted a FOT&E between May and June 2021 to support a Stryker Common Remotely Operated Weapon Station – Javelin (CROWS-J) fielding decision. While testing was adequate to evaluate the crews' ability to identify and engage targets using the improved CROWS-J sights, crew-served weapons, and Javelin missiles, the Army must address several shortfalls to improve Stryker CROWS-J operational effectiveness, suitability, and survivability.

Stryker Common Remotely Operated Weapon Station - Javelin (CROWS-J)
Stryker 30mm Medium Caliber Weapon System (MCWS)

System Description

The CROWS-J and the 30mm Medium Caliber Weapon System (MCWS) are lethality upgrades to the existing Stryker FoV. The Army intends for the CROWS-J to address the obsolescence of the Fire Control Unit, replace the current Remote Weapons System, enable remote firing of a Javelin missile, improve Thermal Imaging Module optics, and integrate smoke grenade launchers. The 30mm MCWS integrates the XM813 cannon (30x173mm) onto a Stryker Double V Hull, equipped with a primary day/night optic intended to enable lethal effects against targets at a range of 3,500 meters while maintaining comparable mobility characteristics of the baseline vehicle.

Program

The Stryker FoV, including its lethality upgrades, is an Acquisition Category IC program. DOT&E approved the Test and Evaluation Master Plan annexes for the CROWS-J in September 2019 and 30mm MCWS in June 2021.

The Army intends to field the CROWS-J under an Urgent Material Release, and continue fielding subsequent brigades under a Conditional Material Release.

The Army executed a multi-vendor competition from August-December 2020 to select a design solution for the 30mm MCWS. The Army intends to begin fielding the First Unit Equipped (1-2 ID) under a Conditional Material Release followed by an execution of FOT&E.

Major Contractors

- CROWS-J:
  - Kongsberg Protech Systems – Kongsberg, Norway; Johnstown, Pennsylvania (Primary System).
  - Raytheon & Lockheed Martin – Tucson, Arizona (Components).

- General Dynamics Land Systems – Sterling Heights, Michigan; Anniston, Alabama (Integrator).
- 30mm MCWS:
  - Oshkosh Defense, LLC – Oshkosh, Wisconsin.

Test Adequacy

The Army conducted a FOT&E between May and June 2021 to support a CROWS-J fielding decision. The Army conducted the FOT&E in accordance with the DOT&E-approved test plan.

Testing was adequate to evaluate the crews' ability to identify and engage targets using the improved CROWS-J sights, crew-served weapons, and Javelin missiles. Crews completed standard qualification gunnery, fired 12 live and 12 simulated Javelin missiles, and conducted target identification against threat and friendly vehicles.

In June 2021, the Army completed CROWS-J live fire testing in accordance with DOT&E-approved test plans. Testing, conducted on a non-functional ballistic hull asset, was adequate to evaluate force protection during a kinetic threat engagement, including direct and indirect hits to the externally stowed Javelin missiles.

The Army Test and Evaluation Command conducted a Cooperative Vulnerability and Penetration Assessment and Adversarial Assessment from June 7-24, 2021 at Aberdeen Proving Ground, Maryland in accordance with the DOT&E-approved test plans.

Details on CROWS-J operational effectiveness and suitability are available in the DOT&E unclassified CROWS-J FOT&E report published in November 2021. The classified annex to the CROWS-J FOT&E report details the assessment of the CROWS-J survivability in a contested environment.

Performance

In accordance with the Stryker Security Classification Guide, the assessment of the Stryker operational effectiveness and suitability is detailed in the Controlled Unclassified Information edition of this report and the CROWS-J FOT&E report published in November 2021. The report details an assessment of the ability of the Stryker unit equipped with the CROWS-J to identify and engage targets, and evaluates the probability of target identification requirement. The report also includes an assessment of reliability, operational availability and New Equipment Training.

Recommendations

The Army should:

1. Address the CROWS-J recommendations documented in the CROWS-J FOT&E report published in November 2021.
2. Consider full integration of the CROWS-J evaluation into the 30mm MCWS FOT&E in 3QFY23 to fully evaluate CROWS-J operational effectiveness, suitability, and survivability.

Navy Programs

Advanced Anti-Radiation Guided Missile - Extended Range (AARGM-ER)

The Navy conducted the first Advanced Anti-Radiation Guided Missile – Extended Range (AARGM-ER) developmental free flight test from an F/A-18 in July 2021 and completed mission planning and munition handling demonstrations. The AARGM-ER IOT&E is scheduled to begin in FY23.

System Description

The AGM-88G AARGM-ER is an air-to-ground missile designed to be employed by the F/A-18, E/A-18G, and F-35 to passively detect and guide on radio frequency emissions from a radar site and then transition to an active millimeter wave terminal radar to detect, track, degrade, and destroy radio frequency-enabled, surface-to-air missile systems. AARGM-ER reuses the same millimeter wave radar as AARGM, and introduces a larger diameter but shorter rocket motor for increased range, F-35A and F-35C internal weapons bay fitment, and a new warhead.

Program

AARGM-ER is an Acquisition Category IB program. DOT&E approved the AARGM-ER Milestone C Test and Evaluation Master Plan (TEMP) in May 2021. The Navy committed to submitting a cybersecurity test strategy for DOT&E approval no later than June 2022. The Navy held a Knowledge Point-4 program review in July 2021 that supported entry into the Production and Deployment phase and the award of the low-rate initial production (LRIP) contract. Though the Navy has deviated from the schedule, approved in the May 2021 TEMP, the program intends to complete the test events described in the TEMP.

Major Contractor

Northrop Grumman Defense Systems – Northridge, California.

Test Adequacy

The Navy conducted the first AARGM-ER developmental free flight from an F/A-18 in July 2021 to demonstrate the AARGM-ER threshold range requirement. The Navy also completed mission planning and munition handling demonstrations. Production-representative hardware and software are not scheduled to be available until the final developmental free-flight test. The integrated testing should provide enough data to validate the modeling and simulation using the production-representative configuration and gain confidence in the final missile configuration prior to dedicated operational test.

Performance

Not enough data are currently available to provide a preliminary assessment of AARGM-ER operational effectiveness, suitability, or survivability. Mission planning and munitions handling demonstrations to date have provided limited data, with no noted performance issues. In accordance with the AARGM-ER Security Classification Guide, additional details are included in the Controlled Unclassified Information edition of this report.

Recommendation

1. The Program Office should address the recommendation included in the Controlled Unclassified Information edition of this report.

Aegis Modernization Program

In August 2021, the Navy conducted three live Evolved Sea Sparrow Missile (ESSM) Block 2 fire events against adversary anti-ship cruise missile surrogates using the Baseline 9.2.2 variant of the Aegis Combat System's Advanced Capability Build 16 (ACB 16). Preliminary evaluation of Baseline 9.2.2 testing suggests anti-air and anti-surface warfare performance is consistent with legacy Aegis capability. While the Navy expects to complete the ACB 16 testing on all delivered Baseline 9.2 variants in FY23, the assessment of ACB 16 operational effectiveness and suitability is at risk due to a lack of an approved Test and Evaluation Master Plan (TEMP). Additionally, the Navy has yet to conduct any operational testing on Baseline 9.2.1.

System Description

The Aegis Combat System is an advanced weapon control system comprised of sensors, control elements, and weapons to detect, track, engage, and destroy adversary targets. The Aegis Combat System key components include: 1) an Aegis Weapon System that includes the AN/SPY-1 three-dimensional multi-function radar, 2) a Phalanx Close-In Weapon System, 3) a 5-inch diameter gun system, 4) the Vertical Launch System that can launch Tomahawk missiles, Standard Missiles-2, -3, and -6, ESSMs, and Vertical Launch Anti-Submarine Rockets, and 5) an AN/SQQ-89 undersea warfare suite, which includes the MH-60R helicopter. The Navy's Aegis Modernization Program updates the Aegis Weapon System to improve Aegis Combat System integration and capabilities on CG 47-class Aegis guided missile cruisers and DDG 51-class Aegis guided missile destroyers to advance their support to anti-air warfare in self-defense and defense of carrier strike groups or expeditionary strike groups, anti-surface warfare, anti-submarine warfare, strike warfare, and integrated air and missile defense.

Program

The Aegis Modernization Program is not an acquisition program. The Navy has updated Aegis through quadrennial ACBs that comprise hardware and software modifications to improve capability. The latest upgrade is the ACB 16. The Navy intends four incremental deliveries within ACB 16: Baseline 9.2.0, Baseline 9.2.1, Baseline 9.2.2, and Capability Package 22-1. The evaluation of ACB 16 will be accomplished as a cumulative collection of operational test data from all baseline variants, with completion expected in FY23. The ACB 16 evaluation will inform deployment decisions and determine delivered capability for ACB 16 and its variants.

The Navy developed an Aegis TEMP revision in FY19 in coordination with DOT&E, which included the test strategy for the first three ACB 16 baselines, but the Navy never provided it for DOT&E approval. The Navy now intends to incorporate an additional phase of development, Capability Package 22-1 (previously referred to as Baseline 9.2.3), into the TEMP revision for DOT&E approval.

The Navy intends to deliver initial capability of the next Aegis ACB, ACB 20, in FY24 in coordination with the DDG 51 Flight III ship's IOT&E. Operational testing of ACB 20 will continue until at least FY27 due to the lack of availability to test some capabilities, including integrated air and missile defense.

Major Contractors

- General Dynamics Marine Systems Bath Iron Works – Bath, Maine.
- Huntington Ingalls Industries – Pascagoula, Mississippi.
- Lockheed Martin Rotary Mission Systems – Moorestown, New Jersey.
- Raytheon Missiles and Defense – Marlborough, Massachusetts.

Test Adequacy

In August 2021, the Navy conducted three live ESSM Block 2 fire events against adversary anti-ship cruise missile surrogates using the Baseline 9.2.2. Additional testing included Baseline 9.2.2 tracking capability against small boats in both day and night conditions, and a live fire event that utilized the Close-In Weapon System, 5–inch diameter gun, and 25mm gun systems to defeat small boats in a night exercise. All testing was conducted in accordance with the DOT&E-approved test plan. The Navy intends to complete Baseline 9.2.2 testing in FY22. The Navy cancelled planned operational testing of Baseline 9.2.1 in FY20 due to the unavailability of the test ship, with the plan to conduct an operational test on Baseline 9.2.1 and Capability Package 22-1 in FY22-23.

In November 2020, the Navy canceled an Adversarial Assessment, the subsequent test in a cybersecurity evaluation to the Cooperative Vulnerability and Penetration Assessment completed in FY19, on Baseline 9.2.0 due to emergent ship repairs on the test ship. The Navy is working to reschedule this Adversarial Assessment in FY22. Additionally, the Navy needs to evaluate differences in subsequent ACB 16 Baselines to determine the scope of their cyber survivability evaluation.

An adequate evaluation of the ACB 16 operational effectiveness, suitability, and survivability is at risk. While the Navy has been coordinating with DOT&E, it has yet to provide the ACB 16 test strategy within an Aegis TEMP update for DOT&E approval. Additionally, the Navy has yet to conduct any operational testing on Baseline 9.2.1.

Performance

Effectiveness

Not enough data are yet available to assess ACB 16 operational effectiveness. The assessment of the Baseline 9.2.0 capability is summarized in a classified Early Fielding Report published in March 2020. Preliminary evaluation of Baseline 9.2.2 testing suggests anti-air and anti-surface warfare performance is consistent with legacy Aegis capability. Preliminary assessment will be summarized in a classified Early Fielding Report in FY22 after the completion of Baseline 9.2.2 testing, and the final assessment will be published in an ACB 16 OT&E report in FY23 after completion of Baseline 9.2.1 and Capability Package 22-1 testing.

Suitability

Not enough data are yet available to assess ACB 16 operational suitability. Preliminary analysis highlights reliability concerns with the Aegis Display System.

Survivability

Not enough data are yet available to assess cyber survivability of any Baseline variant of ACB 16. Survivability assessment of the Baseline 9.2.0 as installed on the CG 47-class Aegis guided missile cruiser in a cyber-contested environment will be published upon completion of the Adversarial Assessment.

Recommendations

The Navy should:

1. Submit, for DOT&E approval, a revised TEMP that details an adequate test strategy and test resources to assess the operational effectiveness and suitability of ACB 16, including additional capabilities provided in each software delivery.
2. Schedule an Adversarial Assessment on an ACB 16 Baseline 9.2.0 ship as soon as feasible to identify and mitigate any cyber vulnerabilities on ships currently employing ACB 16 in the Fleet.
3. Determine and correct cause of reliability issues with the Aegis Display System.

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

The Navy fielded the Air Intercept Missile (AIM)-9X Block II with Operational Flight Software (OFS) 9.411 in September 2021 after successfully demonstrating its operational effectiveness and suitability in FOT&E. AIM-9X Block II OFS 9.411 met or exceeded the probability of acquisition and probability of kill requirements, demonstrating improved performance in the presence of infrared countermeasures. The survivability assessment of the AIM-9X Block II OFS 9.411 in a cyber-contested environment is ongoing.

System Description

The AIM-9X Block II is the latest generation short-range, infrared-tracking, air-to-air missile. Highly maneuverable and day and night capable, the AIM-9X threshold requirement platforms are the F-15C/D and the F/A-18A+/C/D/E/F aircraft. Objective requirement aircraft are the F-16C/D, EA-18G, F-15E, F-22A and F-35A/B/C.

OFS 9.411 is the latest AIM-9X Block II update and consists of a software-only enhancement providing new and improved algorithms intended to improve probability of kill and performance in the presence of infrared countermeasures. Future improvements to AIM-9X Block II include additional pre-planned hardware improvements and obsolescence upgrades.

Program

The AIM-9X Block II is an Acquisition Category IC program. DOT&E approved the OFS 9.4 revision of the Test and Evaluation Master Plan in April 2020. The Navy's Operational Test and Evaluation Force (OPTEVFOR) completed AIM-9X Block II OFS 9.410 FOT&E in January 2021 supporting the fielding decision of the AIM-9X Block II missiles with OFS 9.411. OFS 9.410 and 9.411 are functionally the same software with the same missile capabilities. OFS 9.411 is the fielded version.

Major Contractor

Raytheon Missiles and Defense – Tucson, Arizona.

Test Adequacy

Operational and live fire testing of the AIM-9X Block II missile with 9.410 OFS was adequate to support the evaluation of the operational effectiveness, lethality, and suitability of the AIM-9X. Testing was conducted in accordance with the DOT&E-approved test plan.

AIM-9X Block II OFS 9.410 FOT&E consisted of 20 AIM-9X live-missile firing attempts, 7,170 modeling and simulation (M&S) runs, and 561 captive-carry sorties including 1,095 Captive Carry Reliability Program hours. OPTEVFOR accredited the AIM-9X digital M&S in May 2021.

Assessment of warhead lethality occurred between 2001 and 2003 during Block I testing. LFT&E is also conducting supplementary M&S runs to assess eight additional target types, and results of these analyses will be reported at the end of 2021. DOT&E will determine test adequacy of these activities at their conclusion. OPTEVFOR completed cybersecurity testing in the summer of 2021, and reporting is expected in early 2022.

Performance

Effectiveness

AIM-9X Block II with 9.410 OFS is operationally effective, meeting or exceeding the probability of acquisition and probability of kill requirements. Details are provided in the classified AIM-9X Block II 9.410 OFS FOT&E report published in September 2021.

Suitability

AIM-9X Block II with 9.410 OFS is operationally suitable on F-15, F-16, and F/A-18 aircraft. Mean time between captive-carry failure has improved for all three aircraft, especially the F/A-18, which was rated operationally unsuitable in 2015.

Survivability

Further information on AIM-9X Block II 9.411 cybersecurity survivability will be documented in the classified report on AIM-9X cybersecurity, which will be released in 2022.

Recommendation

1. The Services should complete lethality and cybersecurity testing and consider the two additional recommendations detailed in the classified AIM-9X Block II OFS 9.410 FOT&E report published in September 2021.

CH-53K King Stallion

The Marine Operational Test and Evaluation Squadron (VMX-1) began IOT&E on July 30, 2021. In accordance with the CH-53K Security Classification Guide, the interim assessment of CH-53K effectiveness, suitability and survivability is detailed in the Controlled Unclassified Information edition of this report. The report provides preliminary observations on CH-53K handling qualities in adverse flying conditions, load capacity, maintainability and reliability status as compared to the CH-53E as well the status of the CH-53K survivability key performance parameter. Final assessments of operational effectiveness, suitability, and survivability will be provided after the completion of IOT&E in February 2022.

System Description

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 while maintaining a shipboard logistics footprint equivalent to that of the CH-53E. The Marine Air-Ground Task Force equipped with the CH-53K is intended to conduct heavy-lift missions, support forward arming and refueling, provide assault support in casualty evacuation, and conduct recovery and maritime special operations, as well as airborne control for assault support.

Program

The CH-53K is an Acquisition Category IC program. DOT&E approved the Milestone C Test and Evaluation Master Plan (Revision C) in February 2017 and the Alternative LFT&E Strategy (Revision C) in May 2010. IOT&E started on July 30, 2021 and is intended to support the full-rate production decision scheduled for 2QFY23.

Major Contractor

Sikorsky Aircraft (a Lockheed Martin subsidiary company) – Stratford, Connecticut.

Test Adequacy

In FY21, the Integrated Test Team (ITT) completed sufficient developmental testing to support the start of IOT&E. The Marine Operational Test and Evaluation Squadron VMX-1 began IOT&E on July 30, 2021 with four System Development Test Articles that do not have the full defensive electronic countermeasure (DECM) system. DECM integrated testing with an EDM aircraft configured with a full DECM suite is planned for 2QFY22. FOT&E is planned with low-rate initial production Lot 2 aircraft to include the continuation of DECM testing and the evaluation of aircraft improvements.

Integrated and operational testing completed to date has been conducted in accordance with DOT&E-approved test plans. Cyber security testing is scheduled for February 2022.

In 3QFY20, the Navy resumed live-fire testing of CH-53K on the Ground Test Vehicle (GTV), starting with fuel cell and sponson testing against threshold threats under cruise and hover conditions. Phase II GTV testing of flight controls and the fuel and hydraulic systems began with on-board testing in November 2020 and was completed in March 2021. Phase III GTV testing to dynamically evaluate high-risk shots, including of gearboxes, structure, flight controls, the drive system, and the engine bay fire suppression system in a hover condition, began in May 2021 and completed in December 2021.

Live fire testing of the armor panels installed on the aircraft against operationally representative threats began in April 2021 and concluded in September 2021 with testing of the armored cockpit seats.

Tail rotor blade ballistic testing took place in December 2020. Sikorsky will endurance test the threat-damaged test articles to representative 30-minute fly-home loads in 2QFY22.

The Program Office has continued to defer Phase II of the LFT&E program until after initial operational capability. Phase II of the LFT&E program is essential for a complete survivability assessment of the CH-53K against operationally relevant threats. This phase includes component tests for the main rotor assembly and tail rotor hub against threshold threats originally scheduled to support the Milestone C decision and additional components added or modified during aircraft development. While live fire testing to date has been conducted in accordance with DOT&E-approved LFT&E plans, Phase II live fire testing, defined in the DOT&E-approved Alternate LFT&E Strategy, has not yet been fully funded.

Performance

In accordance with the CH-53K Security Classification Guide, the interim assessment of CH-53K effectiveness, suitability and survivability is detailed in the Controlled Unclassified Information edition of this report. The report provides preliminary observations on CH-53K handling qualities in adverse flying conditions, load capacity, maintainability and reliability status as compared to the CH-53E as well the status of the CH-53K survivability key performance parameter.

Recommendations

The Navy should:

1. Develop an FOT&E program to evaluate deployment capabilities that will not be tested in IOT&E.
2. Develop mitigations to address any design deficiencies identified in testing and plan to verify those mitigations in FOT&E.
3. Develop and fully fund Phase II of the LFT&E program as described in the DOT&E-approved LFT&E Strategy.

CMV-22B Joint Services Advanced Vertical Lift Aircraft – Osprey – Carrier Onboard Delivery

The Navy will declare CMV-22B initial operational capability in 1QFY22 based on the CMV-22B FOT&E conducted by the Air Test and Evaluation Squadron (VX-1) from January 11, 2021 to July 16, 2021 under the auspices of Navy Commander, Operational Test and Evaluation Force (COMOPTEVFOR). Not enough data are yet available to provide a preliminary survivability assessment of the CMV-22B in a contested environment.

System Description

The CMV-22B Osprey is a tiltrotor vertical/short takeoff and landing aircraft intended to replace C-2A Greyhound, the carrier onboard delivery aircraft. The CMV-22B is based on the MV-22B design equipped with increased fuel capacity, fuel jettison, integrated public address system, high-frequency (HF) radio, and cabin and cargo lighting. The Navy Fleet Logistics Multi-Mission Squadrons (VRM-30 and VRM-40) intend to use the CMV-22B to conduct the airborne resupply/logistics for seabasing missions, vertical onboard delivery, vertical replenishment, medical evacuation, Naval Special Warfare support, missions of State, and search and rescue support.

Program

The CMV-22B, as part of the overall V-22 Program of Record, is an Acquisition Category IC program, which entered full-rate production in 2005. The CMV-22B has been incorporated with the current V-22 production line and deployed to the fleet. It will achieve initial operational capability in FY22 and full operational capability in FY23. DOT&E approved the CMV-22B Test and Evaluation Master Plan and the Alternative LFT&E plan in March, 2020.

Major Contractors

Bell-Boeing Joint Venture: Bell Helicopter – Amarillo, Texas. The Boeing Company – Ridley Township, Pennsylvania.

Test Adequacy

The Air Test and Evaluation Squadron (VX-1) conducted FOT&E OT-D1 from January 11, 2021 to July 16, 2021 under the auspices of COMOPTEVFOR. VX-1 conducted OT-D1 during the Composite Training Unit Exercise (COMPTUEX) using VRM-30 aircraft and personnel. Testing was adequate to support an assessment of CMV-22B operational effectiveness, suitability, and survivability and conducted in accordance with the DOT&E-approved test plan.

COMOPTEVFOR conducted the CMV-22B Cooperative Vulnerability and Penetration Assessment and Adversarial Assessment from July 5 – 16, 2021. Testing was adequate and conducted in accordance with the DOT&E-approved test plan.

The Navy conducted live fire testing of the CMV-22B 4-ply wing auxiliary tank fuel cells, hydraulic lines, and enhanced fire suppression powder panels at China Lake, California from October through December, 2020. Testing was adequate and conducted in accordance with the DOT&E-approved live fire test plan. Qualification testing of the improved 2-ply fuel cells is ongoing. Live fire testing of the 2-ply fuel cells is scheduled for early to mid FY23.

Performance

Effectiveness and Suitability

In accordance with the CMV-22B Security Classification Guide, the operational effectiveness and suitability of the CMV-22 is detailed in the Controlled Unclassified Information edition of this report. The report assesses the ability of the CMV-22 to execute carrier onboard delivery, medical evacuation, Naval Special Warfare support, and search and rescue missions. It details the over-the-horizon communications to support "Blue-water" operations beyond range of land. The report also assesses the suitability requirements and training and their effects on the mission.

Survivability

Not enough data are yet available to provide a preliminary survivability assessment of the CMV-22B in a contested environment. Preliminary results against kinetic threats are detailed in the Controlled Unclassified Information edition of this report. Data analysis is ongoing to evaluate the CMV-22B survivability in a cyber-contested environment.

Recommendation

1. The Navy should address the recommendations detailed in the Controlled Unclassified Information edition of this report.

Conventional Prompt Strike

The Navy is currently using Middle Tier of Acquisition Rapid Prototyping and Rapid Fielding acquisition authorities to develop and initially field the Conventional Prompt Strike (CPS) weapon system onboard a *Zumwalt*-class surface combatant, followed by a *Virginia*-class submarine. Not enough data are yet available to evaluate the CPS capabilities required for the CPS program to transition from rapid prototyping to fielding. Testing should incorporate operationally representative targets and environments to provide confidence in the system in support of an early fielding decision.

System Description

CPS is a conventional, boost-glide hypersonic weapon system. The CPS all-up-round missile includes a two-stage solid rocket motor booster and a Common Hypersonic Glide Body (C-HGB) containing a kinetic-energy-projectile warhead. The Navy intends to launch CPS from *Zumwalt*-class surface combatants and *Virginia*-class submarines to attack high-value and time-sensitive targets. The Army plans to employ the same all-up-round from mobile land-based launchers as part of the Long Range Hypersonic Weapon (Dark Eagle) program.

Program

The Navy's CPS acquisition strategy is designed to develop fieldable prototypes and transition to production in three phases. Phase 1 is a Middle Tier of Acquisition Rapid Prototyping program intended to develop and demonstrate a prototype cold-gas launched hypersonic missile system. Phase 2 is a Middle Tier of Acquisition Rapid Fielding program intended to field the hypersonic missile system onboard a *Zumwalt*-class surface combatant. Phase 3 intends to transition the program to a Major Defense Acquisition Program at Milestone C with the intent to conduct IOT&E and field the hypersonic missile system onboard the remaining *Zumwalt*-class combatants and *Virginia*-class submarines.

The Navy received an approval for Phase 1 Rapid Prototyping and expects to receive an approval for Phase 2 Rapid Fielding. The Army plans to deliver a land-based hypersonic prototype capability using the Navy developed missile. The Navy CPS program is responsible for the design and development for the C-HGB and the missile booster; missile booster production; integration of the Army-produced C-HGB with the missile booster to create an all-up-round; and design, development, and production of the Navy's sea-based weapon control system and launcher.

In 2019, the Navy developed a Master Test Strategy (MTS) for the initial phase of the program. In May 2021, DOT&E certified the MTS for the Phase 1 Rapid Prototyping strategy as appropriate to demonstrate the capability

of the cold-gas launched prototype hypersonic missile system. DOT&E is working with the Navy to update the Phase 1 MTS to include programmatic changes and additional performance metrics, and to develop an expanded scope Milestone B Test and Evaluation Master Plan-equivalent document for the Phase 2 Rapid Fielding on *Zumwalt*-class.

Major Contractors

Lockheed Martin Space Systems – Denver, Colorado.

Test Adequacy

The Army and the Navy will start the Phase 1 flight tests as Joint Flight Campaign events to determine Phase 1 flight performance and mission-relevant limitations of the common components of the hypersonic weapon systems. Collection of joint test data is necessary to identify and leverage common practices, test corridors and infrastructure, test data, and modeling and simulation (M&S) capability across the family of hypersonic weapon systems. The Navy intends to execute Phase 2 operational demonstrations, but limited flight test opportunities pose a risk to demonstrating the required operational capability in support of the fielding of the hypersonic missile system onboard a *Zumwalt*-class surface combatant.

In FY20, the CPS program performed a sled test of the CPS/Dark Eagle warhead, which provided data for validating the lethality M&S tools against materials but not operationally representative targets. The CPS program also conducted a Flight Experiment-2 in which a CPS missile was fired from the Pacific Missile Range Facility Barking Sands test range but did not provide data to validate the M&S tools against operationally representative targets. The program has not performed arena testing on the operationally representative warhead, which is fundamental to the development of lethality M&S.

Performance

Effectiveness

Not enough data are yet available to evaluate the CPS effectiveness and lethality required for the CPS program to transition from Phase 1 to Phase 2. Demonstrated capabilities and limitations will be published in a classified Early Fielding Report after the completion of Phase 2 testing.

Suitability

Not enough data are yet available to evaluate the CPS suitability capabilities required for the CPS program to transition from Phase 1 to Phase 2. The program intends to complete an initial Life Cycle Support Plan to address product support and fielding on a *Zumwalt*-class in FY22.

Survivability

No data are currently available to evaluate the survivability of CPS in a contested environment. The Navy plans to evaluate the survivability of CPS in operationally relevant environments by modeling and simulation only, increasing the risk to the survivability assessment unless the modeling and simulation tools are adequately verified, validated, and accredited.

Recommendations

The Navy should:

1. Complete an update to the CPS Phase 1 MTS to account for recent programmatic changes and to include the required performance metrics.
2. Incorporate operationally representative targets and environments into CPS flight tests and other lethality and survivability tests.
3. Fully fund and execute the LFT&E strategy that adequately verifies and validates required modeling and simulation tools in order to create credible weaponeering and mission planning tools in support of the proposed operational fielding dates. Any delay in the start of this effort will substantially increase the risk to assessing the lethal effects of the CPS weapon system in time for operational fielding.
4. Collaborate with the Air Force to identify and leverage common practices, test corridors and infrastructure, test data, and M&S capability across the family of hypersonic weapon systems.

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

Poor or unknown reliability of systems critical for flight operations, including newly-designed catapults, arresting gear, weapons elevators, and radar continue to pose the most significant risk to CVN 78 demonstrating operational effectiveness and suitability in IOT&E scheduled for 2QFY23. Testing of the CVN 78 Integrated Combat System (ICS) was not adequate to assess the combat system's capability against supersonic anti-cruise ship missiles (ASCMs), and there are no future test events planned that could provide additional data on these threats.

CVN 78 Full-Ship Shock Trial (FSST) results identified several design shortfalls not previously discovered by modeling and simulation (M&S) or component-level testing, that, if addressed, could improve the survivability of the CVN 78 against underwater threat engagements.

System Description

The CVN 78 *Gerald R. Ford*-class aircraft carrier is a new class of nuclear-powered aircraft carriers based on the CVN 68 *Nimitz* class hull, with significant design changes intended to enhance CVN 78's ability to launch, recover, and service aircraft while reducing the manning capacity by approximately 20 percent. CVN 78 includes a new nuclear power plant, increasing the electrical power capacity to power among other systems, electromagnetic catapults, and arresting gear. CVN 78 also incorporates a more efficient flight deck layout with additional aircraft fueling stations, redesigned weapons elevators, weapons handling spaces, and magazine stowage to reduce manning, improve safety, and increase weapon throughput. The CVN 78 ICS incorporates several changes, including the:

- Dual Band Radar (DBR) that combines the phased-array SPY-4 Volume Search Radar and the SPY-3 Multi-Function Radar, which will be replaced with the SPY-6(V)3 Enterprise Air Surveillance Radar (EASR) and the AN/SPQ-9B Anti-ship Missile Defense Radar on CVN 79.
- Ship Self-Defense System (SSDS) Mark 2 Mod 6 combat management system, which will be replaced with the new capability build SSDS Mark 2 Baseline 12 on CVN 79.
- Cooperative Engagement Capability (CEC) USG-2B tracking, data fusion, and distribution system.
- SLQ-32(V)6 electronic surveillance and warfare system equipped with Surface Electronic Warfare Improvement Program Block 2, which will be equipped with the Soft Kill Coordination System on CVN 79.
- Rolling Airframe Missile (RAM) Block 2 and the Evolved Sea Sparrow Missile (ESSM) Block 1; RAM Block 2 will be replaced by RAM Block 2A and 2B on CVN 79.

- Phalanx Close-In Weapon System (CIWS) radar, which will be integrated with CEC and the gun integrated with SSDS on CVN 79 to achieve a fully integrated ship self-defense against ASCMs.

The CVN 78 class ships also have enhanced survivability features, including improved protection for magazines and other vital spaces, shock-hardened mission systems and components, and installed and portable damage control, firefighting, and dewatering systems intended to expedite response to, and recovery from, fire, flooding, and battle damage. CVN 78 includes a new Heavy Underway Replenishment system capable of transferring cargo loads of up to 12,000 pounds.

Program

The CVN 78 *Gerald R. Ford*-class is an Acquisition Category IC program. DOT&E approved the Test and Evaluation Master Plan (TEMP) Revision B in 2007, but disapproved TEMP Revision C in 2015 because it proposed deferring full-ship shock trials. The Navy withdrew TEMP Revision D in 2019 before submitting it to DOT&E for approval and is still drafting TEMP Revision E. The first ship in the *Ford*-class, CVN 78, was delivered to the Navy in 2017. It completed Post Delivery Test and Trials in 2021 to demonstrate the basic functionality of the carrier, certify the flight deck, embark an air wing, and serve as the East Coast carrier qualification platform for fleet naval aviators. CVN 78 is now in a planned incremental availability phase that will be followed by IOT&E starting in early 2023 and subsequent deployment. CVN 79 delivery is scheduled for 2024, at which time it is expected to be able to support F-35 operations. CVN 80 construction began in 2017.

The Navy has yet to provide funding for the M&S suite required to evaluate CVN 78's Probability of Raid Annihilation requirement against subsonic ASCM targets. The Navy agrees an unmanned test asset is required to adequately and safely test the self-defense capability of CVN 79 against ASCM surrogates. The Navy committed to providing the resources required to retain this capability via a planned maintenance availability of the Self-Defense Test Ship (SDTS) (i.e., *Paul F. Foster*), as well as the procurement and installation of the necessary CVN 79 combat system elements on this test ship.

Major Contractors

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

Test Adequacy

In December 2020, the Navy concluded the Self-Defense Test Ship phase of CVN 78 ICS operational test by conducting a test against supersonic ASCM surrogates. The Navy completed three of the four planned Self-Defense Test Ship tests in the DOT&E-approved test plan, and those that were completed deviated from the approved test plan. Testing was not adequate to assess the combat system's capability against supersonic ASCMs and subsonic maneuvering ASCMs, and there are no future test events planned that could provide additional data against these threats. DOT&E will issue an interim assessment of CVN 78 self-defense capabilities in FY22.

Only a limited assessment of CVN 78 combat system effectiveness is possible. The 2008 DOT&E-approved Enterprise TEMP called for the use of DDG 1000 combat system performance data to supplement the evaluation of the CVN 78 combat system; however, the redesigned DDG 1000 system differs significantly from the CVN 78 system. The Navy did not supplement the CVN 78 test campaign to compensate for the 10 test events it originally expected to leverage from DDG 1000 testing.

The Navy tested the combat system aboard CVN 78 during Combat Systems Ship's Qualification Trials (CSSQT) and combat systems operational rehearsal events. This testing was not covered by a DOT&E-approved test plan.

From June to August 2021, the Navy completed FSST to assess CVN 78's combat shock survivability. The trial was adequate to evaluate the ship's operational survivability after exposure to an underwater threat induced shock. The trial consisted of a series of three nearby underwater explosions of increasing severity up to two-thirds of the design level requirement/specification. The ship was manned and operational during each shot. Testing included a demonstration of the ship's ability to continue its primary missions after shock. Where shock-hardened ship systems and equipment could not continue operating after shock, trial cards were

written to identify shock deficiencies for correction. In accordance with the approved trial plan, the ship was not outfitted with live ordnance or an air wing, and most JP-5 aviation fuel was removed.

The Navy expects to begin IOT&E in 2QFY23, following planned incremental availability at Newport News Shipyard. The Navy is planning to conduct IOT&E in accordance with draft TEMP Revision E and DOT&E reports to Congress dated November 30, 2018 and November 26, 2019, but the TEMP Revision E and required test plans have not yet been submitted for approval by DOT&E.

While the Navy has proposed several strategies to test the cyber survivability of CVN 78, none of these strategies have been finalized, adequately resourced, or formally approved by DOT&E.

Performance

Effectiveness

Combat System

In accordance with the CVN-78 Security Classification Guide, the effectiveness of the combat system is detailed in the Controlled Unclassified Information edition of this report. The report details the capability of the combat system to detect, track, engage, and defeat the types of threats for which the system was designed.

Sortie Generation Rate (SGR)

CVN 78 is unlikely to achieve its SGR requirement. The target SGR threshold is well above achieved historical rates and based on unrealistic assumptions, including fair weather and unlimited visibility, along with the expectation that aircraft emergencies, failures of shipboard equipment, ship maneuvers, and manning shortfalls will not negatively affect flight operations. Poor reliability of key systems that support sortie generation on CVN 78 could cause a cascading series of delays during flight operations that would likely negatively affect CVN 78's ability to generate sorties. The reliability of these critical subsystems represents the most risk to the successful completion of CVN 78 IOT&E.

Electromagnetic Spectrum Compatibility

Developmental testing identified significant electromagnetic radiation hazard and interference problems. The Navy implemented some mitigation measures and conducted follow-on characterization testing during Independent Steaming Events (ISEs) in developmental test, 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 use to inform decisions on system employment.

Suitability

Reliability

The low reliability of the following four new CVN 78 systems stand out as the most significant challenges expected to affect the ship's flight operations:

Electromagnetic Aircraft Launch System (EMALS)

During the 8,157 catapult launches conducted through ISE 18, EMALS achieved a reliability of 272 mean cycles between operational mission failures (MCBOMF), where a cycle is the launch of one aircraft. This reliability is well below the requirement of 4,166 MCBOMF. The reliability concerns are amplified by the fact that the crew cannot readily electrically isolate EMALS components during flight operations because of the shared nature of the Energy Storage Groups and Power Conversion Subsystem inverters on board CVN 78. The process for electrically isolating equipment is time-consuming. Spinning down the EMALS motor and generators alone is a 1.5-hour process, precluding some EMALS maintenance during flight operations.

Advanced Arresting Gear (AAG)

During 8,157 recoveries, AAG achieved a reliability of 41 MCBOMF, where a cycle is the recovery of a single aircraft. This reliability estimate falls well below the requirement of 16,500 MCBOMF.

The reliability concerns are amplified by the AAG's design, which does not allow the Power Conditioning Subsystem equipment to be electrically isolated from high power buses, limiting corrective maintenance on below-deck equipment during flight operations.

Advanced Weapons Elevators (AWE)

While all 11 AWEs have been installed, only 8 of the 11 have been formally delivered to the Navy. The

other three are installed, but are still the responsibility of the manufacturer. Therefore, only preliminary reliability estimates are available to compare to the requirement of 932 hours between operational mission failure. Through the first 14,842 elevator cycles, 68 operational mission failures were reported. AWE system reliability will be critical as the Navy completes delivery of the remaining three elevators and develops standard procedures for moving ordnance from magazines to the flight deck.

Dual Band Radar (DBR)

Through ISE 18, DBR demonstrated a reliability of 102 hours mean time between operational mission failures. This is below the requirement of 339 hours. However, DBR was operationally available 96 percent of the time, close to the 98 percent requirement.

Survivability

While shock trial data analysis is ongoing, the Navy has already identified several survivability improvement opportunities for the CVN 78 class against underwater threat engagements. Details will be provided in an interim, classified CVN 78 FSST report expected to be published 2QFY22 after all data and observations have been adequately reviewed and analyzed.

The survivability of CVN 78 in a cyber-contested environment has not yet been evaluated. Many subsystems on the ship were tested to various degrees in both developmental testing and operational testing on other ship platforms. However, required CVN 78 platform-level testing has not yet occurred, and some systems specific to CVN 78 have yet to undergo any operational cyber survivability assessments. These assessments will need to be conducted as part of CVN 78 IOT&E.

The survivability of CVN 78 in a contested and congested electromagnetic spectrum environment has not yet been evaluated. Discussions on how to evaluate CVN 78 survivability in contested and congested electromagnetic spectrum environments are ongoing with the Navy.

Recommendations

The Navy should:

1. Address combat system issues identified during CVN 78 ICS testing during CSSQT and on the SDTS.
2. Fund the M&S suite required to assess the CVN 78 Probability of Raid Annihilation requirement for subsonic targets.
3. Implement the recommendation contained in DOT&E's FY20 report to complete Self-Defense Test Ship test events.
4. Continue to improve availability and reliability for EMALS, AAG, DBR, and AWE.
5. Implement major fixes to CIWS hardware and software to improve the system's reliability and operational availability.
6. Continue to characterize the electromagnetic spectrum environment on board CVN 78 and develop operating procedures to maximize system effectiveness and maintain safety. As applicable, the Navy should use the lessons learned from CVN 78 to modify the design of CVN 79 and future carriers.
7. Implement design changes to address survivability issues identified during the FSST.
8. Complete validation of the M&S tools supporting the LFT&E assessment, including comparing the FSST data to relevant M&S predictions.
9. Continue to fund the maintenance availability for the current SDTS (e.g., *Paul F. Foster*) to ensure its readiness to support CVN 79 combat system testing.
10. Continue to fund the procurement and installation of the necessary CVN 79 combat system elements on the Self-Defense Test Ship.
11. Conduct a shore-based operational assessment of EASR at Wallops Island, Virginia. This testing should evaluate EASR's contributions to air traffic control and self-defense missions, as well as provide an early assessment of electromagnetic interference and radiation hazard concerns.
12. Update the CVN 78 platform TEMP to include cybersecurity testing on CVN 78 and testing of the combat system on CVN 79 to assess the effectiveness and suitability of the new combat system with EASR.

DDG 1000 – *Zumwalt*-Class Destroyer

In FY21, the Navy executed three missile exercises on the Self Defense Test Ship (SDTS) to evaluate the DDG 1000's self-defense capability and validate the DDG 1000 combat system modeling and simulation (M&S) test bed. While not enough data are yet available to provide a preliminary assessment of DDG 1000 operational effectiveness, suitability, and survivability, live missile testing highlighted limitations that may restrict operational effectiveness in the air warfare mission. The DDG 1000 IOT&E started in October 2021.

System Description

The DDG 1000 is a long-range, low observable, destroyer class ship intended primarily for forward deployed offensive surface strike (OaSUW) missions. Secondary missions include undersea and surface warfare dominance. The DDG 1000 is equipped with: 1) Modified AN/SPY-3 Multi-Function (X-band) radar that adds a volume search capability, 2) 80 vertical launch cells to employ Tomahawk Land Attack Missiles, Standard Missiles (SM-2/SM-6s), Vertical Launch Anti-Submarine Rockets, and Evolved Sea Sparrow Missiles, 3) an integrated undersea warfare system with a mid-frequency bow-mounted sonar, and 4) two Mk 46 30mm close-in gun systems.

Program

The DDG 1000 is an Acquisition Category IC program. The President's Budget in 2011 truncated the DDG 1000 class to three ships. The Navy commissioned USS *Zumwalt* (DDG 1000) in 2016 and USS *Michael Monsoor* (DDG 1001) in 2019, and expects the delivery of USS *Lyndon B Johnson* (DDG 1002) in FY24. The Navy is updating the DDG 1000 Test and Evaluation Master Plan (TEMP) due to significant modifications to the DDG 1000 operational requirements and warfighting concept of operations. In 2019, the Navy changed the DDG 1000 primary mission to open ocean OaSUW and codified additional changes in a June 2021 revision to the DDG 1000 Operational Requirements Document. The DDG 1000 IOT&E started in October 2021 and will inform the Fleet of the DDG 1000's operational performance but not a Navy buy decision.

Major Contractors

- Bath Iron Works – Bath, Maine.
- Raytheon Company – Andover, Massachusetts.
- Raytheon Missile Systems – Tucson, Arizona.

Test Adequacy

In FY21, the Navy executed three missile exercises on the SDTS to evaluate the DDG 1000's self-defense capability and validate the DDG 1000 combat system M&S test bed.

Due to shipyard delays and persistent combat systems integration faults affecting multiple warfare areas, the test ship could not support the DDG 1000 IOT&E, initially planned for FY19. The Navy started IOT&E in October 2021, but the Navy must still develop a test strategy for the intended OaSUW capability.

The Navy has not planned or funded an adequate ship survivability assessment against underwater threats, to include a demonstration of residual mission capability after such engagements, through a full-ship shock trial. Given the current schedule, this assessment will not be complete prior to initial deployment of a DDG 1000 ship.

The Navy has not yet modeled the ship as built to support an LFT&E assessment, and has yet to verify, validate, and accredit the intended vulnerability M&S needed to evaluate ship survivability against air-delivered threats. Planned shipboard testing will supplement some gaps in the capability of survivability models and support the final survivability assessment.

The Navy plans to start Failure and Recoverability Mode testing on USS *Michael Monsoor* in 1QFY22 to evaluate the mission systems' capability to recover from system failures and effectiveness of damage control response. Development delays and required updates to the ship's combat system and auxiliary systems have limited the opportunity to conduct this evaluation.

The Navy has scheduled the cyber survivability assessment for 3QFY22.

Performance

Effectiveness

Not enough data are yet available to provide a preliminary assessment of DDG 1000 operational effectiveness. The DDG 1000 live missile events using SDTS highlighted performance limitations that may restrict operational effectiveness in the air warfare mission. Final assessment of DDG offensive surface strike effectiveness will be published in a classified report following the completion of the live missile events.

Suitability

Not enough data are yet available to provide a preliminary assessment of DDG 1000 operational suitability.

Survivability

Survivability assessments conducted thus far have not been validated and do not reflect the ship as-built. Consequently, data are insufficient to adequately assess DDG survivability in a contested environment, to include a cyber-contested environment.

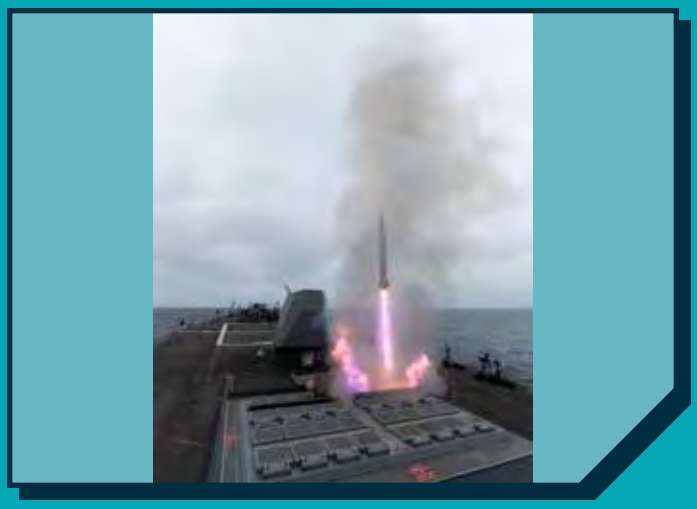
Recommendations

The Navy should:

1. Complete IOT&E prior to the first deployment of a DDG 1000 ship.
2. Complete revision of the TEMP that includes an adequate test strategy for the delivered OaSUW capability as soon as feasible.
3. Schedule, fund, and execute the four remaining DDG 1000 SDTS tests.
4. Complete development and validate the DDG 1000 combat system test bed, to include debris, missile, radar, and electronic warfare models.
5. Document the risk to the warfighter associated with incomplete component shock qualification and lack of full-ship shock trial.
6. Complete validation of LFT&E M&S for the ship as-built and determine required mitigations to identified limitations.

Evolved Sea Sparrow Missile Block 2

In August 2021, the Navy conducted seven Evolved Sea Sparrow Missile (ESSM) Block 2 live-fire events from the USS *Shoup* (DDG 86). The testing identified several deficiencies that the Navy will need to address to mitigate the risk to meeting operational effectiveness requirements prior to declaring initial operational capability, scheduled for 2QFY22. The final evaluation of ESSM Block 2 operational effectiveness, suitability, and survivability will not be available until FY25 when Aegis weapon system upgrades are expected to enable employment of full ESSM Block 2 capabilities.



System Description

The ESSM is a short to medium-range, ship-launched, guided missile intended to provide defensive, hard-kill engagement capability against anti-ship cruise missiles (ASCMs) as part of a layered defense of Aegis cruisers and destroyers and SSDS Mk 2 platforms, to include aircraft carriers and amphibious ships. ESSM Block 2 leverages Standard Missile 6 technology to reduce reliance on illuminator support and mitigate challenges in missile sequencing that are inherent in high-density stream raids. Semi-active guidance (using shipboard illuminators) is retained from ESSM Block 1 to engage stressing radar cross section threats and high-altitude diving ASCMs. The ESSM Block 2 also features a new blast fragmentation warhead. The Navy intends the ESSM Block 2 seeker upgrade to improve performance against stressing air warfare threats (including stream raids) in challenging electromagnetic spectrum environments.

Program

The ESSM 2 is an Acquisition Category II program. The Navy expects to deliver the Test and Evaluation Master Plan (TEMP), to include its LFT&E Strategy, for DOT&E approval in 2QFY22 in support of the full-rate production decision scheduled for FY25. The Navy intends to evaluate ESSM Block 2 operational effectiveness and suitability in two phases of IOT&E to support the initial operational capability and full-rate production decision, respectively. Phase 1 IOT&E, expected to be completed in 2QFY22, employs ESSM Block 2 with current Aegis weapon system capability, which cannot not exercise the full ESSM Block 2 capability. Phase 1 IOT&E also supports development and validation of modeling and simulation (M&S) that the Navy intends to use in Phase 2 IOT&E. Phase 2 IOT&E, expected to be completed in FY25, will employ ESSM Block 2 with an upgraded Aegis weapon system, enabling the exercise of full ESSM Block 2 capability.

Major Contractor

Raytheon Missiles and Defense – Tucson, Arizona.

Test Adequacy

In August 2021, the Navy conducted seven ESSM Block 2 live firing events from the USS *Shoup* (DDG 86) in accordance with the DOT&E approved Phase 1 IOT&E plan. The Navy scheduled an ESSM Block 2 firing event from the Navy's Self-Defense Test Ship in 1QFY22 and is on track to conduct M&S runs and a cybersecurity assessment in FY22 to complete Phase 1 IOT&E. In accordance with the approved plan, Phase 1 IOT&E data will not be sufficient to determine operational effectiveness and operational suitability of ESSM Block 2, but will rather serve to inform ESSM Block 2 capabilities and limitations in support of the initial operational capability. Phase 2 IOT&E events are intended to provide sufficient data for an adequate determination of operational effectiveness, suitability, and survivability.

From June 2019 to October 2020, the Navy conducted warhead characterization testing and limited single-fragment and multiple-fragment ground lethality testing against ASCM target surrogates. The Navy intends to conduct M&S runs against a set of secondary targets in 2QFY22 as lethality runs for score to complement the lethality data from ESSM Block 2 developmental testing, IOT&E flight tests, and IOT&E M&S runs.

Performance

Effectiveness

The Navy will need to address deficiencies identified in Phase 1 IOT&E to mitigate ESSM Block 2 risk to meeting operational effectiveness requirements. The Navy will need to complete the lethality M&S runs for score to adequately evaluate ESSM Block 2 lethal effects. The details are classified and will be summarized in the Early Fielding Report after the completion of Phase 1 IOT&E.

Suitability

Phase 1 IOT&E has not yet provided enough data to support a preliminary assessment of ESSM Block 2 operational suitability or identify any risks to meeting operational suitability requirements. The final operational suitability assessment will be based on data from all test events and fleet firings through the completion of Phase 2 IOT&E.

Survivability

The survivability assessment of the ESSM Block 2 in a cyber-contested environment will be provided after the completion of the Cyber Vulnerability Penetration Assessment and the Adversarial Assessment scheduled in FY22. Planned FOT&E testing will evaluate ESSM 2 performance in the presence of a contested and congested electromagnetic spectrum environment.

Recommendations

The Navy should:

1. Determine the root cause of the classified deficiency identified in Phase 1 IOT&E and implement changes prior to Phase 2 IOT&E to mitigate the ESSM Block 2 risk to meeting operational effectiveness requirements.
2. Complete the lethality M&S runs for score and share all lethality data and reports with appropriate stakeholders to facilitate the final lethality assessment.

F/A-18 Infrared Search and Track Block II

Operational testing of the F/A-18 Infrared Search and Track (IRST) Block II, originally planned for 1QFY21, was delayed until at least 2QFY23 due to hardware and software delays. The IRST Block II program needs to resolve several open deficiencies from previous IRST versions, as well as those discovered during Block II developmental testing with prototype systems, to be operationally effective. The late delivery of production-representative software could negatively affect suitability during IOT&E. The proposed schedule allows minimal time for problem discovery and deficiency resolution prior to the planned start of IOT&E.

System Description

The ASG-34A(V)1 F/A-18E/F IRST is a centerline-mounted store consisting of a long-wave infrared sensor that provides a passive fire control system intended to search, detect, track, and engage airborne targets at long range. The IRST is intended to act as a complementary sensor to the AN/APG-79 fire control radar in a heavy electronic attack or radar-denied environment. It is designed to operate autonomously, or in combination with other sensors, to support the guidance of beyond-visual-range air-to-air missiles, including the AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM) and AIM-9X Sidewinder Block II.

Program

The F/A-18 IRST Block II is an Acquisition Category IC program intended to field the IRST Block II system to carrier-based F/A-18E/F Super Hornet squadrons to improve lethality and survivability in air superiority missions against advanced threats. DOT&E approved the Milestone C Test and Evaluation Master Plan in May 2021. IOT&E is scheduled to begin in 2QFY23 in support of the full-rate production decision scheduled for August 2023.

Major Contractors

Lockheed Martin Missiles and Fire Control – Orlando, Florida. Boeing Defense – St. Louis, Missouri.

Test Adequacy

The Navy plans to conduct IOT&E between January and May 2023 and has not yet provided the IOT&E plan to DOT&E for approval.

In August 2021, the Navy simultaneously executed developmental test events involving F/A-18E/F System Configuration Set H16, IRST Block II, and E-2D with Delta System Software Configuration 4 software during a Gray Flag exercise detachment at Naval Air Station Point Mugu, California. This system-of-systems approach is likely to maximize the effectiveness and efficiency of future operational test events, once IRST Block II hardware issues are addressed and system software is mature and stable.

Performance

Effectiveness

The IRST Block II program needs to resolve several open deficiencies from previous IRST versions, as well as those discovered during Block II developmental test with prototype systems, to be operationally effective. Additionally, the Navy must improve the Super Hornet's operating software and correct existing deficiencies to enable IRST to be an effective contributor to aircraft fire control solutions. The IRST Block II prototype pod demonstrated tactically relevant detection ranges against operationally relevant targets during initial developmental test events. However, the Navy is still developing the IRST and F/A-18E/F software to be able to translate these long-range target detections into stable system tracks that facilitate weapons employment. The Navy continues to discover and fix deficiencies as the program progresses through developmental test. The ability of the Navy and the contractor to fix the critical issues on schedule is the most significant risk to a successful IOT&E.

Suitability

The prototype IRST Block II systems currently being utilized in developmental test are demonstrating reliability well below the Navy's requirements. Additionally, the prototype systems do not possess complete Built-in-Test functionality, which makes fault detection and troubleshooting difficult for maintainers and aircrew. The production-representative versions of the system slated for use in IOT&E are scheduled to arrive in April 2022, with planned IOT&E software delivery occurring two months prior to IOT&E start. Although this revised schedule provides additional opportunity for maintenance process maturity and reliability growth than originally planned, the late delivery of production-representative software could negatively affect suitability during IOT&E.

Survivability

The IRST Block II is intended to contribute to the survivability of the F/A-18E/F by providing target tracks in a contested and congested electromagnetic spectrum environment. This capability remains, however, untested in an operationally representative environment.

The survivability of the IRST Block II in a cyber-contested environment will be evaluated as part of IOT&E.

Recommendation

1. The Navy should address the known IRST Block II and Super Hornet hardware and operating software deficiencies and continue to test unproven capabilities in developmental testing to prepare the system for IOT&E and adequately demonstrate its operational effectiveness, suitability, and survivability.

F/A-18E/F Super Hornet

The F/A-18E/F Super Hornet program experienced development challenges in the latest software update, System Configuration Set (SCS) H16, which delayed the operational test for Block II aircraft by nine months to June 2021. Operational testing of the latest Super Hornet configuration, Block III, is scheduled to begin in 2QFY22. The Navy expects to complete Block II and Block III SCS H16 FOT&E in 2022 to support a fleet release expected in 2QFY22.

System Description

The F/A-18E/F Super Hornet, the U.S. Navy's principal power projection aircraft, is a strike fighter and attack aircraft. It performs a variety of roles that include air superiority, fighter escort, suppression of enemy air defenses, reconnaissance, forward air control, close and deep air support, day and night strike missions, and aerial refueling. The F/A-18E is a single-seat version of the aircraft and the F/A-18F is a two-seat version. The F/A-18E/F Super Hornet replaces the F-14 and F/A-18A-D, and complements the F-35C, as a strike-fighter tactical aircraft employed by Navy carrier strike groups. The SCS is the higher-order aircraft language software that the Navy historically updates on a two-year cycle to further enhance F/A-18E/F capabilities.

Program

The F/A-18E/F Super Hornet is an Acquisition Category IC program. In 2021, DOT&E approved the Test and Evaluation Master Plan for the latest software update, SCS H16, covering both Block II and Block III aircraft. DOT&E approved the first phase of the Block II SCS H16 Test Plan in May 2021. DOT&E also approved a phased entry into Block II SCS H16 FOT&E, requiring the Navy to seek DOT&E approval for subsequent phases as software deficiencies resulting from developmental challenges are resolved. Operational testing of Block II SCS H16 aircraft began in June 2021, with fleet release expected in 3QFY22.

The Navy is also leveraging production of the Kuwaiti Super Hornet to purchase Block III aircraft that include upgraded hardware, advanced cockpit displays, and improved networking capability. Boeing delivered the first two Block III Super Hornets to the Navy in 2021. The Navy also plans to retrofit existing Block II aircraft with the Block III upgrades. Block III operational testing is scheduled to begin by 3QFY22.

Major Contractors

- The Boeing Company, Integrated Defense Systems – St. Louis, Missouri.

- Raytheon Company – Forest, Mississippi.
- General Electric Aviation – Evendale, Ohio.
- Northrop Grumman Corporation – Bethpage, New York.
- Lockheed Martin – Orlando, Florida.

Test Adequacy

The Navy started the Block II SCS H16 operational testing in June 2021. In accordance with the DOT&E-approved test plan, the Navy will collect data against continuous response variables instead of relying on binary response data to provide a more robust evaluation of Super Hornet performance in all environments, while facilitating an assessment of the capability improvements' effect on performance compared to previous SCS releases.

DOT&E approved the SCS H16 operational cybersecurity test plan in May 2021, noting that future iterations of cybersecurity test plans for the air system (both air vehicle and logisitics support) must be more comprehensive.

The Navy has not yet completed the long-standing requirement to conduct end-to-end multiple simultaneous AIM-120 missile engagements to demonstrate that the active electronically-scanned array (AESA) radar can support this required capability. This is planned for in the DOT&E-approved Block II SCS H16 test plan.

A long-standing limitation to F/A-18E/F operational testing has been the lack of a real-time, high-fidelity kill-removal system. The DOD continues to incorporate Open Air Battle Shaping into multiple CONUS ranges and fighter aircraft, to include those utilized by naval aviation OT&E. Efforts are underway to continue integration and updates to Open Air Battle Shaping in H18 and all future F/A-18E/F software releases, which will address this limitation. Utilization of Open Air Battle Shaping will enhance the realism of current and future high-fidelity AESA threat radar emulators while providing critical data from open-air, mission-level testing for use in verification, validation, and accreditation of modeling and simulation solutions.

The Navy simultaneously executed developmental test events involving F/A-18E/F SCS H16, IRST Block II, and E-2Ds with Delta System Software Configuration 4 software during the August 2021 Gray Flag detachment. Although no operational testing data were gleaned, this system of systems approach is likely to maximize the effectiveness and efficiency of future test events.

Performance

Effectiveness

Past effectiveness evaluations concluded that the Super Hornet is operationally effective in most environments. The SCS H16 operational test will evaluate new and enhanced F/A-18E/F capabilities. The limited SCS H16 testing conducted thus far does not appear to change the SCS H14 effectiveness evaluation. Final assessment of Block II SCS H16 operational effectiveness will be published in the Block II SCS H16 FOT&E report in 2022, after the completion of operational testing.

Suitability

Past evaluations concluded that the Super Hornet is operationally suitable, even though the F/A-18E/F's AESA radar has not met reliability requirements. While radar reliability has gradually improved across FOT&E periods, it still fails to meet the reliability requirement established in the Operational Requirements Document. Final assessment of Block II SCS H16 operational suitability will be published in the Block II SCS H16 FOT&E report in 2022, after the completion of operational testing.

Survivability

The Navy is leveraging completed developmental cybersecurity testing to inform the evaluation of Block II SCS H16 survivability in a cyber-contested environment. Additional SCS H16 cybersecurity testing was delayed due to hardware delivery and resource constraints. The Navy has not yet adequately addressed previous cybersecurity deficiencies or developed a comprehensive roadmap to inform future cybersecurity testing.

Recommendations

The Navy should:

1. Continue to improve the reliability of the AESA radar.
2. Allocate adequate resources for planning and conducting comprehensive F/A-18E/F cybersecurity operational testing and address previously identified cybersecurity deficiencies.
3. Incorporate Open Air Battle Shaping and high-fidelity AESA threat radar emulators into future test events, to include for SCS H18 FOT&E.
4. Plan and resource end-to-end testing employing multiple AIM-120 missiles.
5. Continue to utilize more robust data collection and analysis methods during operational test events, to include aircraft instrumentation and the use of continuous variables, in order to more adequately assess F/A-18 capability in the rapidly evolving threat environment.

FFG 62 *Constellation* Class – Guided Missile Frigate

The Constellation Class – Guided Missile Frigate (FFG 62) LFT&E program is currently conducting Phase 1 survivability testing to support model development and validation. This testing, along with completion of modeling and simulation (M&S) plans and validation, expected in 2022, supports an initial survivability assessment of the FFG 62 design. The Navy intends to conduct an early operational assessment of the FFG 62 program in 2QFY22.

System Description

The FFG 62 is a new multi-mission surface combatant intended to operate in complex operational environments with capability to conduct air warfare, anti-submarine warfare, surface warfare, electronic warfare/information operations, and intelligence, surveillance, and reconnaissance missions. The FFG 62 will be smaller and less capable than U. S. Navy destroyers and cruisers, but will have more offensive capability and survivability than previous small surface combatants (e.g., Littoral Combat Ships).

Program

The FFG 62 is an Acquisition Category IB Major Defense Acquisition Program intended to meet the Navy's Small Surface Combatant requirement. The Navy approved the FFG 62 program to enter the acquisition process at Milestone B on November 8, 2018. Having completed the statutory requirements, the Navy approved Milestone B on April 29, 2020. Concurrently, the Navy approved the award of the Detail Design and Construction contract for the first ship, with options for up to ten additional ships, and entry into the Detail Design and Construction (Production) phase with a low-rate initial production quantity of twenty ships. The Navy intends to conduct a Critical Design Review by March 2022, and deliver the lead ship by September 2026.

In June 2020, DOT&E approved the FFG 62 Test and Evaluation Master Plan with the exception of the strategy for testing its anti-air warfare mission capability. The Navy and DOT&E are working together to develop an adequate strategy to test this capability.

DOT&E approved the FFG 62 LFT&E Strategy in April 2020. The FFG 62 LFT&E Strategy includes full-ship shock trials with the option of pursuing an M&S-based shock trial alternative. In coordination with the DOT&E, the Navy will need to first validate M&S as adequate to address LFT&E shock trial objectives.

Major Contractor

Fincantieri Marinette Marine Corporation – Marinette, Wisconsin.

Test Adequacy

In FY21, the Navy conducted the Phase I survivability test program, in accordance with DOT&E-approved test plans, providing adequate data to support M&S development and validation even though this phase did not evaluate specific FFG 62 structure.

The first tests in the test program were a series of Extended Distance Multiple Plate ballistic tests in which fragment simulators and bullets were fired at an array of offset metal plates to record penetration, break-up, residual mass, and residual velocity.

The second test series investigated near-contact underwater explosions against surrogate ship structure in which a series of small charges were detonated in close proximity to stiffened metal plates at offsets that would generate holing.

Effectiveness

The Navy conducted no operational testing in FY21. The Navy intends to conduct an early operational assessment of the FFG 62 program in 2QFY22.

Suitability

The Navy conducted no operational testing in FY21. The Navy intends to conduct an early operational assessment of the FFG 62 program in 2QFY22.

Survivability

The Navy remains in development of the Detail Design Survivability Assessment Report M&S Plan to include verification and validation plans for specific M&S codes following completion of the Phase I survivability testing. COVID-19 delayed classified work in FY21. These efforts intend to support the Detail Design Survivability Assessment Report scheduled to be delivered in FY25.

The Navy compared the results of the Extended Distance Multiple Plate ballistic tests to available computer modeling techniques to assess M&S adequacy and determine M&S modification requirements. The results of these tests showed good correlation with existing penetration models for some metrics, but also showed a need for M&S improvement in others.

Analysis of the near-contact underwater explosion tests is in progress. DOT&E expects a report in FY22.

Recommendation

1. The Program Office PMS 515 should generate the Detail Design Survivability Assessment Report M&S Plan and individual M&S validation plans in accordance with the FFG 62 LFT&E strategy.

LHA 6 Flight 1 (LHA 8) Amphibious Assault Ship

The LHA 6 Flight 1 (LHA 8) operational assessment, conducted from October 20 through November 19, 2020, indicated that the LHA 8 well deck adds needed capability to launch and recover surface connectors. The LHA 8 design, however, includes several design features that could negatively affect operational effectiveness of the LHA Flight 1 ships if not mitigated prior to ship delivery expected in FY25. The survivability of the LHA 8 to air-delivered and underwater threats will remain unknown unless the Navy plans, funds, and executes an adequate LFT&E strategy.

System Description

The USS *America* LHA 6 class are large-deck amphibious assault ships intended to provide transportation and operational support for deployed Marine Corps forces, to include the F-35B Joint Strike Fighter, the AV-8B, the MV-22, the CH-53, the AH-1, the UH-1, and the H-60 squadrons, as well as the Marine Air Ground Task Force (MAGTF). The LHA 6 Flight 1 variant, LHA 8 and beyond, adds a well deck capable of deploying two Landing Craft Air Cushion hovercraft. The LHA 8 will serve as the primary command ship and aviation platform for an Amphibious Ready Group equipped with the Ship Self-Defense System, the primary control and decision system that integrates air search radars, trackers, an electronic warfare system, and hard-kill and soft-kill weapons to provide self-defense against anti-ship cruise missiles (ASCMs).

Program

The LHA 6 program (formerly the LHA (R) program) is an Acquisition Category IC program. The Navy completed the LHA 6 Flight 0 IOT&E in December 2017. From October to November 2020, the Navy and Marine Corps conducted an operational assessment intended to solicit fleet operator feedback on the LHA 6 Flight 1 design and its potential effect on operational effectiveness and suitability of the delivered ship. The Navy expects to deliver a Test and Evaluation Master Plan revision for DOT&E approval in FY22, detailing the OT&E and LFT&E requirements for the LHA 6 Flight 1. The first LHA 6 Flight 1 ship, USS *Bougainville* (LHA 8), is expected to be delivered in FY25. The LHA 6 Flight 1 FOT&E will begin following ship delivery.

The Navy agrees an unmanned test asset is required to adequately and safely test the self-defense capability of LHA 8 against ASCM surrogates. The Navy committed to providing the resources required to retain this capability via a planned maintenance availability of the Self-Defense Test Ship (e.g., *Paul F. Foster*), as well as the procurement and installation of the necessary LHA 8 combat system elements on this test ship.

Major Contractors

- LHA 8: Huntington Ingalls Industries, Ingalls Shipbuilding Division – Pascagoula, Mississippi.
- Ship Self-Defense System: Lockheed Martin – Moorestown, New Jersey.
- Enterprise Air Surveillance Radar (EASR): Raytheon Missiles and Defense – Marlborough, Massachusetts.
- RAM Block 2A and ESSM Block 1 missiles: Raytheon Missiles and Defense – Tucson, Arizona.
- Cooperative Engagement Capability (CEC): Raytheon – St. Petersburg, Florida.
- Surface Electronic Warfare Improvement Program Block 2 (SEWIP Block 2): Lockheed Martin – Syracuse, New York.

Test Adequacy

The Navy and Marine Corps conducted an operational assessment of the LHA 8 ship design between October 20 and November 19, 2020 in accordance with DOT&E-approved test plans. During the three, 3-day events, subject matter experts in operations and maintenance reviewed the LHA 8 design to identify risks that could affect operational effectiveness and suitability. The operational assessment also informed operational testers on the required FOT&E scope and design.

The Navy does not yet have a well-defined LFT&E plan required to evaluate the survivability of the LHA 8 to air delivered or underwater kinetic threats.

Performance

Effectiveness

Not enough data are yet available to provide a preliminary assessment of the LHA 8 operational effectiveness due to the ship's stage of development. Operational assessment of the LHA 8 design indicated that the well deck adds needed capability to launch and recover surface connectors, but several design features could negatively affect operational effectiveness of the LHA Flight 1 ships. Additional details are summarized in the classified DOT&E LHA 6 Flight 1 Operational Assessment report published in September 2021.

Suitability

Not enough data are yet available to provide a preliminary assessment of the LHA 8 operational suitability due to the ship's stage of development. The LHA 8 operational assessment could not measure reliability, maintainability, or availability of LHA 8. Final assessment of LHA 8 operational suitability will be published after the completion of the LHA 8 FOT&E.

Survivability

The Navy has initiated the vulnerability modeling of the LHA Flight 1 design, but no relevant data are yet available to assess ship survivability either against kinetic or cyber threats.

Recommendations

The Navy should:

1. Validate the sufficiency of modified ship-space following operational assessment to support Marine Corps Tier-2 equipment.
2. Conduct land-based operational testing of the LHA 8 combat system to ensure the system is mature enough for at-sea operational test of the platform, and test EASR's electronic protection capability.
3. Continue to fund the maintenance availability for the current Self-Defense Test Ship (e.g., *Paul F. Foster*) to ensure its readiness to support LHA 8 combat system testing.
4. Continue to fund the procurement and installation of the necessary LHA 8 combat system elements on Self-Defense Test Ship.
5. Develop FOT&E test plans informed by the LHA 8 operational assessment.
6. Evaluate all recommendations in the DOT&E Operational Assessment report published in September 2021.
7. Develop an adequate LFT&E strategy to assess ship survivability of the LHA 6 Flight 1 ships, including the survivability of the ship to lethal, underwater threat-induced shock effects.

Littoral Combat Ship (LCS)

Preliminary assessments indicate that the *Independence* variant of the Littoral Combat Ship (LCS) with the Surface Warfare (SUW) Increment 3 mission package (MP) is operationally effective, demonstrating the capability to defeat small boats in a simultaneous attack. Both LCS seaframe variants remain operationally unsuitable due to previously observed low reliability and availability caused by propulsion failures. The LCS survivability is challenged in a contested environment against selected kinetic threat types, and the survivability of the LCS variants in a cyber-contested environment is currently unknown.

System Description

The LCS is a small surface vessel designed for operation in littoral, shallow waters while also capable of open-ocean operations. The LCS comprises two seaframe variants: the *Freedom* variant and the *Independence* variant. The *Freedom* variant is a 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 is an aluminum trimaran with two steerable waterjets driven by diesel engines and two steerable waterjets driven by gas turbine engines. LCS seaframes host and derive mission capability from the SUW, Mine Counter Measure (MCM), and Anti-Submarine Warfare (ASW) MPs.

The SUW MP derives capability from the following components:

- Two Mk 46 30mm guns
- MH-60R or MH-60S helicopter
- MQ-8 Fire Scout unmanned air vehicle
- Two 11-meter rigid-hull inflatable boats
- 24 Longbow Hellfire missiles or Surface-to-Surface Missile Module (SSMM)

The MCM MP derives capability from the following components:

- AN/ASQ-235 Airborne Laser Mine Detection System
- AN/AQS-20C mine hunting sonar
- Knifefish Block I unmanned undersea vehicle (post MCM MP IOT&E capability)
- AN/DVS-1 Coastal Battlefield Reconnaissance and Analysis (COBRA) Block 1
- Airborne Mine Neutralization System
- Barracuda Mine Neutralization System (post MCM MP IOT&E capability)

- Unmanned Influence Sweep System

The ASW MP derives capability from a combined variable depth sonar and multi-function towed array to detect, classify, and localize a threat submarine, and from Mk 54 torpedoes deployed from an MH-60R helicopter to destroy threat submarines. The LCS platform baselines also intend to include a newly developed Light Weight Tow to improve LCS survivability against an incoming threat torpedo, but the Navy has yet to fund its development or installation.

Program

The LCS seaframes and its separate mission packages are Acquisition Category IC programs. Components of the mission packages are individual programs of record. DOT&E approved an update to Revision B of the LCS Test and Evaluation Master Plan (TEMP) in 2018 that accounted for testing of the three mission packages and the two seaframe variants. This led to SUW MP Increment 3 testing that supported initial operation capability of the SSMM in March 2019 and a subsequent purchase authorization of the SUW MP Increment 3 in August 2019. The Navy intends to update the TEMP to incorporate changes to previously identified testing required for the MCM and ASW MP IOT&E in support of their beyond low rate production. The schedule for the TEMP update, IOT&E, and production decision continues to fluctuate. The Navy is under contract for all remaining builds of the two LCS seaframes.

Major Contractors

- Lockheed Martin and Fincantieri Marinette Marine – Marinette, Wisconsin.
- Austal USA – Mobile, Alabama.
- Northrup Grumman – Falls Church, Virginia.

Test Adequacy

The FY20 integrated tests were sufficient to determine the performance of the SUW Increment 3 MP on the *Independence* variant. Test results showed significantly less variability in performance than anticipated, enabling DOT&E to approve the removal of two events and saving approximately $11 million in test resources.

In FY21, the Navy tested the Unmanned Influence Sweep System from the *Independence* variant of the LCS in accordance with the DOT&E-approved test plan. Details are in the Unmanned Influence Sweep System section of this report.

In FY21, the Navy continued hydrodynamic testing of the variable depth sonar and multi-function towed array following modifications intended to improve dynamic stability at higher speeds and affect operational effectiveness of the LCS with the ASW MP. Consequently, the Navy has not yet started the operational testing on an LCS platform with the ASW MP.

In FY21, the Navy started evaluating the survivability of the full set of LCS variants and MP combinations in a cyber-contested environment. The Navy intends to conduct a Coordinated Vulnerability and Penetration Assessment and an Adversarial Assessment for the following three combinations: 1) the LCS *Freedom* variant with SUW MP in 1QFY22, 2) the LCS *Independence* variant with ASW MP, not yet scheduled, and 3) the first available variant with MCM MP, not yet scheduled. If post-test analysis determines that there are interface differences that remained untested, the Navy will need to schedule up to three additional evaluations identified in the Revision B TEMP to assess the survivability of the remaining combinations of the LCS variants and MPs.

The LCS LFT&E assessment of the survivability of both LCS variants against air-delivered and underwater threats, and the lethality of the SSMM weapons, concluded in late 2019.

Performance

Effectiveness

Preliminary assessment indicates that the *Independence* variant with the SUW Increment 3 MP is operationally effective, demonstrating the capability to defeat small boats in a simultaneous attack represented with the Navy's expendable high-speed maneuvering surface target. The capability against more stressing operationally representative small boats could not be evaluated due to the limitations of existing surface targets. Testing highlighted problems that required operators to shift to an alternate defense mode.

The modeling and simulation results of the SSMM, the Army-developed Longbow Hellfire Missile will be provided in the SUW Increment 3 MP on the *Independence* variant report expected to be published in 2QFY22.

Not enough data are currently available to assess the operational effectiveness of either the ASW MP or MCM MP and their components. Preliminary assessments indicate that the Navy must overcome several challenges to reduce the risk to meeting operational effectiveness requirements.

Suitability

Both LCS seaframe variants remain operationally unsuitable due to low reliability and availability caused by propulsion failures, detailed in the LCS *Independence* variant with SUW Increment 2 report in FY16 and the LCS *Freedom* variant with SUW Increment 3 report in 3QFY20. The Navy will continue to measure platform reliability and availability during all remaining test events to determine if the most significant reliability concerns have been resolved.

Preliminary assessments indicate that the SUW Increment 3 MP is suitable, pending the resolution of seaframe reliability and availability. The SSMM, part of the SUW MP Increment 3, experienced no reliability or availability failures during testing. The Mk 50 30mm guns, consistent with prior evaluations, are sufficiently reliable and available.

Not enough data are yet available to assess the suitability of either the ASW MP or the MCM MP and their components. However, the reliability and availability of the Unmanned Influence Sweep System and the launch and recovery systems on the LCS introduce risk to the operational suitability of the MCM MP.

Survivability

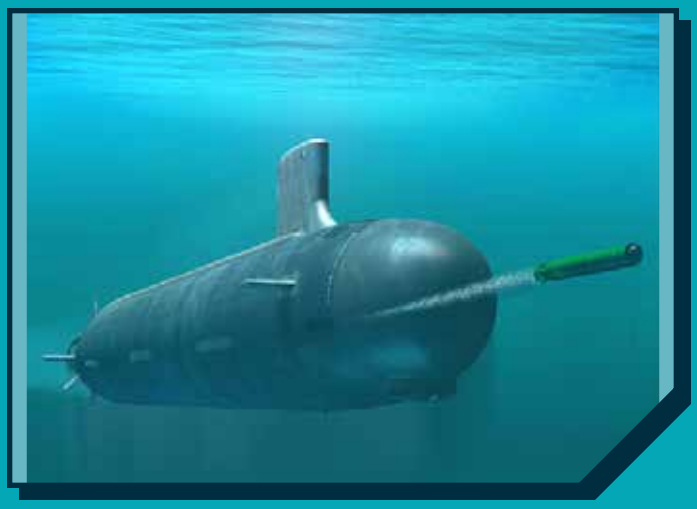
LFT&E analysis highlighted several LCS design features that drive survivability performance of each Variant against selected kinetic threat categories. Not enough data are yet available to assess the survivability of the LCS variants with any of the MPs in a cyber-contested environment.

Recommendation

1. The Navy should develop expendable and credible small boat target surrogates capable of achieving higher speeds to determine the operational effectiveness of the LCS with the SUW MP in a more stressing operational environment.

Mk 48 Torpedo Modifications

Based on the demonstrated performance in IOT&E, completed in September 2021, the Mk 48 torpedo with Advanced Processor Build 5 (APB 5) software is operationally effective and suitable. The APB 5 torpedo provides additional capability to acquire surface ships while maintaining the previously demonstrated performance when acquiring submarines. The APB 5 torpedo is vulnerable in a cyber-contested environment.



In November 2020, the Navy started FOT&E of the next torpedo variant, the APB 5+ torpedo. Limited availability of test assets to support FOT&E presents a risk of significant delay to APB 5+ initial operational capability.

System Description

The Mk 48 heavyweight torpedo is the only anti-submarine and the primary anti-surface ship weapon used by U.S. submarines and designed to defeat all threat surface ships and submarines in all ocean environments.

The latest improvement to the Mk 48 torpedo, the APB 5, is intended to improve the torpedo's ability to detect and classify threat submarine and surface ships. A follow-on improvement, APB 5+, is intended to transfer targeting functions from the submarine combat system to the torpedo, improve the operator interface with the torpedo, and provide the torpedo with higher data exchange rates.

Program

The Mk 48 heavyweight torpedo was first fielded in 1972. The current, Mk 48 Mod 7 torpedo variant, a shared development effort with the Royal Australian Navy, is an Acquisition Category III program, first fielded in 2008. The Navy has since made improvements to the Mk 48 Mod 7 through incremental APB software releases that may include minor hardware updates (e.g., upgraded processors and modified interfaces).

The Navy started APB 5 IOT&E of Mk 48 Mod 7 torpedoes in August 2018 with focus on Anti-Submarine Warfare (ASW) performance. This allowed the Navy to declare early operational capability in May 2019 and deliver upgraded ASW capability for use against submarines and surface ships.

In 2020, the Navy started developmental testing of APB 5+. The Navy intends to submit the APB 5+ update to the TEMP for DOT&E approval in 1QFY22. The APB 5+ in-water FOT&E is scheduled for FY22. Limited availability of test assets to support FOT&E presents a risk of significant delay to APB 5+ initial operational capability.

Major Contractor

Lockheed Martin Sippican Inc. – Marion, Massachusetts.

Test Adequacy

In September 2021, the Navy concluded the APB 5 IOT&E that started in 2018, resulting in 193 total at-sea torpedo firings as compared to the planned 127. Specifically, in FY21, the Navy completed six at-sea torpedo firings and 216 torpedo-simulated engagements in the Environment Centric Weapons Analysis Facility (ECWAF). While the Navy executed 66 more at-sea torpedo firings than planned, the Navy did not conduct the planned number of at-sea torpedo firings under certain specified conditions due to: 1) limited availability of submarines to support testing in test locations with desired environmental conditions, 2) prioritization of Fleet events that limited data collection in some scenarios, and 3) prioritization of free-play events. While testing was not conducted in accordance with DOT&E-approved test plans, sufficient data were collected to assess operational effectiveness, suitability, and survivability of the APB 5 torpedo in most scenarios. The Navy committed to collecting data in untested scenarios in future test events since limited data from at-sea torpedo firings in a specific ocean environment could affect the validation of the ECWAF. The Navy intends to conduct at-sea torpedo firings in the required ocean environment during the APB 5+ torpedo FOT&E in FY22. If the Navy is able to accredit the ECWAF as a representative test environment against both surface ships and submarines, at-sea torpedo firings for a follow-on variant, APB 6, could decrease by approximately 50 percent.

The Navy is upgrading mobile countermeasure surrogates to better emulate modern threat countermeasures and may defer APB 5 countermeasure testing to APB 6 torpedo testing, when this new test capability is expected to be available.

The Navy also conducted two integrated (developmental and operational) test events for the APB 5+ torpedo in November 2020 and March 2021 in accordance with a DOT&E-approved data collection plan.

Performance

Effectiveness

Preliminary analysis suggests the new APB 5 tactics provide operationally significant effectiveness against surface ships while maintaining previous performance using legacy tactics. Anti-Submarine Warfare tactics improved performance against some combinations of scenarios and environments. A final assessment of APB 5 torpedo operational effectiveness will be published in a classified IOT&E report in 2QFY22.

Not enough data is yet available to provide a preliminary assessment of the APB 5+ torpedo operational effectiveness. The integrated test events thus far demonstrated that APB 5+ torpedo has simplified operator control of the torpedo.

Suitability

The APB 5 torpedo is operationally suitable demonstrating adequate reliability, availability, and maintainability.

Not enough data are yet available to provide a preliminary assessment of the APB 5+ torpedo operational suitability.

Survivability

APB 5 is vulnerable in a cyber-contested environment. Specific vulnerabilities and their effect on warfighting capability will be published in the classified APB 5 torpedo IOT&E report in 2QFY22.

Recommendations

The Navy should:

1. Address the recommendations in the classified 2019 DOT&E Early Fielding Report.
2. Complete development and validation of surface ship models in the ECWAF to support the operational assessment of the APB 6 torpedo.
3. Collect torpedo performance data with upgraded surrogate countermeasures, in APB 6 testing.
4. Ensure the availability of test assets to complete the APB 5+ FOT&E and support the initial operational capability.

Mk 54 Lightweight Torpedo Upgrades Including the High Altitude Anti-Submarine Warfare Weapon Capability (HAAWC)

The High Altitude Anti-Submarine Warfare Weapon Capability (HAAWC) is operationally effective, demonstrating the capability to accurately deliver the Mk 54 torpedo, from the P-8A, to the intended entry point, as assigned by the P-8A combat system. The HAAWC is not operationally suitable, and is vulnerable in a cyber-contested environment. The Navy expects HAAWC to enter full-rate production in FY22.

While the Navy completed additional torpedo firings in FY21 to advance Mk 54 Mod 1 torpedo IOT&E objectives, test unit and test range availability may challenge the completion of IOT&E and initial operational capability.

System Description

The Mk 54 lightweight torpedo is the primary anti-submarine weapon employed from U.S. surface ships, aircraft, and helicopters. Surface ships employ the Mk 54 from surface vessel torpedo tubes as a reactionary weapon against very close threat submarines and as a vertically launched anti-submarine rocket (VLA) for offensive attack against threat submarines. The Navy developed the Mk 54 to defeat all types of threat submarines in all ocean environments. When fixed to an Air Launch Accessory (ALA) wing kit, the Mk 54 torpedo can also be released from the P-8A Poseidon from higher altitudes than conventional employment. This Mk 54 – ALA configuration is termed HAAWC. The ALA glides the Mk 54 down to an acceptable altitude and then releases the torpedo to an intended torpedo entry point assigned by the aircraft's combat system.

Program

The Mk 54 is an Acquisition Category III program first fielded in 2004. The Navy has since been developing and delivering incremental modifications of the Mk 54 torpedo variants. In 2007, the Navy upgraded the sonar array for the Mk 54 Mod 1 torpedo variant, as well as the torpedo logic, to provide a clearer picture of the intended target within the undersea environment. The Mk 54 Mod 1 torpedo also incorporates the Advanced Processor Build 5 software that was developed and evaluated within the Mk 48 heavyweight torpedo program. The Navy intends to deliver the Mk 54 Mod 1 torpedo in two increments: the Mk 54 Mod 1 Increment 1 is in test, and the Mk 54 Mod 1 Increment 2 is scheduled to be delivered in FY26 with additional software-driven features. The Navy started the Mk 54 Mod 1 Increment 1 IOT&E in December 2019 with the plan for reaching initial operational capability in 4QFY22. The initial operational capability, scheduled for 4QFY22, is at high risk due to the limited

availability of test assets and range locations required to complete IOT&E. The Navy has not approved the Mk 54 Mod 1 torpedo for use in VLA.

HAAWC entered Milestone C in December 2018. The Navy completed IOT&E in January 2021 in support of the full-rate production decision expected in 2QFY22. The Navy is updating the HAAWC software to address deficiencies identified in IOT&E. The upgraded software, operational flight program (OFP) 3.5, will be evaluated in FOT&E, expected to start in 2QFY22. The Navy intends to deliver the FOT&E Test and Evaluation Master Plan in FY22 for DOT&E approval.

Major Contractors

- Raytheon Integrated Defense Systems – Tewksbury, Massachusetts.
- Progeny Systems Corporation – Manassas, Virginia.
- Boeing Company – St. Charles, Missouri.

Test Adequacy

In FY21, the Navy continued to execute the Mk 54 Mod 1 IOT&E that started in December 2019. In May 2021, the Navy conducted additional Mk 54 Mod 1 Increment 1 torpedo firings needed to advance IOT&E. Testing was conducted in accordance with DOT&E-approved test plans. While the Navy reports challenges to obtaining fleet assets to support operational testing of the Mk 54 Mod 1 torpedo, they still project to complete Mk 54 Mod 1 Increment 1 IOT&E by the end of FY22.

In May 2019, the Navy executed the Mk 54 Mod 1 Cooperative Vulnerability and Penetration Assessment and the Adversarial Assessment in accordance with DOT&E-approved test plans.

In March 2021, the Navy completed HAAWC IOT&E. Testing, conducted in accordance with DOT&E-approved test plans, was adequate to determine HAAWC operational effectiveness, suitability, and survivability.

Performance

Effectiveness

Not enough data are yet available to provide a preliminary assessment of the Mk 54 Mod 1 torpedo operational effectiveness to intercept threat submarines.

The HAAWC is operationally effective. HAAWC has demonstrated the capability to accurately deliver the Mk 54 torpedo to the intended entry point, as assigned by the P-8A combat system. The Navy restricted HAAWC release to a temporary threshold due to performance limitations below this altitude, precluding the assessment of the HAAWC release at the Navy's minimum altitude requirement for HAAWC. The Navy also restricted the release airspeed to a temporary threshold, precluding the assessment of HAAWC at the maximum calibrated airspeed within the intended operating envelope for HAAWC release. While the Navy cannot employ the HAAWC from the full range of intended release altitudes, the available range of release altitudes provide an enhanced operational capability. Details are summarized in the classified HAAWC IOT&E report published in July 2021.

Suitability

Preliminary assessment thus far has not highlighted any significant risks to the Mk 54 Mod 1 meeting operational suitability requirements.

The HAAWC is not suitable due to a demonstrated ALA reliability issue. The Navy completed the root cause analyses and implemented OFP 3.5 fixes intended to improve ALA reliability. These fixes will be verified in the HAAWC FOT&E scheduled for FY22.

Survivability

Mk 54 Mod 1 is vulnerable in a cyber-contested environment. The specific vulnerabilities and their effect on warfighting capability will be detailed in the Mk 54 Mod 1 IOT&E report intended to support the initial operational capability decision.

HAAWC is vulnerable in a cyber-contested environment. The specific vulnerabilities and their effect on warfighting capability are detailed in the

classified HAAWC IOT&E report published in July 2021.

Recommendations

The Navy should:

1. Secure the test assets and test ranges required to complete IOT&E of Mk 54 Mod 1 Increment 1 and mitigate the risk to declaring initial operational capability scheduled for 4QFY22.
2. Address all recommendations outlined in the classified HAAWC IOT&E report.
3. Provide the HAAWC Test and Evaluation Master Plan for DOT&E approval prior to OFP 3.5 FOT&E.

MQ-4C Triton

In December 2020, the Navy restructured the MQ-4C program to enable the delivery of incremental capabilities in support of the EP-3E retirement. The Navy intends to field the first increment, designed to deliver signals intelligence (SIGINT) capability, as an initial operational capability. The contractor and developmental test schedules have little margin for contingencies prior to operational testing and the fielding decision.

System Description

The MQ-4C Triton is a high-altitude, long-endurance intelligence, surveillance, and reconnaissance unmanned aircraft intended to support global naval operations by collecting, processing, and distributing target track data, signals intelligence, and imagery intelligence data to fleet tactical operation centers and intelligence exploitation sites. Commanders will employ the MQ-4C to provide persistent maritime surveillance to detect, classify, identify, track, and assess maritime and littoral targets in support of surface warfare, intelligence operations, strike warfare, maritime interdiction, amphibious warfare, homeland defense, and search and rescue missions.

Program

The MQ-4C Triton is an Acquisition Category IC program and a critical component of the Navy's Maritime Intelligence, Surveillance, Reconnaissance, and Targeting (MISR&T) transition plan to retire the EP-3E Aries II aircraft in accordance with the requirements in Section 112 of the FY11 National Defense Authorization Act. DOT&E approved Revision D of the Test and Evaluation Master Plan (TEMP) in January 2017.

The Navy restructured the program into an incremental development approach. The first increment is designed to deliver SIGINT capability sufficient to support the MISR&T transition plan. The Navy intends to field this increment as an initial operational capability. Updates to the Acquisition Program Baseline, Acquisition Strategy, Capability Development Document, and TEMP are ongoing.

Major Contractor

Northrop Grumman Aerospace Systems, Battle Management and Engagement Systems Division – Rancho Bernardo, California.

Test Adequacy

The program started developmental flight test using a prototype, initial operational capability configuration in July 2021. The current schedule for the contractor and developmental test program provides little margin for discovery and correction of deficiencies before operational testing.

Performance

Not enough data are currently available to provide a preliminary assessment of the MQ-4C operational effectiveness, suitability, and survivability.

Recommendation

1. The Navy should restore more margin in the developmental test schedule to allow for the discovery and correction of deficiencies prior to operational testing.

MQ-8 Fire Scout Unmanned Aircraft System (UAS)

In April 2021, the Navy started the FOT&E of the MQ-8C Surface Warfare Increment but the test was delayed due to a Fleet-wide operational pause of MQ-8B and MQ-8C flights from Navy vessels.

System Description

The MQ-8C is a helicopter-based tactical unmanned aerial system designed to support intelligence, surveillance, and reconnaissance, surface warfare, and mine countermeasures payloads. The air vehicle is a modified Bell 407 airframe intended to support Littoral Combat Ship (LCS) missions, but can also operate from other suitably equipped ships.

Program

The MQ-8 Fire Scout is an Acquisition Category IC program that entered Milestone C in 2QFY17. The MQ-8C has three expected increments of capability: the Endurance Baseline Increment, Surface Warfare Increment, and Mine Countermeasures Increment. The Navy accepted 38 Endurance Baseline Increment MQ-8Cs and has no additional procurement planned.

Major Contractor

Northrop Grumman – San Diego, California.

Test Adequacy

In FY21, the Navy conducted land-based testing of the Surface Warfare Increment that included overland surveillance, intelligence gathering, and maritime search and surveillance. The land-based test phase will inform the evaluation of the AN/ZPY-8 radar's ability to provide actionable radar images and location for overland contacts of interest, as well as the radar's ability to detect, track, classify, and localize maritime contacts.

In April 2021, the Navy started the Surface Warfare Increment FOT&E as employed from an LCS. The test was delayed due to problems detailed in the Controlled Unclassified Information edition of this report. The Navy

intends to resume FOT&E following the resolution of those problems.

Performance

Effectiveness

Not enough data are yet available to provide a preliminary assessment of the Surface Warfare Increment of MQ-8C operational effectiveness as employed from an LCS.

Suitability

Not enough data are yet available to provide a preliminary assessment of the Surface Warfare Increment of MQ-8C operational suitability as employed from an LCS.

Survivability

Not enough data are yet available to provide a preliminary assessment of the Surface Warfare Increment of MQ-8C survivability in a cyber-contested environment. The Navy has been leveraging development test and evaluation results to prepare the MQ-8C for a Cooperative Vulnerability and Penetration Assessment and an Adversarial Assessment that will occur after a new software release.

Recommendations

The Navy should:

1. Resolve problems that delayed FOT&E to successfully resume and complete FOT&E.
2. Complete operational testing of the Surface Warfare Increment of MQ-8C prior to deployment on LCS.

Next Generation Jammer Mid-Band (NGJ-MB)

The Navy Milestone Decision Authority approved the Next Generation Jammer Mid-Band (NGJ-MB) to proceed through Milestone C without completing the planned Capabilities Based Test and Evaluation period.

The Navy needs to overcome several challenges to demonstrate the NGJ-MB's operational effectiveness and suitability as it proceeds to IOT&E. The lack of validated or accredited digital models needed to supplement NGJ-MB operational flight testing present a significant risk to NGJ-MB IOT&E. The Navy and contractor continue to develop the system to resolve performance problems.

System Description

The NGJ-MB is an airborne electronic attack system. It consists of two pods mounted under the EA-18G aircraft wings that integrate with the AN/ALQ-218 radio frequency receiver. Each pod contains four active electronically scanned arrays, which radiate over a band of frequencies, and a ram-air turbine that generates internal power. The NGJ-MB is the first of the three NGJ programs intended to engage multiple advanced threats at greater stand-off ranges, compared to the legacy AN/ALQ-99 Tactical Jammer System.

Program

The NGJ is an Acquisition Category IC program being acquired in three separate acquisition programs: Increment 1 (Mid-Band (MB)), Increment 2 (Low-Band (LB)), and Increment 3 (High-Band (HB)). These will eventually replace all of the legacy ALQ-99 Tactical Jammer System pods that have been developed and fielded since 1971 on the recently-retired EA-6B Prowler and are currently flown on the EA-18G Growler. In May 2021, the Secretary of the Navy approved the NGJ-MB program to move past Milestone C, thereby authorizing procurement of low-rate initial production (LRIP) pods. The LRIP pods are scheduled for delivery beginning in September 2023. The first System Demonstration Test Asset (SDTA) shipset that supports IOT&E, scheduled for 2QFY23, will be delivered in February 2022. DOT&E approved the Milestone C NGJ-MB Test and Evaluation Master Plan (TEMP) in November 2020.

Major Contractors

- Raytheon Space and Airborne Systems – El Segundo, California.
- The Boeing Company, Integrated Defense Systems – St. Louis, Missouri.
- Northrop Grumman Mission Systems – Linthicum, Maryland.

Test Adequacy

No operational testing has been conducted on the NGJ-MB system thus far. For Milestone C, the Navy used a combination of ground-based testing, mostly in anechoic chambers, and early developmental flight testing to assess NGJ-MB performance against the system specifications. Since the Navy did not accomplish the planned early operational tests, they moved these tests to a Capabilities Based Test and Evaluation period just prior to IOT&E. If the tests are not accomplished prior to IOT&E, then they will occur during IOT&E and likely extend the planned IOT&E schedule.

The Navy is in the process of developing an incremental operational test strategy intended to provide the data required for an adequate verification and validation of critical modeling and simulation (M&S) needed to supplement NGJ-MB operational flight testing. This approach has been neither fully developed and vetted by the Navy nor approved by DOT&E.

In May 2017, the Navy conducted a Cyber Table Top event for the NGJ-MB, but has not yet completed a Cooperative Vulnerability Identification event identified in the DOT&E-approved TEMP.

Performance

Effectiveness

The Navy needs to overcome several challenges to demonstrate the NGJ-MB's operational effectiveness as it proceeds to IOT&E. As of Milestone C, the NGJ-MB system has achieved several key performance parameters, but is still underperforming in several important areas. The NGJ-MB design is not expected to undergo any major hardware changes, so additional system development will occur mostly through software updates. The Navy continues to test the system both in laboratories and in flight.

The lack of validated or accredited digital models needed to supplement NGJ-MB operational flight testing present a significant risk to NGJ-MB IOT&E. The Navy has a plan for validation, but has been unable to collect the data necessary to validate the models. The operational test team determined operational test flights would need to begin in 3QFY22 to collect the necessary data for model validation and to have the time to complete all planned operational test events by the planned end of IOT&E. The Program Office stated that the SDTA pods will likely be delivered to the operational test team later than 3QFY22, which may not allow sufficient time to validate, accredit, and use the digital models to supplement the flight test data. In addition, test data classification problems have prevented M&S personnel from analyzing the data.

Suitability

The Navy needs to overcome several challenges to demonstrate the NGJ-MB's operational suitability as it proceeds to IOT&E. Preliminary analysis is highlighted in the Controlled Unclassified Information edition of this report.

Survivability

No data are currently available to inform the NGJ-MB's survivability in a cyber-contested environment or take actions to address any identified vulnerabilities.

Recommendations

The Navy should:

1. Revise the NGJ-MB schedule as necessary to ensure sufficient time for completion of the ship-based testing, large-force exercises, tests against advanced radar signal emulators, and other important test events needed to support an adequate IOT&E.
2. Develop and codify its incremental operational flight test strategy and demonstrate that it can provide information to support adequate operational testing and provide the data necessary to validate the required M&S.
3. Obtain required security clearances for operational test and M&S personnel so they can access the test facilities and data needed to support the validation and accreditation of digital M&S tools required to evaluate operational effectiveness.

4. Complete the Cooperative Vulnerability Identification event required in the TEMP to identify vulnerabilities in the NGJ-MB system and allow the program to prioritize vulnerability resolution. This will facilitate more effective Cooperative Vulnerability and Penetration, and Adversarial Assessments during IOT&E.

Offensive Anti-Surface Warfare (OASuW) Increment 1

The Offensive Anti-Surface Warfare (OASuW) Increment 1 program continues the development of missile hardware and software to increase targeting capabilities as an incremental upgrade to the currently fielded air-to-ground missile (AGM)-158C Long Range Anti-Ship Missile (LRASM). In March 2021, the program began developmental flight testing of the newest variant, LRASM 1.1, in preparation for operational testing and the declaration of early operational capability scheduled for FY23. In 4QFY21, the Navy also announced the pursuit of a dual OASuW and land strike capability in a planned modification to LRASM 1.1, scheduled to reach early operational capability in 4QFY24.

System Description

AGM-158C LRASM, the weapon system for the OASuW Increment 1, is a long-range, conventional, air-to-surface, precision-standoff weapon intended to be launched from the Navy's F/A-18E/F and the Air Force's B-1B aircraft. Once launched, LRASM uses an anti-jam GPS system to guide to an initial point and then employs a radio frequency sensor and an infrared sensor to locate, identify, and provide terminal guidance to the target.

Program

The OASuW Increment 1 began as an accelerated acquisition program to procure a limited number of air-launched missiles to meet the U.S. Pacific Fleet Urgent Operational Need generated in 2008. The OASuW program leveraged the Defense Advanced Research Projects Agency LRASM initiative that was derived from the Joint Air-to-Surface Standoff Missile Extended Range. As part of the OASuW Increment 1, the Navy funded an incremental upgrade to the LRASM baseline, referred to as LRASM 1.1, to bridge the gap until an OASuW Increment 2 program of record is established.

LRASM 1.1 incorporates missile hardware and software improvements to address component obsolescence and enhance targeting capabilities. The Navy intends to field LRASM 1.1 to operational units and declare early operational capability in 1QFY23 before the last integrated test shot and the operational test phase. DOT&E approved the LRASM 1.1 Master Test Strategy in January 2020.

In 4QFY21, the Navy announced the pursuit of a modification to LRASM 1.1, initially referred to as the LRASM C-2 and expected to be designated the AGM-158C2, intended to remove certain components to reduce unit cost and provide both OASuW and land strike capability. The Navy plans to conduct an integrated test shot for LRASM C-2 in 1QFY24 and reach early operational capability in 4QFY24.

The DOD continues to plan for OASuW Increment 2, with initial operational capability anticipated in FY28-30, intended to deliver long-term anti-surface warfare capabilities to counter future threats.

Major Contractor

Lockheed Martin Missiles and Fire Control – Orlando, Florida.

Test Adequacy

Developmental flight testing of LRASM 1.1 components on a Sabreliner flying test bed began in March 2021 and is scheduled to continue through January 2022. Integrated testing, scheduled to be executed from 2022 through 2023, will include test shots with inert warheads from F/A-18E/F aircraft at ship targets and modeling and simulation (M&S)-based testing. Operational testing scheduled for 2024 will include shots (including one with a live warhead), an M&S-based test event, and cybersecurity operational test events using a signal processor-in-the-loop lab environment. Live integrated and operational free-flight tests will provide validation data for the Navy Commander, Operational Test and Evaluation Force (COMOPTEVFOR) to accredit the M&S required to assess LRASM operational effectiveness across the operational environment. COMOPTEVFOR will complete verification, validation, and accreditation of the LRASM M&S suite by the end of IOT&E.

In 2021, the Navy conducted two sled tests of inert LRASM 1.1 warheads to assess proper function and survivability of the new Electronic Safe and Arm Fuze against representative maritime target components. Analysis is ongoing to determine if the collected data are adequate to demonstrate end-to-end warhead performance.

No LRASM C-2 operational test activity occurred in 2021. The Navy still needs to complete development of the LRASM C-2 requirements and concept of operations, as well an adequate OT&E plan to support their planned early operational capability declaration in 4QFY24 and a subsequent full-rate production decision. The Navy needs to ensure adequate M&S resources are available to develop and test the new LRASM C-2 land strike capability.

Performance

Not enough data are currently available to provide a preliminary assessment of LRASM operational effectiveness, lethality, suitability, and survivability. Developmental flight testing in 2021 provided data that will be used to improve targeting algorithms, which are likely to have the greatest effect on missile performance for both LRASM 1.1 and LRASM C-2.

Recommendations

The Navy should:

1. Complete the development and validation of the M&S environment to facilitate the operational effectiveness evaluation of LRASM 1.1.
2. Plan and execute an adequate LRASM C-2 OT&E to support the full-rate production decision.
3. Ensure adequate LRASM 1.1 M&S resources remain when LRASM C-2 M&S operational testing requirements are established.
4. Demonstrate end-to-end performance of the Electronic Safe and Arm Fuze, including the detonation of a warhead against a representative target as a risk reduction event prior to, or in conjunction with, the Operational Test Event (OTE-2) lethality demonstration identified in the Master Test Strategy.

Over-The-Horizon Weapons System (OTH-WS)

In March 2021, the Navy conducted three of six planned Over-The-Horizon Weapon System (OTH-WS) live fire test events employed from a Littoral Combat Ship. In May 2021, the Navy conducted three of six operational test firings; the remaining missions will be fired during FY22. The Navy expects to complete IOT&E in 3QFY22. The lethal effects of the OTH-WS are currently unknown and need to be adequately evaluated to support the fielding decision.

System Description

The OTH-WS is a long-range, surface-to-surface missile employed by either the Littoral Combat Ship or the planned guided-missile frigate, intended to engage maritime targets both inside and beyond the firing unit's radar horizon. The OTH-WS is a stand-alone system consisting of an operator interface console, naval strike missile, and a missile launching system, requiring minimal integration into the host platform. The OTH-WS receives targeting data via tactical communications from combatant platforms or airborne sensors and requires no guidance after launch. The U.S. Marine Corps will employ the naval strike missiles from the Joint Light Tactical Vehicle-based mobile launch platform as a component of a Navy/Marine Expeditionary Ship Interdiction System.

Program

OTH-WS is an Acquisition Category II, Non-Developmental Item (NDI) program. In FY18, the Navy awarded a firm-fixed-price contract to Raytheon Missile Systems to integrate the OTH-WS onto several Navy platforms. Though the program entered Milestone C in 3QFY21, the Navy has yet to submit a Test and Evaluation Master Plan to DOT&E for review and approval. IOT&E started in March 2021 and is intended to inform a full-rate production decision currently scheduled for FY22. The full-rate production decision is expected to slip to FY23 due to the test event issue in May 2021.

Major Contractor

Raytheon Missile and Defense – Tucson, Arizona.

Test Adequacy

In March 2021, the Navy conducted three of the planned six OTH-WS live fire test events employed from a Littoral Combat Ship at the Point Mugu Sea Range off the coast of California. In May 2021, during the execution of the remaining three live fire test events, the Navy experienced an issue and halted the remaining tests to determine the root cause. The test events were executed in accordance with a DOT&E-approved IOT&E Plan. The Navy expects to complete the remaining three live fire test events in 3QFY22.

In August 2021, the U.S. Marine Corps fired two naval strike missiles during the Large Scale Exercise at the Pacific Missile Range Facility in Hawaii. The Navy authorized the assignment of those two operational test assets to support this emergent need. The Navy coordinated with the Marine Corps to optimize this test opportunity and collect pertinent data in support of the OTH-WS operational assessment.

The Navy and DOT&E have not yet agreed to an adequate LFT&E strategy required to determine OTH-WS lethality. The Navy has not approved funding and has not planned or executed any lethality testing, precluding an assessment of OTH-WS operational effectiveness and lethality in support of the fielding decision.

Performance

Effectiveness

The Navy conducted three of six planned IOT&E live firing events in FY21; IOT&E is planned to complete in 3QFY22. Based on the three live firings in FY21, the system demonstrated a potential to provide the Navy with the capability to defeat surface vessels over-the-horizon. A final assessment of the OTH-WS operational effectiveness will be provided after the completion of operational testing and required lethality testing.

Suitability

The issue experienced during IOT&E also precluded a preliminary assessment of OTH-WS operational suitability. The Navy identified a failed component and implemented specific inspections on the naval strike missiles to prevent similar occurrences in future test events. The root cause of the failed component is still pending.

Survivability

The Navy expects to execute a Cooperative Vulnerability and Penetration Assessment and an Adversarial Assessment in FY22 to support the evaluation of OTH-WS survivability in a cyber-contested environment.

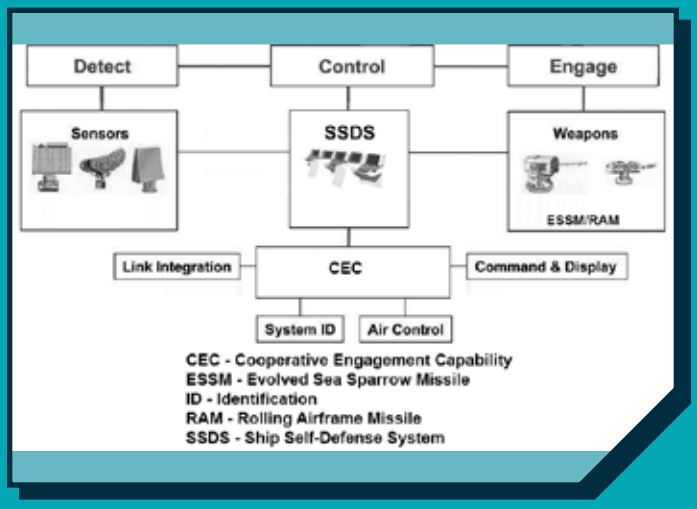
Recommendations

The Navy should:

1. Fund, develop, and execute a DOT&E-approved LFT&E strategy to determine the naval strike missile lethality in support of the operational effectiveness assessment and the fielding decision.
2. Continue addressing February 2020 Early Fielding Report recommendations.

Ship Self-Defense System (SSDS) Mk 2 Integrated Combat Systems

The Navy needs to complete development of a T&E strategy to evaluate SSDS Mk 2 Integrated Combat System (ICS) performance on next generation and in-service SSDS-equipped ships. In addition, the Navy should continue to fund and execute planned repairs to the Self Defense Test Ship (SDTS) and install the appropriate combat system equipment on the SDTS to support adequate testing of the SSDS Mk 2 ICS.



System Description

For amphibious ships and aircraft carriers, the SSDS Mk 2 is the core combat system control element that integrates organic shipboard sensors, trackers, tactical datalinks, and weapons to provide a rapid detect-track-engage self-defense capability against anti-ship cruise missiles. The SSDS Mk 2 consists of a network of processors that host tactical programs, and hardware that provides an interface between SSDS and all connected processors and external systems.

The SSDS Mk 2 has six variants hosted on various surface ship classes: Mod 1 on CVN 68-class aircraft carriers, Mod 2 on LPD 17-class amphibious ships, Mod 3 on Landing Helicopter Dock (LHD) 1-class amphibious ships, Mod 4 on LHA 6-class amphibious ships, Mod 5 on Dock Landing Ship (LSD) 41/49 classes of amphibious ships, and Mod 6 on CVN 78-class aircraft carriers.

The Navy intends to upgrade all of the above SSDS Mk 2 Mods with new software and hardware known as the "Baseline 12" configuration. The Navy plans to deliver the SSDS Mk 2 Baseline 12 combat systems with LHA 6 Flight 1 (LHA 8) ships (Mod 4), LPD 17 Flight II ships (Mod 2), and CVN 79 (Mod 6). The Baseline 12 combat systems are also intended to be back-fit onto in-service ships with legacy SSDS configurations. SSDS Mk 2 Baseline 12 will integrate the following new and existing combat system elements in various configurations:

- SPY-6(V)2 and SPY-6(V)3 Enterprise Air Surveillance radars (EASR)
- SPQ-9B horizon search radar
- SPS-48 and SPS-49 air search radars
- Mk 9 Tracker Illuminator System
- Cooperative Engagement Capability (CEC)
- SLQ-32(V)6 equipped with the Surface Electronic Warfare Improvement Program (SEWIP)

- Rolling Airframe Missile (RAM) Block 2, 2A, and 2B
- Evolved SEASPARROW Missile (ESSM) Block 1
- Close-In Weapon System

Program

Several Major Defense Acquisition programs comprise the SSDS ICS on LHA 8, LPD 17 Flt II, and CVN 79 ships:

- SSDS — designated an Acquisition Category IC program in 2005 when the Navy transitioned to the Mk 2 variant that integrated the CEC
- CEC Block 2 — an Acquisition Category II program that achieved Milestone B approval in June 2020
- SEWIP Block 2 — an Acquisition Category II program that completed IOT&E in 2016
- RAM Block 2/2A/2B — an Acquisition Category II program; RAM Block 2 completed IOT&E in 2016
- ESSM Block 1 — an Acquisition Category II program that completed IOT&E in April 2003
- EASR — unique variants of the SPY-6 family of radars, which is an Acquisition Category IC program that has not yet undergone IOT&E

In 2018, DOT&E approved revision C of the SSDS Test and Evaluation Master Plan (TEMP) which encompassed FOT&E of Mk 2 capability for in-service ships. In addition to testing on CVN 78 and LHA 6, the TEMP revision included FOT&E test events for SSDS Mk 2 systems (retrofitted to replace SSDS Mk 1) on LSD 41/49 ship classes.

Major Contractors

- SSDS: Lockheed Martin – Moorestown, New Jersey.
- SPY-3 and SPY-4 (Dual Band Radar): Raytheon Integrated Defense Systems – Tewksbury, Massachusetts.
- EASR: Raytheon Integrated Defense Systems – Marlborough, Massachusetts.
- RAM and ESSM: Raytheon Missile Systems – Tucson, Arizona.
- CEC: Raytheon Integrated Defense Systems – St. Petersburg, Florida.
- SLQ-32 with SEWIP Block 1: General Dynamics Advanced Information Systems – Fair Lakes, Virginia.
- SLQ-32 with SEWIP Block 2: Lockheed Martin – Syracuse, New York.

Test Adequacy

In-service SSDS-equipped ships

The CVN 78 *Gerald R. Ford*-class Nuclear Aircraft Carrier article in this Annual Report summarizes the adequacy of the CVN 78 ICS testing conducted to date.

The Navy did not allocate funding to conduct the operational test campaign for LSD 41/49 ship classes as outlined in the approved SSDS TEMP Revision C. The LSD ships upgraded from SSDS Mk 1 to SSDS Mk 2 have deployed with a combat system that completed 1 of 9 planned operational tests.

Next-generation SSDS-equipped ships

The Navy agrees an unmanned sea-going test asset (e.g., SDTS) is required to adequately and safely test SSDS combat systems. The Navy committed to providing the resources required to retain this capability via a planned maintenance availability of the existing SDTS (e.g., *Paul F. Foster*), as well as the procurement and installation of the necessary combat system elements on the SDTS.

In April 2021, the Navy announced that they did not intend to update the extant SSDS Mk 2 TEMP to direct T&E of a fleet-wide SSDS Mk 2 upgrade and modernization program. Instead, the Navy proposed to develop a broader ICS test strategy across all SSDS-equipped ships intended to encompass SSDS and other ICS elements. DOT&E concurred with this approach. In May 2021, the Navy initiated development of an ICS operational test strategy. Through December 2021, the Navy generated cost and resource estimates to execute some future testing, but these estimates are inadequate because the Navy has not yet determined which ICS elements and their associated test programs will be included in the test strategy. Multiple combat system elements currently lack developmental and operational test programs to inform the overarching test strategy; some estimates of required test assets, such as live missiles, have been arbitrarily generated. Until developmental and

operational test strategies for SSDS Mk 2 and these major combat system elements are determined, the adequacy of ICS developmental and operational testing is at risk.

The Navy does not have an operational test strategy for testing of SSDS Mk 2 Baseline 12-equipped ships intended to be upgraded with either variant of the EASR. Currently, the Navy does not intend to develop an EASR TEMP, and has not yet determined how they will document for approval the developmental and operational testing required for the EASR variants on SSDS ships.

The Navy has not yet determined if they will have sufficient ESSM Block 1 missiles to support testing of CVN 78 and LHA 8. These missiles, required for combat system testing in FY25 and beyond, are no longer in production and will have to be taken from fleet inventories.

Performance

Effectiveness

The effectiveness of SSDS Mk 2 Mod 6 and the CVN 78 Integrated Combat System is discussed in the CVN 78 *Gerald R. Ford*-class Nuclear Aircraft Carrier article in this Annual Report.

Suitability

The suitability of SSDS Mk 2 Mod 6 is yet to be determined. SDTS is not an adequate platform to assess combat system suitability, and no operational testing has yet been conducted on board CVN 78.

Survivability

The Navy has not yet scheduled or resourced the SSDS Mk 2 Mod 6 cybersecurity testing aboard CVN 78 as outlined in the approved SSDS TEMP Revision C.

Recommendations

The Navy should:

1. Address combat system issues identified during CVN 78 ICS testing on the SDTS.
2. Fund the modeling and simulation suite required to support assessment of the CVN 78 Probability of Raid Annihilation requirement for subsonic targets.
3. Continue to fund the maintenance availability for the current SDTS (e.g., *Paul F. Foster*) to ensure its readiness to support future combat system testing.
4. Continue to fund the procurement and installation of the necessary combat system elements on SDTS.
5. Define the ICS elements to be included in the SSDS ICS TEMP.
6. Develop and resource adequate developmental and operational test strategies for all ICS elements in the SSDS ICS TEMP.
7. Determine how operational testing for EASR variants will be documented for DOT&E approval.
8. Determine if the remaining ESSM Block 1 inventory is adequate to support testing needs.
9. Develop plans for addressing incomplete testing in the 2018 SSDS TEMP Revision C.

Surface Electronic Warfare Improvement Program (SEWIP) Block 2

In April 2021, the Navy completed two days of operational testing against surrogate anti-ship cruise missiles and targeting radars to evaluate the Surface Electronic Warfare Improvement Program (SEWIP) Block 2 on CVN 78. Preliminary assessment identified several shortfalls that could reduce operator situational awareness or cause unnecessary missile firings, degrading SEWIP Block 2 operational effectiveness. Preliminary results also suggest that SEWIP Block 2 does not meet its minimum threshold for system reliability. Not enough data are yet available to provide a survivability assessment of the SEWIP Block 2 in a cyber-contested environment. The Navy plans to conduct operational testing of SEWIP Block 2 on DDG 1000 and DDG 51 Arleigh Burke class with a modified Aegis Combat System in FY22.

System Description

SEWIP (AN/SLQ-32) is an electronic support system that detects, identifies, and tracks adversary anti-ship cruise missiles (ASCM) and targeting radars. SEWIP (AN/SLQ 32 V6) Block 2 incorporates a new antenna system, enhanced processing capabilities, and a High Gain High Sensitivity subsystem to improve battlefield situational awareness. SEWIP Block 2 also added a Soft Kill Coordination System to improve decoy employment and combat system soft kill integration.

Program

SEWIP Block 2 is an Acquisition Category II program that entered Milestone C in January 2013. The Navy completed SEWIP Block 2 IOT&E in 2016 and approved full-rate production in 2016. SEWIP Block II FOT&E assesses system upgrades since IOT&E, examines combat system and decoy integration capabilities of the Soft Kill Coordination System, and evaluates SEWIP Block 2 integration with the DDG 51 Arleigh Burke class and its modified Aegis Combat System, the Ship Self-Defense Combat System on CVN 78, and the Total Ship Computing Environment combat system on DDG 1000.

Major Contractor

Lockheed-Martin – Syracuse, New York.

Test Adequacy

In April 2021, the Navy completed one phase of SEWIP Block 2 FOT&E, a two-day operational test aboard CVN 78 dedicated to SEWIP Block 2 surrogate ASCM and targeting radar runs. Due to a delay in starting test and test equipment malfunctions, the Navy did not complete all planned test runs in the DOT&E-approved test plan. In addition, only two Lear aircraft were resourced to support the test, contributing to the limited data collection. Data collected during an earlier developmental test and during ASCM profiles against the Navy's self-defense test ship for CVN 78 are being evaluated to supplement operational test data. The sufficiency of these data to support the operational effectiveness and suitability of SEWIP Block 2 on CVN 78 is yet to be determined. A final assessment will be published in a classified FOT&E report for SEWIP Block 2 on CVN 78 upon completion of tests.

The Navy expects to test SEWIP Block 2 on a DDG 1000 class ship and on DDG 51 Arleigh Burke class with its modified Aegis Combat System in 3QFY22. The Navy intends to evaluate the survivability of SEWIP Block 2 on a DDG 51 Arleigh Burke class during Aegis cybersecurity testing in 1QFY23.

The Navy recently developed additional threat emulations for targeting radars and more representative stream raids. These added threat emulations, if effectively employed within the test designs, will more adequately inform system capability in the DDG 1000 and Aegis phases of the FOT&E.

SEWIP Block 2 with CVN 78 testing was limited to a subset of congested and contested electromagnetic spectrum environments due to limited CVN 78 availability to support testing, requiring future phases of test to include a more comprehensive and complex electromagnetic spectrum environment.

Performance

Effectiveness

Analysis of FOT&E data for SEWIP Block 2 on CVN 78 is in progress, precluding a final assessment of SEWIP Block 2 operational effectiveness. Preliminary assessment identified shortfalls that could reduce operator situational awareness or cause unnecessary missile firings, degrading operational effectiveness. The operational effectiveness for SEWIP Block 2 on the DDG 51 Arleigh Burke class and DDG 1000 will remain unknown until the completion of these phases of FOT&E.

Suitability

Analysis of FOT&E data for SEWIP Block 2 on CVN 78 is in progress, precluding a final assessment of SEWIP Block 2 operational suitability. Preliminary results and Fleet operational data suggest that SEWIP Block 2 does not meet its minimum threshold for system reliability.

Survivability

Not enough data are yet available to provide a survivability assessment of the SEWIP Block 2 in a cyber-contested environment. The Navy plans to evaluate the survivability of SEWIP Block 2 against the cyber threat during the DDG 51 Arleigh Burke class FOT&E test period.

Recommendations

The Navy should:

1. Continue to develop emulations for emerging threat ASCMs.
2. Ensure sufficient test time is planned for evaluating SEWIP Block 2 on DDG 1000 and DDG 51 Arleigh Burke class ships to account for unplanned test delays; the Navy should also resource four Lear aircraft to support these test events.
3. Plan and resource testing of SEWIP Block 2 with a complex electromagnetic spectrum environment for remaining test phases.

Tactical Tomahawk Modernization

The upgraded version of the Tomahawk Weapon System (TWS) is operationally effective, demonstrating performance in a GPS-denied environment and the ability to communicate over the Advanced Communication Architecture. The Navy should correct deficiencies identified in the operational test prior to the introduction of the upgraded TWS to the Fleet. Details are available in a classified TWS FOT&E report, published in October 2021.

System Description

The TWS consists of three segments intended to provide surface combatants and submarines with long-range, precision-guided, land attack cruise missile capability. The three segments include the All Up Round (AUR), the Theater Mission Planning Center (TMPC) for mission planning and distribution, and the Tactical Tomahawk Weapon Control System (TTWCS) for the initialization, preparation, launch, and post-launch control of the missile.

Program

The TWS is an Acquisition Category IC program. The current AUR, the Block IV variant, entered service in 2004 with a 30-year life cycle and 15-year recertification cycle. DOT&E approved Revision H of the TWS Test and Evaluation Master Plan in 2018. In 2020, the Navy began a modernization and recertification of the AUR to extend the missile's certification another 15 years by replacing obsolete and expired components, upgrading the communications systems to operate on the Advanced Communication Architecture, and providing a targeting capability in a GPS degraded or denied environment. This modernized AUR is designated Tomahawk Block V. The Navy is leveraging the overall TWS modernization program to support the development of the Maritime Strike Tomahawk (MST), an anti-ship capability, and to introduce an advanced warhead design to improve TWS lethality.

Major Contractors

- Missile segment: Raytheon Missiles and Defense – Tucson, Arizona.
- Weapon Control System segment: Lockheed Martin – Valley Forge, Pennsylvania.

- Mission Planning segment:
  - Peraton, Inc. – San Jose, California (Mission Distribution System).
  - Tapestry Solutions – St. Louis, Missouri (Tomahawk Planning System).
  - BAE Systems – San Diego, California (Targeting Navigation Tool Set).

Test Adequacy

The Navy conducted operational testing on the TWS at the Washington Planning Center, Washington Navy Yard, Naval Surface Warfare Center Dahlgren, Virginia, Pacific Missile Test Center, Pt Mugu, California, and USS *Chafee*, (DDG 90), Pearl Harbor, Hawaii between August 2020 and May 2021 using fleet operators. The testing consisted of 3 live flight tests, 17 high-fidelity simulated launches, and 10 mission planning events. Testing, conducted in accordance with DOT&E-approved test plans, was adequate to evaluate the operational effectiveness and suitability of upgraded and modernized TWS.

In FY21, the Navy also conducted a Cooperative Vulnerability and Penetration Assessment and an Adversarial Assessment of the TMPC and TTWCS to assess their survivability in a cyber-contested environment. The Navy deviated from the DOT&E-approved test plan by placing the Tomahawk AUR and elements of the TMPC "off limits" due to the concern of inadvertently damaging these test assets, critical to the program. Consequently, the cyber survivability assessment of the TWS does not consider some attacker profiles.

Performance

Effectiveness

TWS continues to be operationally effective. Testing demonstrated no degradation in capability as compared to the legacy system. Specifics on missile accuracy and mission tasking response time are provided in a classified TWS FOT&E report published in October 2021.

The Tomahawk Block V AUR demonstrated sufficient accuracy in a GPS-denied environment and the capability to operate on the Advanced Communication Architecture network. The classified TWS FOT&E report highlights deficiencies that should be resolved prior to the introduction of the upgraded TWS Block IV to the fleet. The upgraded and modernized AUR maintains the legacy AUR lethality since the warhead remained unchanged.

Suitability

TWS remains operationally suitable, meeting or exceeding the reliability and availability requirements. There were no hardware failures during testing. The Navy corrected the four identified software deficiencies and demonstrated the effectiveness of the corrections prior to the completion of the test.

Survivability

The survivability assessment of TWS in a cyber-contested environment is detailed in the classified TWS FOT&E report published in October 2021.

Recommendation

1. The Navy should resolve the major deficiencies identified during operational testing prior to fleet release. Detailed recommendations are included in the classified TWS FOT&E report published in October 2021.

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

Analysis of the Unmanned Influence Sweep System (UISS) IOT&E, conducted in FY21, is ongoing, precluding an evaluation of UISS operational performance at this time. While the UISS demonstrated the capability to sweep mines, successfully activating the threat mines simulated in the test, it also experienced problems that challenged its operational effectiveness and suitability. The Navy expects to complete UISS IOT&E in early FY22 to support a full-rate production decision scheduled for April 2022.

System Description

The UISS is a mine clearance system that activates threat mines as it passes by them, referred to as mine sweeping. The UISS includes an Unmanned Surface Vehicle (USV) that powers and tows the Unmanned Surface Sweep System (US3). The USV operates along pre-planned tracks and uses a radar and camera surveillance suite to provide a remote operator with situational awareness and the ability to avoid obstacles or other watercraft. The US3 creates a magnetic field and acoustic noise to represent a target vessel, causing the threat mine to detonate. The Navy intends for the UISS to clear mines within an assigned area, such as a sea-lane, strait, choke point, or fleet operating area, enabling safe transit. The LCS is the primary host, but the UISS can be employed from any appropriately equipped vessel, or from shore.

Program

The UISS is an Acquisition Category III program intended to provide the only organic capability to sweep mines after the Navy retires the aging MCM-1 class Mine Countermeasures Ships and MH-53E Airborne Mine Countermeasures helicopters. The Navy completed an operational assessment in November 2019, informing the decision to proceed with UISS low-rate initial production. The Navy expects to complete UISS IOT&E in early FY22 to support a full-rate production decision scheduled for November 2022. UISS IOT&E contributes to the assessment of mission capability provided by the Mine Counter Measure (MCM) mission package on LCS. The Navy further intends the USV component of UISS to support additional MCM capability with different payloads that are in development.

Major Contractor

Textron Systems Corporation – Hunt Valley, Maryland.

Test Adequacy

In FY21, the Navy conducted the following test events to evaluate the UISS:

- Technical evaluation on LCS in October 2020 to gain Fleet operator proficiency and demonstrate launch and recovery capability. LCS crane problems prevented the intended launch and recovery cycles.
- Operational test in March 2021 of UISS against mine surrogates in shallow waters near Panama City, Florida. The Navy collected UISS effectiveness and reliability data, but operations were shore-based and did not provide launch and recovery data from an LCS.
- Technical evaluation in April/May 2021 that demonstrated launch and recovery capability from an LCS using Fleet operators.
- Operational test in May/June of UISS conducting full mission profiles from an LCS off the shore of southern California. The Navy collected effectiveness and suitability data for UISS sweep of mine surrogates in both shallow and deep fields, launch and recovery data from an LCS, and system maintenance. The Navy only conducted about half of the planned profiles in shallow water due to UISS maintenance issues and target availability.
- Cybersecurity evaluation in September 2021, including both a Cooperative Vulnerability and Penetration Assessment and an Adversarial Assessment, of surrogates for the UISS and the LCS mission package computing environment that were validated as equivalent to their low-rate production and delivered systems for the purpose of this test. The Navy conducted the assessments at the Aberdeen Test Center in Maryland.

The Navy has not conducted all planned testing, and some of the conducted tests deviated from approved DOT&E-approved test plans. Analysis is in progress to determine if the collected data are sufficient to evaluate operational effectiveness, suitability, and survivability.

Performance

Effectiveness

Analysis of the test data is ongoing, precluding the evaluation of UISS operational effectiveness at this time. The UISS demonstrated the capability to sweep mines, successfully activating the threat mines simulated in the test. The Navy did not resolve the shortfall that affects mission planning, as demonstrated in the November 2019 operational assessment.

Suitability

Analysis of the test data is ongoing, precluding the evaluation of UISS operational suitability at this time. The UISS experienced problems throughout testing that will degrade its operational suitability and effectiveness. Maintainers revealed limitations in maintainer documentation that will have to be addressed to support operational suitability. Underwater explosion testing data are not yet available to determine UISS operability following mine explosions caused by mine sweep operations.

Survivability

Analysis of the test data is ongoing, precluding survivability evaluation of the UISS in a cyber-contested environment at this time.

Recommendations

The Navy should:

1. Complete the analysis of the adequacy of executed test plans, and in coordination with DOT&E, determine the need to conduct additional tests in FY22 to close the data shortfalls required to credibly evaluate UISS operational effectiveness.
2. Address the recommendations outlined in the Controlled Unclassified Information edition of this report.

VH-92A® Presidential Helicopter Replacement Program

The United States Marine Corps intends to declare initial operational capability in 2022 based on the IOT&E conducted by Marine Helicopter Squadron One (HMX-1) using production representative System Demonstration Test Article aircraft from February 8 to April 16, 2021 under the auspices of the Commander, Operational Test and Evaluation Force. The VH-92A operational effectiveness, suitability and survivability is detailed in the VH-92A IOT&E report, published in September 2021. VH-92A is a registered trademark of the Department of the Navy.

System Description

The VH-92A is a four-bladed, dual-piloted, twin-engine helicopter based on the Sikorsky S-92 medium-lift helicopter, equipped with the Mission Communication System (MCS) to enable simultaneous short- and long-range secure and non-secure voice and data communications. HMX-1 will use the VH-92A aircraft to conduct administrative lift and contingency operations intended to provide safe and timely, pre-planned or unscheduled, transport of the President of the United States and other parties as directed by the White House Military Office. The Navy intends for the VH-92A to be air transportable to remote locations via a single Air Force C-17 cargo aircraft. The VH-92A will replace the legacy fleet of VH-3D and VH-60N aircraft.

Program

VH-92A is an Acquisition Category IC program that does not include a full-rate production decision. DOT&E-approved the VH-92A Test and Evaluation Master Plan in 2015 and the IOT&E plan in 2020 in support of the United States Marine Corps declaration of initial operational capability and the White House Military Office's VH-92A Commissioning Program. The Navy intends to procure 23 VH-92A aircraft to replace 23 legacy aircraft.

Major Contractor

Sikorsky Aircraft Corporation, a Lockheed Martin Company – Stratford, Connecticut.

Test Adequacy

Operational, live fire, and cybersecurity testing were conducted in accordance with DOT&E-approved test plans and were adequate to evaluate operational effectiveness, suitability, and survivability of the VH-92A as operated by HMX-1.

HMX-1 conducted IOT&E using production-representative System Demonstration Test Article aircraft from February 8 to April 16, 2021 under the auspices of the Commander, Operational Test and Evaluation Force. The majority of the operations took place in the National Capital Region using facilities and landing zones routinely employed by HMX-1. IOT&E also included a three-aircraft deployment to Joint Base Charleston, South Carolina. During IOT&E, HMX-1 flew 130.9 hours and completed 18 operationally representative administrative lift and contingency operation missions.

Performance

Effectiveness and Suitability

In accordance with the VH-92A Security Classification Guide, the operational effectiveness and suitability of the VH-92A is detailed in the Controlled Unclassified Information edition of this report. The report assesses the VH-92A operationally effectiveness for administrative lift missions and contingency operation missions to include the contribution of MCS to operational performance. The report details the lift capacity, range, and airspeed compared to in-service aircraft. The report also assesses the VH-92A suitability requirements, the organizational-level MCS diagnostic capability at HMX-1 and time required to access MCS components.

Survivability

The VH-92A survivability assessment against operationally relevant threats, to include assessment in a cyber-contested environment, is summarized in two classified annexes of the VH-92A IOT&E report, published in September 2021.

Recommendation

1. The Navy should consider addressing the recommendations offered in the Controlled Unclassified Information edition of this report.

Air Force Programs

AGM-183A Air-Launched Rapid Response Weapon

The AGM-183A Air-Launched Rapid Response Weapon (ARRW) program has not yet demonstrated the required warfighting capability. The program conducted several developmental ground and flight tests demonstrating adequate interface integration with the B-52H aircraft. The program is implementing corrective actions within a series of rocket motor booster test flights. Hardware and software problems have delayed planned operational demonstration flights.

System Description

The ARRW is a conventional, boost-glide, hypersonic weapon consisting of a solid rocket motor booster, a glider protective shroud, and a glider vehicle containing a kinetic energy projectile warhead. A standoff air-to-ground missile launched from a B-52H aircraft, the ARRW is intended to attack high-value, time-sensitive, land-based targets.

Program

ARRW is a Section 804 Rapid Prototyping Middle Tier of Acquisition program leveraging lessons learned from the Defense Advanced Research Projects Agency Tactical Boost Glide vehicle program. The program is currently developing an Integrated Master Test Plan and an Operational Demonstration test plan for DOT&E approval. After completion of the booster rocket flight tests, the program plans to proceed into all-up round (AUR) testing (including live warheads). The Air Force intends to complete at least one AUR test to determine if the system has reached an early operational capability state, before awarding a contract for production. The Air Force will consider transitioning the program from a Rapid Prototyping to a Rapid Fielding program after successfully deploying the ARRW residual capability.

The program flight test schedule could be delayed due to the limited number and availability of hypersonic flight corridors, target areas, and test support assets. The program will be competing for these limited resources with other hypersonic programs, including those being developed by the Navy, Army, and Missile Defense Agency.

Major Contractors

Lockheed Martin Corporation, Missiles and Fire Control (LMMFC) Division – Orlando, Florida. Boeing Aircraft Modernization and Sustainment – Oklahoma City, Oklahoma.

Test Adequacy

The ARRW Integrated Master Test Plan consists mostly of developmental ground and flight testing, and some lethality live fire testing. The Air Force plans to execute an Operational Demonstration using prototype AURs to assess the operational capabilities and limitations of the system. The limited number of test assets will not allow a standard assessment for operational effectiveness, lethality, suitability, and survivability.

In FY21, the program completed five instrumented measurement vehicle captive-carry flight tests to demonstrate initial weapon-aircraft interface integration, as well as proper fit and mechanical function of the weapon with the B-52H aircraft. The ARRW program twice attempted to execute one of the three planned booster test flights with a simulated glider. The booster test flights are intended to demonstrate final weapon-aircraft integration with the production-representative missile, the capability to launch the weapon inside the flight envelope, and proper performance of the booster rocket. Four AUR tests will ensue upon the conclusion of booster flight testing.

The ARRW program executed one successful high-speed ground sled test to demonstrate warhead lethality performance against a variety of component-level targets. It continues to execute its series of six warhead arena tests needed to characterize the warhead fragment mass and velocity distribution in support of the ARRW lethality evaluation.

The Air Force plans to use engagement-level and mission-level modeling and simulation (M&S) to assess ARRW survivability against surface-to-air missile systems, anti-aircraft-artillery batteries, and air-to-air missiles.

Performance

Effectiveness

Hardware and software problems have delayed planned ARRW operational demonstration flights, precluding an initial assessment of any risks to demonstrating the ARRW's intended operational effectiveness requirements. Instrumented measurement vehicle captive-carry test flights validated the initial weapon-aircraft interface integration, confirmed aircraft mechanical fit and function data, and were used to develop and mature the software for the production-representative missile. These flight tests experienced two unexpected test events, which required a redesign of the fin control system. The Air Force validated all corrective actions in the final captive carry flight before proceeding into booster flight testing.

The first booster test flights experienced an unexpected test event on both attempts. During the first test, the missile, by design, did not separate from the B-52 because the system determined there was a fin actuator problem. The Air Force implemented a corrective action before the second attempt. During the second attempt, the missile experienced an unexpected test event after release from the B-52 aircraft that prevented the booster motor from igniting, leading to a loss of the test asset. The Air Force is currently conducting a Failure Review Board to determine the root cause(s) of the failure and implement corrective actions to the missile system before the next booster test flight. Although the second booster test experienced an unexpected event, it did demonstrate the safe release and separation of the weapon system from the aircraft. The second booster test also validated the fin actuator corrective action.

Lethality testing is ongoing, precluding an initial assessment of ARRW warhead performance. Given the limited number of planned test events, there is risk to demonstrating the ARRW lethal effects against the required tactical and strategic targets.

Suitability

The limited number of planned flight hours and test assets (booster and AUR) will preclude an adequate interim assessment of all ARRW operational suitability metrics.

Survivability

The engagement-level or mission-level simulations have not yet been completed to assess ARRW survivability in a contested environment. Pending the verification, validation, and accreditation of the M&S tools, the final survivability assessment should estimate the probability that a single ARRW will

complete its mission given the capability of various early warning radars, surface-to-air missile systems, anti-aircraft-artillery batteries, and air-to-air missiles to detect and engage ARRW in various one-on-one scenarios. The final survivability assessment should also estimate such probability in the presence of multiple threat systems connected by a command, control, communications, and intelligence network capable of detecting, tracking, and engaging multiple airborne targets, including hypersonic weapons like the ARRW.

Recommendations

The Air Force should:

1. Collaborate with the Office of the Secretary of Defense stakeholders and the Army and Navy hypersonic Program Offices to identify and leverage common best practices, test corridors and infrastructure, test data management and analyses, and M&S capability.
2. Verify, validate, and accredit all M&S tools intended to enable an adequate assessment of ARRW performance.
3. Conduct an adequate survivability assessment of ARRW in a cyber-contested environment.

AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM)

The Advanced Medium-Range Air-to-Air Missile (AMRAAM) Air Intercept Missile (AIM)-120D System Improvement Program (SIP)-3 continued operational testing in CY21, completing eight planned missile flight tests. Assessment of the AIM-120D SIP-3's operational effectiveness, suitability, and survivability is pending FOT&E completion and will be reported on in CY22.

System Description

The 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 the AMRAAM. F-15C/D/E, F-16C/D, F/A-18C/D/E/F, EA-18G, F-22A, F-35A/B/C, and AV-8B aircraft are capable of employing the AMRAAM. The AIM-120D is the newest variant in the AMRAAM family of missiles, and includes both hardware and software improvements over the AIM-120C3-C7. Four planned follow-on SIPs will provide updates to the AIM-120D to enhance missile performance and resolve previous deficiencies.

Program

The AMRAAM SIP-3 upgrade is a project under the Acquisition Category I AMRAAM program. DOT&E approved the SIP-3 revision of the Test and Evaluation Master Plan in 2019. The Air Force and Navy plan to field SIP-3 software following the completion of SIP-3 operational testing.

Major Contractor

Raytheon Missiles and Defense – Tucson, Arizona.

Test Adequacy

Between February 2020 and November 2021, the Air Force and Navy conducted integrated developmental and operational testing and dedicated operational testing. Testing was conducted in accordance with the DOT&E-approved test plan, and included eight planned missile flight tests. Seven flight tests were successful and an earlier no-test was re-accomplished successfully.

Modeling and simulation runs were conducted to quantify performance across the flight envelope. Details will be provided in the DOT&E report to be released in 2022.

The AIM-120 Cooperative Vulnerability and Penetration Assessment and the Adversarial Assessment are ongoing. Subsequent analysis and reporting are expected to complete in CY22.

Performance

Effectiveness

Assessment of the AIM-120D SIP-3's operational effectiveness is pending FOT&E completion and will be reported on in CY22. Given no recent upgrades to the AIM-120D warhead, the AIM-120D SIP-3 maintains the lethality performance of the legacy weapon.

Suitability

Assessment of the AIM-120D SIP-3's operational suitability is pending FOT&E completion and will be reported on in CY22.

Survivability

The AMRAAM's survivability in a cyber-contested environment will be provided in CY22 after the completion of the DOT&E-approved Cooperative Vulnerability and Penetration Assessment and Adversarial Assessment.

Recommendations

None.

Air Operations Center–Weapon System (AOC-WS)

The Air Force continues to develop the Air Operations Center-Weapon System (AOC-WS) Block 20 software, but it is unlikely to be sufficiently mature to support a full OT&E until FY23. The Air Force plans to meet a long-standing cybersecurity assessment requirement, revise an outdated Test and Evaluation Master Plan (TEMP), and re-submit to DOT&E for review and approval in FY22.

System Description

The AOC-WS is a system of systems that incorporates numerous third-party, commercial off-the-shelf, and Agile-developed software applications. It provides the Commander, Air Force Forces, or the Joint/Combined Forces Air Component Commander with the capability to exercise command and control of joint or combined air forces, including planning, directing, and assessing air, space, and cyberspace operations, as well as air defense, airspace control, and the coordination of space and mission support not resident within theater.

Program

The AOC-WS 10.1 (AN/USQ-163 Falconer) was a Major Automated Information System program or Acquisition Category IAM when it completed initial operational testing in February 2005. Since FY19, the Program Office delivered incremental updates via Agile Release Events (AREs) to both maintain and upgrade the system. The AOC-WS 10.1 TEMP, approved in 2011, is no longer current, and the Program Office expects to update the TEMP in FY22.

AOC-WS Block 20 started as a Defense Innovation Unit Experimental effort in 2017. The Program Office transitioned it to six Middle Tier of Acquisition Section 804 programs in FY19. The program intends to transition all efforts to the Software Acquisition Pathway in FY22. As more Block 20 capabilities are developed, the program will continue to transition AOC-WS from the fielded increment 10.1 to a hybrid configuration of AOC-WS 10.1 and Block 20 capabilities.

There is currently no DOT&E-approved TEMP or test strategy for AOC-WS Block 20. In FY22, the Air Force Operational Test and Evaluation Center (AFOTEC) intends to provide a revised overarching test plan and the Program Office intends to update the 10.1 TEMP that allows for an assessment of the continued evolution of 10.1 and Block 20 capabilities.

Major Contractors

Raytheon Intelligence, Information and Services – Dulles, Virginia. Air Force Life Cycle Management Center, Detachment 12 – Boston, Massachusetts.

Test Adequacy

The Air Force conducted three ARE upgrades of AOC-WS 10.1 in FY21. AFOTEC conducted five OT&E events, and those were consistent with the initial test strategy briefed to DOT&E.

Performance

AOC-WS 10.1 upgrades are operationally effective and suitable. In accordance with the AOC-WS Security Classification Guide, additional details are provided in the Controlled Unclassified Information edition of this report.

Recommendations

The Air Force should:

1. Provide a Block 20 acquisition strategy with estimated milestone dates. This is necessary for test planning and compliance with DOD policies governing Middle Tier of Acquisition and Software Acquisition Pathway programs.
2. Submit a TEMP to DOT&E describing an approach to testing the AOC-WS configuration that includes the continued evolution of 10.1 and Block 20.
3. Implement a solution to meet the long-standing requirement to collect and report reliability, availability, and maintainability data for the AOC-WS.

B-52H Commercial Engine Replacement Program (CERP)

The B-52H Commercial Engine Replacement Program (CERP) is in the engine source selection and system design phase. In FY21, following engine source selection, the Air Force developed initial test plans for contractor and government assessments using digital system models.

System Description

The B-52H is a long-range, all-weather bomber that can carry up to 70,000 pounds of precision-guided or unguided conventional and nuclear stores. Units equipped with the B-52H conduct long-range, all-weather conventional and nuclear strike operations against ground and maritime targets in low-to-medium adversary threat environments. The B-52H CERP replaces the legacy TF33 engines with more fuel-efficient, commercial-derivative engines to increase system reliability and reduce sustainment costs. This upgrade will also increase electrical power generation capacity and provide modern digital engine controls and displays.

Program

B-52H CERP is a Middle Tier of Acquisition (MTA) rapid prototyping development program. DOT&E approved the initial B-52 CERP Test and Evaluation Master Plan (TEMP) in March 2020. In September 2021, the Air Force selected the Rolls Royce F130 as the commercial replacement engine.

In FY22, Boeing will deliver the initial increment of the CERP digital design, known as the Virtual System Prototype. The Virtual System Prototype will be used to support initial performance analysis, production process planning, system support analysis, and early training activities, and inform the decision to transition to the second MTA phase.

This second phase will focus on maturation of the digital model, leading to a decision to modify two B-52 aircraft prototypes. These aircraft would be used to conduct developmental testing and an operational demonstration.

Aircraft rapid prototyping test results are currently planned to support the Air Force decision to transition from an MTA program to a Major Defense Acquisition program at the low-rate initial production decision intended to modify 11 B-52 aircraft. The Air Force is assessing options to complete this transition earlier in the acquisition cycle and will document such changes in acquisition program documents at the selected entry milestone.

An IOT&E is currently planned to support a full-rate production/modification decision for the remaining 63 aircraft.

Major Contractors

Boeing Defense, Space, and Security – St. Louis, Missouri. Rolls Royce North America-Defense – Indianapolis, Indiana.

Test Adequacy

The B-52H CERP TEMP defines an adequate operational test strategy for the rapid prototyping program and IOT&E. The Program Office is developing a B-52 enterprise-level cybersecurity strategy to progressively evaluate cybersecurity vulnerabilities across multiple modernization programs, including B-52H CERP.

Performance

B-52H CERP is in the system design phase. In FY21, in advance of engine source selection, the Air Force developed initial test plans for contractor and government assessments using digital system models. Integrated ground and flight test of the MTA prototype aircraft is scheduled to begin in FY25, leading to an operational demonstration in FY26. The IOT&E, designed to determine operational effectiveness, suitability, and survivability in both the conventional and nuclear environments, is planned for FY28.

Recommendation

1. The Air Force should complete development of a B-52 enterprise-level cybersecurity test strategy.

B-52 Radar Modernization Program (RMP)

In June 2021, the Air Force completed the Milestone B acquisition decision and awarded a four-year Engineering, Manufacturing, and Development (EMD) contract to Boeing as the prime contractor. DOT&E approved the B-52 Radar Modernization Program (RMP) Test and Evaluation Master Plan (TEMP) in April 2021 in support of this acquisition decision.

System Description

The B-52H is a long-range, all-weather bomber that can carry up to 70,000 pounds of precision-guided or unguided conventional and nuclear stores in an internal bomb bay and/or external wing pylons. Units equipped with the B-52H conduct long-range, all-weather conventional and nuclear strike operations against ground and maritime targets in low-to-medium adversary threat environments. The B-52H RMP will replace the legacy APQ-166 radar with the modified APG-79 Bomber Modernized Radar System (BMRS). Replacement of the aging legacy radar will increase system reliability and reduce sustainment costs. The BMRS will also provide new capabilities to track moving surface and air targets.

Program

The B-52 RMP is an acquisition category IB Major Defense Acquisition Program. The Air Force approved the initial acquisition strategy in March 2018 and released the development Request for Proposal in October 2019. DOT&E approved the B-52 RMP TEMP in April 2021.

In June 2021, the Air Force completed the Milestone B acquisition decision and awarded a four-year EMD contract with Boeing as the prime contractor. Critical Design Review is planned for early 2022, followed by the modification of two test aircraft.

Flight test is scheduled to begin in FY23 to support an FY24 Milestone C/low-rate initial production decision to modify 28 of the remaining 74 B-52 aircraft. A February 2021 USD R&E review of the developmental test strategy concluded that the program test schedule was high risk based on comparison to previous aircraft radar development programs.

Major Contractor

Boeing Defense, Space, and Security – St. Louis, Missouri.

Test Adequacy

DOT&E approved the B-52 RMP TEMP in April 2021. The TEMP defines an adequate operational test strategy and necessary test resources for integrated testing and IOT&E. The Program Office is developing a B-52 enterprise-level cybersecurity strategy to progressively evaluate cybersecurity vulnerabilities across multiple modernization programs, including B-52H RMP.

Performance

B-52 RMP is in the system design phase. Integrated ground and flight tests to characterize system performance are scheduled to begin in FY23. IOT&E to determine operational effectiveness, suitability, and survivability in both the conventional and nuclear environments is planned for FY25. Based on a review of previous aircraft radar modernization programs, system development strategy, and preliminary design, the developmental areas with highest potential to affect operational effectiveness and suitability include radar software performance, mission systems integration, and radar cooling systems.

Recommendation

1. The Air Force should complete development of a B-52 enterprise-level cybersecurity test strategy.

F-15 Eagle Passive Active Warning and Survivability System (EPAWSS)

F-15 Eagle Passive Active Warning and Survivability System (EPAWSS) development continued in FY21 and the program successfully completed Milestone C in December 2020. The Air Force continues to integrate software, firmware, and hardware fixes to improve performance and address deficiencies uncovered in ground and flight testing. The Air Force needs to complete an update to the Test and Evaluation Master Plan (TEMP) to support Decision Point (DP) 2 authorizing aircraft retrofits and preparations for dedicated IOT&E in FY23.

System Description

The AN/ALQ-250 EPAWSS is a self-protection system intended to enable F-15 aircrew to detect, identify, locate, deny, degrade, disrupt, and defeat air and surface-to-air threats during operations in highly contested environments. EPAWSS replaces three functionally obsolete F-15 legacy Tactical Electronic Warfare System components: the AN/ALR-56C Radar Warning Receiver, the AN/ALQ-135 Internal Countermeasures Set, and the AN/ALE-45 Countermeasures Dispenser Set. The EPAWSS radar warning function scans the radio frequency environment and provides the aircrew with identification and location information on potential threat signals. If necessary, the system can respond with countermeasures (jamming or expendables) to defeat a threat radar or missile. EPAWSS integrates with the AN/APG-82(V)1 radar and F-15 mission computer.

Program

EPAWSS is an Acquisition Category IC program. The Air Force Service Acquisition Executive approved Milestone C DP 1 on December 1, 2020, authorizing the procurement of low-rate initial production aircraft retrofit kits and installation hardware. DP 2, scheduled to occur in May 2022, authorizes the start of fleet aircraft modifications. DOT&E approved the Milestone B TEMP in 1QFY18 and is working with the Air Force to update the TEMP for DP 2. Assuming authorization at DP 2, the Air Force plans to start retrofitting 217 F-15Es and equipping all F-15EXs as they are produced (144 planned). The first operational unit will receive EPAWSS-equipped aircraft in late CY23. The Air Force intends to start fielding EPAWSS on F-15E aircraft in FY23 and F-15EX aircraft in FY24.

Major Contractors

The Boeing Company – St. Louis, Missouri. BAE Systems is the major subcontractor.

Test Adequacy

During FY21, the Air Force completed a series of developmental ground and flight test events as part of EPAWSS Integrated T&E. Ground testing of an uninstalled system at the Integrated Demonstrations and Applications Laboratory, Wright-Patterson Air Force Base (AFB), Ohio provided data to evaluate the radar warning function against most radio frequency emitters required by the system to engage in the presence of background emitters. The Air Force tested the jamming effectiveness against a sample of required threats at several government ground-mount and hardware-in-the-loop test facilities: the Multi-Spectral Test and Training Environment, Eglin AFB, Florida; the Advanced Threat Simulator System, Point Mugu, California; and a test facility at Wright-Patterson AFB, Ohio. Installed system testing in the Benefield Anechoic Facility at Edwards AFB, California assessed integration with F-15E avionics and weapons, as well as installed radar warning performance.

The Air Force 96th Test Wing conducted flight testing of the incremental software releases, each integrating new capabilities with the hardware/firmware and correcting deficiencies. Operational testers participated in these developmental flights and will participate in the additional ground and flight testing that will occur before DP 2. Test data available by mid-FY22 should be adequate to support DP 2, which will be followed by dedicated IOT&E in FY23.

In August, 2020 and March 2021, the Air Force conducted two of the three planned developmental test cybersecurity assessments in the Boeing Electronic Systems Integration Lab. The last assessment is planned for 1QCY22. The Air Force plans to conduct platform-level, on-aircraft operational cybersecurity testing later in CY22.

Performance

Effectiveness

Not enough data are currently available to assess the risk to EPAWSS demonstrating operational effectiveness as it proceeds to IOT&E. Since DP 1, the Air Force has continued to mature the software and hardware to address the deficiencies identified during early developmental testing, and significant additional effectiveness data have been collected, indicating further progress. DOT&E will submit an Operational Assessment report prior to DP 2 in 2QCY22 and will continue to monitor the development of the EPAWSS program as the program prepares to conduct an IOT&E in 2QCY23.

Suitability

Not enough data are currently available to assess the risk to EPAWSS demonstrating operational suitability as it proceeds to IOT&E. Currently, Air Force aircrews and maintainers (with substantial Boeing assistance) operate and support EPAWSS during flight testing using contractor-provided training and preliminary technical orders. Air Force maintainers have identified a problem replacing the Low-Band Antenna line-replaceable unit. The four antenna cables must be phase-matched after the unit has been replaced, which is time-consuming. A potential solution being implemented includes a redesign of the cables with a built-in phase adjustment. Air Force maintainers will evaluate this redesign in CY22.

Air Force maintainers completed one of two planned maintenance demonstrations to assess the removal and replacement of each EPAWSS line-replaceable unit and the adequacy of the technical orders. Their report is pending completion of analysis. Scored reliability data currently include only hardware failures; software failures will be included starting in 1QFY22. Hardware failure during flight operations data to date indicate the system can potentially meet the required 24 hours mean time between unscheduled maintenance; however, the high incidence of unscored software failure indications in prior software versions is a concern. Preliminary assessment of the EPAWSS operational suitability will be provided in time to support DP 2.

Survivability

Not enough data are currently available to assess the EPAWSS survivability in a cyber-contested environment. The Air Force continues to improve the EPAWSS cybersecurity posture by implementing and validating corrective actions based on the vulnerabilities found during the first cybersecurity assessment.

Recommendations

The Air Force should:

1. Score all failure indications (hardware and software) and track all operational suitability metrics, including contractual suitability metrics, to support DP 2 and entry into IOT&E.
2. Continue to plan and execute the F-15 platform-level cybersecurity testing.

F-15 Eagle Integrated Infrared Search and Track

The F-15 Eagle Integrated Infrared Search and Track (EI-IRST) Legion Pod Block 1.5 is operationally effective, providing the F-15C a new capability to engage airborne targets. The Air Force will need to monitor the Legion Pod to determine if the system is suitable for operational use and complete the cyber assessments to determine the survivability of the Legion Pod in a cyber-contested environment. The 53d Wing submitted a Capabilities and Limitations Report to Headquarters, Air Combat Command to allow for operational use of EI-IRST Legion Pod Block 1.5 on F-15C Eagle aircraft.

System Description

The EI-IRST Legion Pod is a passive, long-wave, infrared sensor system intended to allow the F-15C to detect, track, target, engage, and employ weapons against enemy aircraft within its field of regard in a contested, degraded operations environment. Its primary function is to generate precise tracking and targeting data in a radio frequency-contested environment. The F-15C EI-IRST also complements the fire control radar to enhance F-15 effectiveness, lethality, and survivability.

Program

The F-15 EI-IRST Legion Pod is an Acquisition Category II program intended to procure 38 Legion Pods. DOT&E concurred with the Air Force on the F-15C EI-IRST Block 1.5 Risk Assessment Level of Test, dated May 2020, resulting in a Level II OT&E plan (a limited operational test) adequate to evaluate the F-15C EI-IRST Block 1.5. The program has completed Block 1.5 development, and the Air Force started the fielding of the Legion Pods to select F-15C combat squadrons in 4QFY21. The Air Force has not funded the follow-on Block 2 pod in the FY22 budget submission. Due to the lack of funding, the milestone decision authority has not yet approved the Milestone C decision, delaying the approval of the Milestone C Test and Evaluation Master Plan for the Block 2 effort.

Major Contractors

The Boeing Company – St. Louis, Missouri – F-15C integration. Lockheed-Martin – Legion Pod development.

Test Adequacy

The Air Force 53d Wing conducted a Force Development Evaluation from August 2020 to May 2021, during which 140 missions and 214 sorties were flown with the Block 1.5 Legion Pod. During the test, the Air Force 85th Test and Evaluation Squadron employed two AIM-9X Block II missiles cued from the Legion Pod. Due to problems associated with the AIM-120C and -120D missiles, the test squadron did not execute a live fire employment testing with those two missile types. In coordination with DOT&E, the test team has deferred these live fire tests to follow-on testing. The Legion Pod Block 1.5 Force Development Evaluation was adequate to determine operational effectiveness, but not adequate to determine system suitability or survivability.

Performance

Effectiveness

The Legion Pod Block 1.5 is operationally effective, providing the F-15C a new capability to engage airborne targets. The one effectiveness challenge noted with the Legion Pod is an angle-of-attack restriction imposed on the F-15 when carrying the pod. Funding was not available to perform the flight sciences missions required to clear the Legion Pod to basic aircraft limits. As a result, the F-15C with the Legion Pod is limited in angle-of-attack and unable to operate in the entirety of the aircraft's basic envelope.

Suitability

Operational suitability of the Legion Pod is currently unknown due to the lack of sufficient data collected during the Force Development Evaluation. Testers highlighted three Line Replaceable Units in the Legion Pod as having potentially high failure rates but there were insufficient data to determine the reliability of the Environmental Cooling Unit, Infrared Receiver, and Inertial Measurement Unit. The Legion Pod experienced numerous problems related to connectivity with the Data Transfer Module, which required the pilot to do a hard reset of the Legion Pod.

Survivability

The 53d Wing conducted an incomplete Cooperative Vulnerability and Penetration Assessment and Adversarial Assessment of the Legion Pod, precluding an adequate survivability assessment of the Legion Pod in a cyber-contested environment.

Recommendations

(U) The Air Force should:

1. Plan and fund flight science missions to expand the operational envelope of the F-15 with the installed Legion Pod.
2. Continue to collect suitability data for the Legion Pod, to include the Environmental Cooling Unit, Infrared Receiver, and Inertial Measurement Unit to determine if the system is suitable for operational use.
3. Investigate the cause of the Data Transfer Module-induced resets and provide a correction in a future release of the Operational Flight Program or Legion Pod software.
4. Plan, fund, and complete a cybersecurity assessment of the Legion Pod.

F-16 Radar Modernization Program

The APG-83 F-16 Radar Modernization Program (RMP) full-rate production decision, scheduled in March 2023, is currently at risk due to the Air Force's insufficient coordination and funding for the various hardware upgrades required to modernize the aircraft, as well as a failure to plan, schedule, and resource an adequate APG-83 IOT&E through the F-16 Integrated Test and Evaluation structure. In March 2021, the Air Force approved the F-16 RMP to enter Milestone C.

System Description

The APG-83 Scalable Agile Beam Radar (SABR) is a multifunction Active Electronically Scanned Array (AESA) radar intended to replace the legacy APG-68 radar. It provides F-16 pilots with air-to-air and air-to-ground situational awareness, high-resolution synthetic aperture radar mapping, fire control, and datalink support to air-to-air missiles.

Program

The APG-83 F-16 RMP is an Acquisition Category II program. The program does not have an approved Test and Evaluation Master Plan (TEMP). The Air National Guard acquired and is fielding 72 APG-83 radars with initial capability to meet a U.S. Northern Command Joint Emergent Operational Need (JEON) for homeland defense.

This initial JEON fielding was not on DOT&E oversight and included Phase 1 and Phase 2 developmental and operational testing of partial APG-83 capabilities and reliability enhancements. The JEON program was originally planned for completion in July 2021, but was delayed due to production issues and may continue into 2022.

The Air Force approved the F-16 RMP to enter at Phase 3 and Milestone C in March 2021, based on the JEON Phase 1 and Phase 2. The F-16 RMP, which is on DOT&E oversight, intends to deliver full APG-83 capability and begin purchasing up to 450 radars for active duty Air Force F-16s. The Program Office is currently planning on making a F-16 RMP full-rate production decision in March 2023.

Major Contractor

Northrop Grumman Mission Systems – Linthicum, Maryland.

Test Adequacy

The test adequacy of the F-16 RMP cannot yet be assessed since the Air Force has not submitted a TEMP, Test Strategy, or Test Plan for approval. To date, there have been working-level discussions between the Program Office, the Operational Test Agency, and DOT&E to develop an adequate test strategy and plan.

The Air Force has not adequately resourced the program nor submitted a TEMP for approval that includes an IOT&E and FOT&E plan with resources to support operational testing. There is very high risk to the F-16 RMP full-rate production timeline based on this failure to develop and resource an adequate IOT&E plan.

Performance

Effectiveness

The operational effectiveness assessment of the F-16 RMP is pending approval of an adequate TEMP and Test Plan, completion of IOT&E, and subsequent analysis of operational testing results.

Suitability

The operational suitability assessment of the F-16 RMP is pending approval of an adequate TEMP and Test Plan, completion of IOT&E, and analysis of operational testing results.

Survivability

The survivability assessment of the F-16 RMP in a cyber-contested environment is pending approval of an adequate TEMP and Test Plan, completion of IOT&E, and analysis of operational testing results.

Recommendation

1. The Air Force should develop and deliver an adequate TEMP and Test Plan for the F-16 RMP IOT&E to DOT&E for review and approval as soon as possible to meet the full-rate production decision scheduled for March 2023.

F-22A – Raptor Advanced Tactical Fighter Aircraft

The F-22 Raptor Release 1 (R1) Force Development Evaluation (FDE) will need to address several challenges to meet operational effectiveness and suitability requirements. A major limitation to delivering the originally planned F-22 R1 capability include Federal Aviation Administration restrictions that prohibit the use of Link-16 transmit capabilities. A final evaluation of F-22 R1 effectiveness, suitability, and survivability should be available in early CY22 pending completion of the Phase 2 dedicated mission trials and cybersecurity testing.

System Description

The F-22A Raptor is an air superiority, fifth-generation fighter aircraft that delivers low observability to threat radars, high maneuverability, sustained supersonic speed, and advanced integrated avionics. Units equipped with the F-22A conduct offensive counter-air, defensive counter-air, and limited ground attack missions in high-threat environments. The latest hardware and software modernization efforts, termed R1, provide capabilities detailed in the Controlled Unclassified Information edition of this report as per the F-22 Security Classification Guide.

Program

The F-22A Raptor started as a Major Defense Acquisition Program, with the first production aircraft fielding in 2003. The Air Force has since been implementing hardware and software modernization efforts known as capability "Releases" using rapid prototyping and rapid fielding acquisition authorities. The first such program is the F-22 Raptor R1 FDE. The Tactical Link-16 (TACLINK) and Tactical Mandates (TACMAN) Test and Evaluation Master Plans, approved by DOT&E in 2018, provide the capstone test strategy and concepts for the R1 FDE test plan approved by DOT&E in July 2020. TACLINK and TACMAN were originally planned as Acquisition Category II programs but will now deliver capability incrementally through the Section 804 Middle Tier of Acquisition (MTA) F-22 Rapid Prototyping and F-22 Rapid Fielding MTA programs. Since R1 only provides a fraction of the overall TACMAN and TACLINK capabilities, the Air Force tasked the USAF Warfare Center, 53rd Wing to execute the R1 FDE.

Major Contractor

Lockheed Martin Aeronautics Company – Fort Worth, Texas.

Test Adequacy

DOT&E approved the USAF Warfare Center F-22 Raptor R1 FDE test plan as adequate for evaluating current R1 capabilities. The R1 test design is divided into three phases. Phase 1 includes early operational test support to developmental testing and operational testing with early, non-fielding capabilities. Phase 2 includes dedicated operational testing during mission trial events, and Phase 3 includes post-fielding monitoring. With limited F-22 developmental testing resources, the early operational test support in Phase 1 supplemented developmental testing by providing necessary assets, generating a significant amount of additional data, and incorporating testing in an operational environment for early R1 releases. R1 developmental testing was completed on August 16, 2021 with a total of 263 sorties and 308 flight hours. Software development included 14 software drops (at an agile 4-6 week release cycle) and over 3,600 hours of testing. During Phase 1 FDE, operational test aircraft accumulated 286 sorties and 332 flight hours. Weapons employment included successful live drops of the Joint Direct Attack Munition, and live shots with the Advanced Medium-Range Air-to-Air Missile and Air Intercept Missile (AIM)-9X Sidewinder. Phase 2 FDE operational testing started in August 2021, and will include three offensive counter-air and two defensive counter-air mission trial events at the Nevada Test and Training Range, Nevada. These mission trial events are to assess R1 capabilities in an operationally representative threat environment, and in the configuration Air Combat Command will release to the field. R1 cybersecurity testing focuses on the F-22 Integrated Maintenance Information System and is due to complete in early CY22.

Performance

Effectiveness

F-22 R1 will need to continue to address several challenges to meet operational effectiveness requirements. Phase 1 testing identified areas of concern that will continue to be assessed during Phase 2 testing. A major limitation to delivering the originally planned F-22 R1 capability are the Federal Aviation Administration restrictions that prohibit the use of Link-16 transmit. A final evaluation of the F-22 R1 operational effectiveness in mission-level, advanced threat, and operationally realistic scenarios should be available in early CY22 pending completion of the Phase 2 dedicated mission trials.

Suitability

F-22 R1 will need to continue to address several challenges to meet operational suitability requirements. In accordance with the F-22 Security Classification Guide, additional details are provided in the Controlled Unclassified Information edition of this report.

Survivability

The survivability assessment of F-22 R1 in a cyber-contested environment is pending completion of R1 cybersecurity testing, scheduled in early CY22.

Recommendation

1. The Air Force should continue to resolve the identified deficiencies and imposed limitations to successfully demonstrate the F-22 R1 warfighting capability.

Family of Advanced Beyond Line-of-Sight Terminals (FAB-T)

The Family of Advanced Beyond Line-of-Sight Terminals (FAB-T) IOT&E is in progress and scheduled to be completed in FY22. In accordance with the FAB-T Security Classification Guide, the updates on the FAB-T acquisition, test adequacy and operational performance in supporting critical nuclear, command, control and communications are provided in the Controlled Unclassified Information edition of this report.

Major Contractor

Raytheon Technologies Corporation Missiles and Defense – Marlborough, Massachusetts.

Recommendations

The Air Force should:

1. Update the FAB-T TEMP with the latest plan and schedule to verify the correction of FAB-T deficiencies and to complete testing of FAB-T capabilities delayed to FOT&E.

The Air Force and Space Force 4th Test and Evaluation Squadron should:

1. Complete development and verification, validation and accreditation of the threat hardware-in-the-loop modeling and simulation needed for completing the FAB-T IOT&E.
2. Complete the FAB-T IOT&E with user community support.

Global Positioning System (GPS) Enterprise

The U.S. Space Force successfully upgraded the current Operational Control System (OCS) Architecture Evolution Plan with M-code Early Use (MCEU) and Contingency Operations (COps), enabling command and control of core Military Code (M-code) capability from the existing GPS constellation as well as the employment of GPS III satellites for constellation sustainment. Full control of modernized civil and M-code signals and navigation warfare functions, as well as improved cybersecurity, continue to be delayed due to ongoing development and deployment delays of the next generation Operational Control System (OCX), along with delays in the fielding of M-code capable receivers for use by the U.S. and allied warfighters.

System Description

The GPS Enterprise is a satellite-based global radio navigation system of systems intended to provide accurate and secure positioning, navigation, and timing (PNT) information to military and civilian users worldwide. The GPS Enterprise consists of three operational segments: space, control, and user segments. The space segment includes the GPS constellation of 31 satellites. The control segment (primary and alternate) operates the GPS constellation; supports launches, anomaly resolution, and disposal operations; and tasks navigation warfare effects in support of Combatant Commands. The user segment includes the Military GPS User Equipment (MGUE) intended to modernize military GPS receivers, including the ability to receive M-code.

Program

The GPS Enterprise consists of multiple programs pursuing a wide range of acquisition strategies to advance the space, control, and user segments:

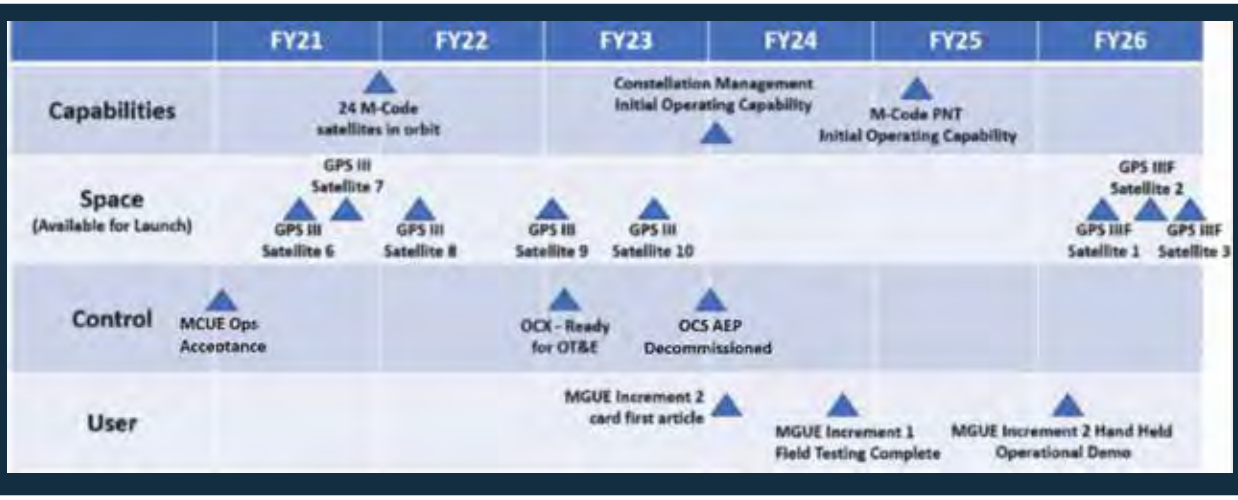
- GPS III – Acquisition Category IC program entered Milestone C in January 2011. The U.S. Space Force has successfully launched five GPS III satellites since 2018 and plans to launch five more by 2025.
- GPS III Follow-On Production (GPS IIIF) – Acquisition Category IB program, intended to provide enhanced regional military protection signals and support for search and rescue services. The Air Force made the GPS IIIF Milestone C decision in July 2020 based on the completion of Critical Design Review and prior to development or testing of any GPS IIIF satellites. The first launch is expected in 2026, followed by 21 additional GPS IIIF satellites over the subsequent decade.

- Operational Control System (OCS) Architecture Evolution Plan fielded two Acquisition Category III upgrades: M-code Early Use (MCEU) to command and control core M-code capability from the existing GPS constellation (GPS IIR-M, GPS IIF, and GPS III), and Contingency Operations (COps), delivered in March 2020 as a "bridge capability" and risk mitigation effort to enable employment of GPS III satellites using legacy and M-code signals for operational constellation sustainment.
- MGUE Increment 1 – Acquisition Category IC program entered Milestone B in January 2017 (relieved of Milestone C requirements). The program is intended to deliver M-code capability, which will improve GPS signal availability in degraded threat environments. Ongoing delays of final software and hardware builds by MGUE Increment 1 vendors continue to cause delays to MGUE Increment 1 lead platform test schedules, which increases the risk for platforms seeking to implement MGUE. Consequently, the Army and Marine Corps decided not to field their respective platforms with the ground-based MGUE Increment 1 card. Due to Application-Specific Integrated Circuit obsolescence and limited production, the Services have turned to commercially available, MGUE-derived M-code receivers to continue meeting PNT requirements. Those systems will undergo operational testing outside of the MGUE Increment 1 program of record.
- MGUE Increment 2 – Middle Tier Acquisition program, intended to support low-power applications such as guided munitions and hand-held devices, and address MGUE Increment 1 Application-Specific Integrated Circuit hardware obsolescence.
- Operational Control System (OCX) – Acquisition Category ID program entered Milestone B in June 2017 (relieved of Milestone C requirements) and is intended to provide full control of modernized civil and M-code signals and navigation warfare functions, as well as improved cybersecurity. The subsequent OCX Block 3F upgrade will allow OCX to command and control GPS IIIF satellites. The U.S. Space Force plans to replace OCS with OCX in FY23 following a successful IOT&E in January 2023.

DOT&E approved the GPS Enterprise Test and Evaluation Master Plan (E-TEMP) Revision B on August 9, 2018 and the partial E-TEMP Revision C on August 25, 2021. The Program Office continues to revise the GPS E-TEMP to align space threat requirements, address cyber testing, and enable the concurrent delivery of OCX, MGUE Increment 2, upgraded Nuclear Detonation Detection System control system, GPS IIIF satellites, and OCX Block 3F. Figure 1 summarizes the GPS Enterprise major events and testing through FY26. The next GPS operational test is an OCX cyber assessment scheduled for late 2022, followed by the initial operational testing of OCX in January 2023 and GPS Enterprise IOT&E later in 2023. The MGUE Increment 1 aviation/maritime card will undergo operational testing in 2024 as integrated on the B-2 platform although, given the sundown plans for the Air Force to retire the B-2 in the early 2030 timeframe, any future schedule slips may warrant the Air Force to select another platform to support the

Figure 1.

GPS Enterprise Schedule (FY21 to FY26)



planned integration of the MGUE Increment 1 card. The GPS Enterprise Multi-Service Operational Test and Evaluation (MOT&E), designed to assess all three third generation segments together, is scheduled for 2025.

Major Contractors

Space Segment

- Block IIR/IIR-M/III/IIIF 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 – Denver, Colorado
- OCX: Raytheon Technologies, Intelligence, Information, and Services – Aurora, Colorado
- OCX 3F: Raytheon Technologies, Intelligence, Information, and Services – Aurora, Colorado

User Segment (MGUE Increment 1 and 2

- MGUE Increment 1 and 2:
  - L3Harris Technologies, Inc. – Anaheim, California
  - Raytheon Technologies, Space and Airborne Systems – El Segundo, California
  - BAE Systems – Cedar Rapids, Iowa
- MGUE Increment 2 Handheld Device:
  - Technology Advancement Group – Dulles, Virginia
  - Raytheon Technologies, Space and Airborne Systems – El Segundo, California
  - BAE Systems – Cedar Rapids, Iowa

Test Adequacy

In 2020, the U.S. Space Force Space Training and Readiness Space Delta 12, 4th Test and Evaluation Squadron conducted operational and cybersecurity testing of the two upgrades to OCS, COps, and MCEU at the GPS Master Control Station at Schriever Space Force Base, the GPS Alternate Master Control Station at Vandenberg Space Force Base, and the GPS monitoring and ground antenna facility at Canaveral Space Force Station. The 4th Test and Evaluation Squadron also conducted cyber-resiliency testing of the GPS III satellite simulator at a Lockheed contractor facility. Operational and cyber testing were conducted in accordance with the DOT&E-approved TEMP and test plans.

Performance

Effectiveness

The OCS Architecture Evolution Plan upgrades, MCEU, and COps, are operationally effective, enabling the constellation to use both legacy signals and M-code signals. The GPS operators at the Master Control Station can successfully command and control the GPS III satellites as part of the full GPS constellation, allowing the OCS to produce a global core M-code signal in space usable by M-code capable receivers. While the U.S. Space Force demonstrated the ability to employ both legacy (pre-M-code) signal and M-code signals through MCEU, the lack of M-code capable receivers limits the M-code use by U.S. and allied warfighters.

Suitability

The GPS III, OCS Architecture Evolution Plan upgrades, COps, and MCEU are operationally suitable. While operator surveys identified concerns with initial training, documentation, and the user interface, COps and MCEU are fully mission-capable. Future operational tests will continue to focus on training, job aids, and technical order documentation.

Survivability

COps and MCEU are vulnerable in a cyber-contested environment. Despite the lack of specifically defined cyber survivability requirements, the GPS Enterprise will operate in a cyber-contested environment, warranting an adequate cyber assessment of the GPS Enterprise, to include GPS vehicles prior to launch. The Program Office continues to develop a space threat plan to adequately evaluate the survivability of the entire GPS Enterprise in a contested space environment that includes kinetic engagements, cyber, electromagnetic spectrum fires, nuclear, and directed energy weapons.

Recommendations

The U.S. Space Force should:

1. In coordination with DOT&E and respective Service operational test agencies, support the development of operational test procedures to standardize the characterization of the GPS M-code derived PNT performance of all DOD systems equipped with M-code capable GPS receivers.
2. Continue to plan to conduct operational testing of the GPS Enterprise against current and emerging space threats to assess its ability to support DOD missions in a contested space environment.
3. Plan to conduct regular Enterprise-wide testing events leveraging existing exercises and navigation warfare events to gauge the GPS Enterprise's ability to support the warfighter using the new M-code capabilities.
4. Plan to conduct a no-notice transfer from the Master Control Station to the Alternate Master Control Station, during the GPS Enterprise IOT&E of the space segment and OCX run control segment, to verify system survivability.
5. Include cyber survivability requirements in all GPS Enterprise acquisition programs to ensure the Enterprise is designed to respond to adversarial threats.

HH-60W Jolly Green II

The Air Force is tracking several deficiency reports that increase the HH-60W's risk to meeting operational effectiveness and survivability requirements. There are no significant risks to the HH-60W demonstrating operational suitability in IOT&E. Delays in correcting deficiencies identified in developmental testing increase risk to the schedule for IOT&E, initial operational capability, and full-rate production decision.

System Description

The Air Force HH-60W Jolly Green II is a new-build, dual-piloted, twin-engine helicopter that will replace the HH-60G. The aircraft is designed to extend the combat radius without aerial refueling and conduct an out-of-ground-effect hover at its mid-mission gross weight. The HH-60W design is intended to enhance survivability while units equipped with the HH-60W recover isolated personnel from hostile or denied territory, day or night, in adverse weather, and in a full range of threat environments from terrorist to chemical, biological, radiological, and nuclear. Commanders will also employ the HH-60W to support humanitarian missions, civil search and rescue, disaster relief, and medical and non-combatant evacuation operations.

Program

HH-60W is an Acquisition Category IC program. DOT&E approved the LFT&E Strategy in April 2015 and the Milestone C Test and Evaluation Master Plan in January 2020. DOT&E approved portions of the Air Force Operational Test and Evaluation Center (AFOTEC) IOT&E plan to support pre-IOT&E test events because challenges with several critical capabilities delayed the start of dedicated IOT&E. The program plans an initial operational capability decision in May 2022 and the full-rate production decision in August 2022.

Major Contractor

Sikorsky Aircraft Corporation – Stratford, Connecticut.

Test Adequacy

The HH-60W IOT&E is based on two-ship mission scenarios in a variety of environmental, threat, and mission conditions. Although AFOTEC planned to start dedicated IOT&E in July 2021, the program does not expect availability of several crucial operational capabilities before February 2022. These delayed capabilities are

compressing the schedule available for IOT&E before the planned initial operational capability and full-rate production decisions.

AFOTEC began collecting preliminary data on HH-60W operational performance during the 41st Rescue Squadron's participation in the Red Flag Rescue exercise in May 2021 and has continued observing training and familiarization operations, collecting data when operationally relevant. Analysis is ongoing to determine what data will be acceptable for evaluation. AFOTEC also conducted the first of three phases of cybersecurity testing from July to August 2021.

The Air Force continued analytical efforts to evaluate aircraft system-level vulnerability and force protection against kinetic threats, directed energy weapons, electromagnetic, and chemical, biological, radiological, and nuclear threats. The Air Force plans to complete an infrared signature analysis to evaluate the effectiveness of the upturned exhaust system.

Performance

While the unit equipped with HH-60W demonstrated the capability to support personnel recovery missions, the Air Force is tracking several deficiency reports that increase the HH-60W's risk to meeting operational effectiveness requirements. Preliminary data from the first unit's aircraft operations suggest the HH-60W should be able to meet most operational suitability requirements, to include reliability, availability, and maintainability. The program will need to mitigate deficiencies in the countermeasures dispenser set and supply operationally representative software and mission data load for the radar warning receiver to enable an adequate HH-60W survivability assessment in a contested environment. In accordance with the HH-60W Security Classification Guide, additional details are provided in the Controlled Unclassified Information edition of this report.

Recommendation

1. The Air Force should update the test, fielding, and acquisition schedules to account for developmental delays and allow for an adequate assessment of HH-60W operational effectiveness, suitability, and survivability.

Joint Cyber Warfighting Architecture (JCWA)

United States Cyber Command (USCYBERCOM) continues to define the Joint Cyber Warfighting Architecture (JCWA) concept, but a lack of governance has led to an ad-hoc alignment of T&E efforts for the systems JCWA encompasses. This will result in fielding capabilities without demonstrating or understanding their contribution to JCWA operational effectiveness, suitability, or survivability. USCYBERCOM has not designated an Operational Test Agency to define and develop metrics needed to conduct integrated JCWA-level OT&E. T&E strategies and processes are maturing, but not fast enough to support initial delivery of capability and features.

System Description

JCWA is designed to collect, fuse, and process data and intelligence to provide situational awareness and battle management at the strategic, operational, and tactical levels while also enabling access to a suite of cyber capabilities needed to rehearse and then act in cyberspace. Given this construct, JCWA is also expected to illuminate cyber capability shortfalls to guide the acquisition of needed cyber warfighting capabilities.

Program

JCWA is not a program of record itself but currently encompasses the following four acquisition programs:

- **Unified Platform (UP)** will act as a data hub for JCWA, unifying disparate cyber capabilities in order to enable full-spectrum cyberspace operations.
- **Joint Cyber Command and Control (JCC2)** will provide situational awareness, battle management, and cyber forces' management for full-spectrum cyber operations.
- **Persistent Cyber Training Environment (PCTE)** will provide individual and collective training as well as mission rehearsal for cyber operations.
- An access component will provide additional capability for cyber operations.

USCYBERCOM relies heavily on the Services for acquisition of the programs that comprise JCWA. To guide these individual acquisition programs, USCYBERCOM established the JCWA Integration Office and the JCWA Capabilities Management Office. Both lack the authority or resources to effectively manage critical JCWA-level activities. Each program has different release and deployment schedules, and there are no validated JCWA-level mission thread requirements or plans for an integrated JCWA-level operational test.

Major Contractors

Each Service uses a multitude of contracts and contractors for the acquisition of UP, JCC2, PCTE and JCWA's access component. A complete list of major contractors is provided in the Controlled Unclassified Information edition of this report.

Test Adequacy

In FY20, the JCWA Integration Office initiated the development of a JCWA T&E strategy by establishing multiple working groups to inform test infrastructure requirements and develop test scenarios based on mission threads. The development of the JCWA test strategy is still maturing and needs greater support from USCYBERCOM and the Services to plan and resource dedicated operational testing to validate COF mission thread effectiveness, suitability, and survivability in support of the deployment of capability. In parallel, each of the programs is developing T&E strategies independent of the JCWA construct, which may lead to inefficiencies and test inadequacies. In FY21, multiple JCWA components conducted early program-level T&E, including early cybersecurity assessments. DOT&E informed and monitored testing conducted to date and will use the data in its operational assessments where appropriate.

Performance

Effectiveness and Suitability

Not enough data have yet been collected to enable a preliminary assessment of the JCWA-level operational effectiveness and suitability or the performance of its individual components.

Survivability

No data have yet been collected to enable an evaluation of JCWA mission resilience in a cyber-contested environment.

Recommendations

1. The DOD should identify, resource, and empower a JCWA-level acquisition management organization to coordinate the integration of JCWA capability. Lack of JCWA governance has resulted in ad-hoc efforts to synchronize T&E across the architecture.
2. USCYBERCOM, in coordination with DOT&E and the Services, should develop, resource, and execute a JCWA-level T&E strategy.
3. USCYBERCOM, in coordination with DOT&E, the National Security Agency, and the Services, should plan and conduct robust cyber testing of JCWA and its subcomponents.

KC-46A Pegasus

Air Mobility Command issued an interim capability release for the KC-46A to support limited operational refueling taskings in 2021, but shortfalls in the Remote Vision System (RVS), refueling boom, and several systems that provide the aircrew threat situational awareness prevent the completion of IOT&E and a full-rate production decision until FY24. The Air Force Operational Test and Evaluation Center (AFOTEC) has completed 60 percent of effectiveness testing and 93 percent of suitability testing.

System Description

The KC-46A aerial refueling aircraft is a modified Boeing 767-200ER commercial airframe with military and technological upgrades required to perform aerial refueling of tactical and strategic aircraft, airlift and aeromedical evacuation, and to provide force protection against kinetic and chemical, biological, radiological, and nuclear threats. Notable upgrades include a fly-by-wire refueling boom, centerline and wing pod refueling drogues, a dual remote Air Refueling Operator's Station (AROS) enabled by an exterior RVS, additional fuel tanks in the body, a boom refueling receiver receptacle, a 787 digital cockpit update, Large Aircraft Infrared Countermeasures, a modified ALR-69A radar warning receiver (RWR), and Tactical Situational Awareness System (TSAS). The KC 46A cargo bay is designed to accommodate palletized cargo, aeromedical evacuation equipment, and roll-on command, control, and communications gateway payloads.

Program

The KC-46A Pegasus is an Acquisition Category IC program intended to be the first increment of 179 replacement tankers for the fleet of more than 400 KC-135 and KC-10 tankers. DOT&E approved the Milestone C Test and Evaluation Master Plan update in 2016 and the IOT&E test plan in April 2019. In a May 2020 memorandum, DOT&E communicated to the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics that DOT&E will not submit an IOT&E report on KC-46A until operational testing of a production-representative RVS is complete. The Air Force expects a corrected RVS version 2.0 to be ready for operational testing in mid-FY24. Air Mobility Command issued interim capability releases for KC-46A refueling taskings using its centerline drogue system in July 2021 and using the boom in August 2021.

Major Contractor

The Boeing Company, Commercial Aircraft, in conjunction with Defense, Space & Security – Seattle, Washington.

Test Adequacy

IOT&E has been ongoing since May 2019. In FY21, AFOTEC completed 60 percent of the effectiveness test points in accordance with the DOT&E-approved test plan; 16 percent are deferred, pending long-term updates to the boom, RVS, Wing Aerial Refueling Pod (WARP), RWR, and TSAS. Aeromedical and cargo operations testing is nearly complete.

During IOT&E, the Air Force collected and adjudicated suitability data during over 9,660 flight hours on four test aircraft, exceeding the minimum planned 1,250 flight hours for IOT&E. Testing and normal flight operations (21,419 flight hours on 46 aircraft) have accumulated ten times the required flight hours for an adequate suitability assessment, with 23 of 24 specific maintenance demonstrations completed. The Program Office commissioned a review of the entire Pegasus fleet's maintenance data to help guide future decisions on the program.

The KC-46A program completed continuous wave immersion electromagnetic pulse risk-reduction testing in November 2020 and some passive system testing in August 2021.

AFOTEC conducted cooperative cybersecurity testing in October 2020 but was unable to adhere to the test plan detailed in the Controlled Unclassified Information edition of this report. AFOTEC also conducted part of a cybersecurity Adversarial Assessment in July 2021, which experienced similar problems. Planning for a second phase of Adversarial Assessment scheduled for FY24 is underway.

Future assessments will be focused on solutions to fleetwide maintenance and supply issues, as well as already planned changes to the existing baseline (e.g., boom upgrades, WARP, and RVS upgrades).

Performance

Effectiveness

Testing to date identified shortfalls that require correction to mitigate the risk to achieving operational effectiveness in IOT&E:

- AFOTEC identified some shortfalls in the AROS functions that increase operator workload, which may degrade operational effectiveness in certain conditions. Refueling in lighting conditions that require the long-wave infrared sensor is prohibited until RVS 2.0 is complete. Boom refueling of certain platforms will resume after the boom actuator redesign. WARP capability will enter IOT&E in FY22, but an observation from developmental testing is that high receiver closure-to-contact speeds increase the likelihood of damage to drogue baskets.
- Aeromedical evacuation operations have progressed to the transport of actual patients, during which AFOTEC observed minor problems with loading patients and administering intravenous fluids.
- Cargo operations made progress, but KC-46A crews must reject a portion of standard cargo pallets due to KC-46A restrictions on pallet weight distribution. Aircrews also report excessive workload and delays in determining if proposed cargo is safe for transport in the aircraft and interfacing with cumbersome aircraft cargo management systems.

Suitability

The KC-46A is not yet meeting all operational suitability requirements, and therefore there is risk to achieving operational suitability in IOT&E:

- The program's reliability growth plan will likely meet suitability requirements by 50,000 fleet flight hours. The fleet suitability metrics, collected so far, are similar to those observed on IOT&E test aircraft.
- The following suitability metrics do not yet meet thresholds: operational availability; mission capability rate (MCR); maintenance man hours per flight hour; mean time between maintenance; and break rate. Factors most recently influencing operational availability and mission capability rates include insufficient cargo configuration guidance, restrictive fuel tank inerting procedures, and reliability problems with the auxiliary power unit drain mast and surge boot assembly.
- Operator surveys describe Type 1 training as inadequate to support the operation of multiple datalink systems to support mission readiness for net-ready taskings.

Survivability

The KC-46A needs to overcome several challenges to meet some of its survivability requirements. In accordance with the KC-46 Security Classification Guide, additional details are provided in the Controlled Unclassified Information edition of this report. The survivability of the KC-46A in a nuclear threat-induced environment cannot be determined without the active system test, scheduled to be completed in 3QFY22. Electromagnetic pulse testing to date indicates the shielding integrity of the aircraft is good, with no obvious shielding gaps. In addition, maintenance of the aircraft does not degrade electromagnetic pulse hardness.

Recommendations

The Air Force should:

1. Improve training and technical data to enable timely and repeatable configuration of aircraft data systems such as the military data network to support mission readiness for net-ready taskings.
2. Continue to redesign the RVS and the refueling boom to facilitate their readiness for operational testing, scheduled in FY24.
3. Address the recommendation highlighted in the Controlled Unclassified Information edition of this report to support survivability of the KC-46A.

Massive Ordnance Penetrator Modification

The Air Force conducted testing of the Large Penetrator Smart Fuze (LPSF) integrated into the Massive Ordnance Penetrator (MOP) against low-fidelity subscale and full-scale targets. The Air Force must also execute the planned subscale tests and a final full-scale qualification event to determine MOP operational effectiveness. The Air Force delayed the fielding of the LPSF-enabled MOP from FY22 to at least FY25 due to delays in constructing the required target surrogates.

System Description

The Guided Bomb Unit (GBU)-57 MOP is a large, GPS-guided, penetrating weapon designed to attack Hard and Deeply Buried Targets (HDBTs) such as bunkers and tunnels. The GBU-57 warhead is intended to be more lethal than its predecessors, the GBU-28 and GBU-37. The LPSF integrates and advances smart fuze capability into the MOP warhead, providing increased probability of kill against HDBTs by minimizing the effects of target intelligence uncertainty. The B-2 Spirit is the only aircraft in the Air Force inventory programmed to employ the MOP.

Program

The MOP was developed from an Air Force-led Quick Reaction Capability (QRC) as a SECDEF special interest effort. The MOP transitioned to the Air Force as an Acquisition Category IC program in August 2017. The Air Force established the LPSF QRC program in August 2018 to respond to an Urgent Operational Need, validated in July 2018, to integrate and qualify a smart fuze capability into the MOP. This upgrade provides the capability to hold additional high-value HDBTs with limited threat intelligence at risk.

The Air Force was on track to field an LPSF-enabled MOP in FY22. Contracting award delays and significant Defense Threat Reduction Agency (DTRA) target construction overruns in the HDBT Defense System Program Element resulted in the Air Force Program Executive Officer for Weapons pulling funds from the full-scale LPSF MOP testing. Based on current funding options, the LPSF MOP fielding will be in FY25 or later.

Major Contractor

The Boeing Company, Defense, Space & Security – St. Louis, Missouri.

Test Adequacy

The Air Force conducted LPSF QRC testing in accordance with the DOT&E-approved Smart Fuzing Test Strategy, dated December 2020. The GBU-57 MOP intends to complete accuracy validation drops in a contested GPS environment during 1QFY22. In December 2020, the Air Force conducted one live weapon drop from a B-2 on a simple tunnel target to evaluate the initial LPSF design. In August 2021, the Air Force conducted one live weapon drop from a B-2 to validate MOP performance. In FY21, the Air Force completed 13 of 16 sled tests.

Prior to funding cuts, delays with contracting processes and internal test plan reviews for subscale and full-scale targets constructed by DTRA resulted in construction delays and cost overruns. Target construction was also delayed by pandemic-induced supply and labor shortages and the loss of priority status at the test range.

The next phase of the program, currently unfunded, intends to finalize smart fuze software, improve weaponeering tactics, and validate through demonstration lower-risk smart fuze capability against a full-scale, high-fidelity underground target.

Performance

In accordance with the MOP Security Classification Guide, preliminary analysis of effectiveness and suitability is provided in the Controlled Unclassified Information edition of this report. The survivability assessment of MOP in a contested environment is classified.

Recommendations

The Air Force should:

1. Revalidate the Urgent Operational Need requirement for the LPSF QRC against legacy and pacing threats.
2. Complete the LPSF testing to validate the ability to meet Combatant Command requirements.
3. Develop and submit a MOP test plan for DOT&E approval to enhance communication and coordination between stakeholders and provide decision-makers with better visibility of the MOP program.

DTRA should:

1. Evaluate and expedite contracting and test plan review processes to minimize delays to target construction.

MH-139A Grey Wolf

Supplemental type certifications for the MH-139A continued to slip, further delaying developmental testing of military capabilities. Additionally, the contractor has imposed new flight envelope restrictions on the aircraft that will limit the aircraft's capability to perform basic flight maneuvers, if not mitigated. The MH-139A program needs to address several additional challenges to mitigate the risk to meeting operational effectiveness, suitability, and survivability requirements.

System Description

The MH-139A Grey Wolf is a dual-piloted, twin-engine helicopter based on the commercial AW139 with added military capabilities in communication, navigation, identification, and survivability. The Air Force intends for the MH-139A to replace the UH-1N to provide rapid transport capability for two primary commands.

Program

MH-139A is an Acquisition Category IB program. DOT&E approved the Milestone B Test and Evaluation Master Plan in June 2018 and the Alternative LFT&E Strategy in May 2019. In April 2021, the program reported an Acquisition Program Baseline breach to the service acquisition executive, requesting to delay the Milestone C from September 2021 to January 2023.

The MH-139A acquisition strategy relies on initial contractor flight testing to obtain a series of civil supplemental type certification approvals before the military flight release required for government developmental test.

Major Contractor

The Boeing Company, Defense, Space & Security – Ridley Park, Pennsylvania.

Test Adequacy

The Air Force participated in contractor ground and flight testing throughout FY21 at Duke Field, Florida, and at contractor facilities in Philadelphia, Pennsylvania that will support the supplemental type certification approvals, specification compliance, and airworthiness. The military utility of this phase of testing was limited.

The 47th Cyberspace Test Squadron conducted Cooperative Vulnerability Identification developmental testing on the aircraft and ground support equipment that will support adversarial developmental testing in FY22.

The Air Force Operational Test and Evaluation Center published three periodic reports in FY21 summarizing the observations from contractor testing and site visits to domestic and foreign military, government, and commercial operators of the AW139 that identified best practices as well as potential mission capability risks and mitigations.

The 704th Test Group executed live fire testing of the installed armor, aircraft structure against incendiary rounds for fire risk, and main and tail rotor blades at Aberdeen Proving Ground, Maryland and Wright-Patterson AFB, Ohio in accordance with DOT&E-approved test plans.

The Program Office is developing plans to perform infrared signature and electromagnetic pulse testing to collect data for evaluation of aircraft survivability.

Performance

The MH-139A deficiencies, identified in ground and flight testing to date, combined with new flight envelope restrictions, increase the MH-139A risk to meeting operational effectiveness requirements. Concerns persist from the FY20 annual report regarding the effects of the cabin layout on supporting employment of armed tactical response forces as well as flight manual restrictions on takeoffs in crosswinds, near obstacles, in degraded visual environments, and austere landings. The Program Office also needs to address several challenges for the MH-139A to be operationally suitable and survivable. In accordance with the MH-139A Security Classification Guide, additional details are provided in the Controlled Unclassified Information edition of this report.

Recommendations

The Air Force should:

1. Update the Test and Evaluation Master Plan to reflect the new schedule.
2. Evaluate aircraft capability in degraded visual environments and austere landings prior to IOT&E.

Presidential and National Voice Conferencing (PNVC) Integrator

In August 2021, DOT&E conditionally approved the Presidential and National Voice Conferencing (PNVC) Integrator Test and Evaluation Master Plan supporting the Milestone B/C decision, MOT&E, followed by a Limited Deployment Decision, Trial Period, and Operational Acceptance. The program plans to start a Multi-Service Operational Test and Evaluation in FY22. In accordance with the PNVC Integrator Security Classification Guide, the PNVC Integrator system description as well as updates on the PNVC Integrator acquisition, test adequacy and operational performance to support critical nuclear, command, control and communications are provided in the Controlled Unclassified Information edition of this report.

Major Contractor

Raytheon Technologies Corporation Missiles and Defense - Marlborough, Massachusetts.

Recommendations

1. The PNVC Program Office and Space Force should address the recommendations provided in the Controlled Unclassified Information edition of this report.

Small Diameter Bomb Increment II

The Small Diameter Bomb (SDB) Increment II program continued integration testing on the F/A-18E/F and started early flight testing on the F-35. In FY21, the Navy executed four F/A-18E/F missions with the SDB II as part of the quick reaction assessment, but all four were unsuccessful.

System Description

The SDB II, also known as the GBU-53/B Stormbreaker, is a 250-pound class, air-to-ground glide weapon capable of destroying moving targets in adverse weather. It uses deployable wings to increase standoff range and is also the first Network Enabled Weapon using weapon datalink, allowing post-launch tracking and control of the weapon via Inflight Target Updates (IFTUs). The new multi-mode seeker uses both a millimeter-wave radar and an infrared sensor to operate in adverse weather using the Normal Attack mode. It also has Laser Illuminated Attack and Coordinate Attack modes for maximum employment flexibility. Once launched, the SDB II guides to a designated target cue, which is updated inflight via the weapon datalink until the seeker locates, identifies (if able), and provides terminal guidance to the target. The SDB II incorporates a multi-function warhead 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 to enable target penetration.

Program

SDB II is an Acquisition Category ID program intended to deliver capabilities deferred from SDB I. DOT&E approved the SDB II Milestone C Test and Evaluation Master Plan (TEMP) in April 2015. A TEMP update containing a cybersecurity strategy for Phase II is expected in FY22. The Air Force fielded the SDB II on the F-15E in FY20 following completion of Multiservice Operational Test and Evaluation (MOT&E) Phase I. The Navy intends to complete the Quick Reaction Assessment and field the SDB II on the F/A-18E/F in FY22. The MOT&E Phase II on the F-35 is scheduled to be completed in FY24. Specifically, developmental test and OT&E of the SDB II on the F-35B is expected to take place in FY22, leading to an early operational capability declaration, while developmental test and IOT&E on the F-35C is scheduled to start in FY23, leading to an initial operational capability declaration and full-rate production decision.

Major Contractor

Raytheon Missile Division – Tucson, Arizona.

Test Adequacy

SDB II testing in FY21 included developmental test flight science environmental/loads testing and jettison missions on the F-35B.

The Navy performed four F/A-18E/F missions with the SDB II as part of the quick reaction assessment, but all four were unsuccessful.

Phase I cybersecurity testing conducted by the Air Force was inadequate to support SDB II survivability evaluation in a cyber-contested environment. The extensive test shortfalls from Phase I need to be addressed during planned MOT&E Phase II testing.

Performance

Effectiveness

The SDB II is operationally effective as employed by the F-15E.

The first three F/A-18E/F missions were unsuccessful due to configuration errors, datalink entry failures, and aircraft software deficiencies. The Navy has resolved these hardware and software deficiencies. A fourth test was also unsuccessful, and analysis of that event is ongoing.

The SDB II demonstrated the expected lethality against target surrogates for legacy main battle tank, infantry fighting vehicle, anti-aircraft gun, surface-to-air missile target-erector-launcher, rocket launcher, and small patrol boat targets.

Suitability

SDB II is operationally suitable as employed by the F-15E. During F/A-18E/F integration the weapon has been reliable, but aircraft OFP and equipment issues have resulted in four failed tests and several cancelled missions. The complexity of cryptographic information delivery, loading, and mission planning, including exclusion zone creation processes, continues to be a problem, with only modest mission planning improvements incorporated into the Joint Mission Planning System to date. These problems were first identified during F-15E testing of the SDB II.

Survivability

The survivability of the SDB II in a cyber-contested environment is currently unknown due to the lack of adequate test assets provided by the vendor.

Recommendations

1. The Navy should develop and fund an adequate MOT&E Phase II cybersecurity T&E strategy to support an evaluation of SDB II survivability in a cyber-contested environment.
2. The Navy and Air Force should streamline the mission planning process to decrease the required timeline and increase reliability, particularly with regard to cryptographic data entry.
3. The DOD should continue to advocate for operationally suitable initiatives to streamline the cryptographic information delivery, loading, and verification process.

Wide Area Surveillance

The Air Force completed Wide Area Surveillance (WAS) IOT&E in July 2021 and conducted a full-rate production decision for the Scorpion System component of the WAS program in October 2021.

System Description

The WAS program consists of two advanced sensors: the Stateside Affordable Radar System and the Scorpion System, designed to provide complementary coverage volumes to detect and track a wide range of airborne targets in the National Capital Region. CONUS Air Defense Sectors will incorporate WAS data into Battle Control System – Fixed command and control systems.

Program

WAS is an Acquisition Category IC program. DOT&E approved the IOT&E test plan in October 2020. The Air Force entered full-rate production for the Scorpion System component of the WAS program in October 2021.

Test Adequacy

The Air Force Operational Test and Evaluation Center completed IOT&E in July 2021 in accordance with the DOT&E-approved test plan.

Performance

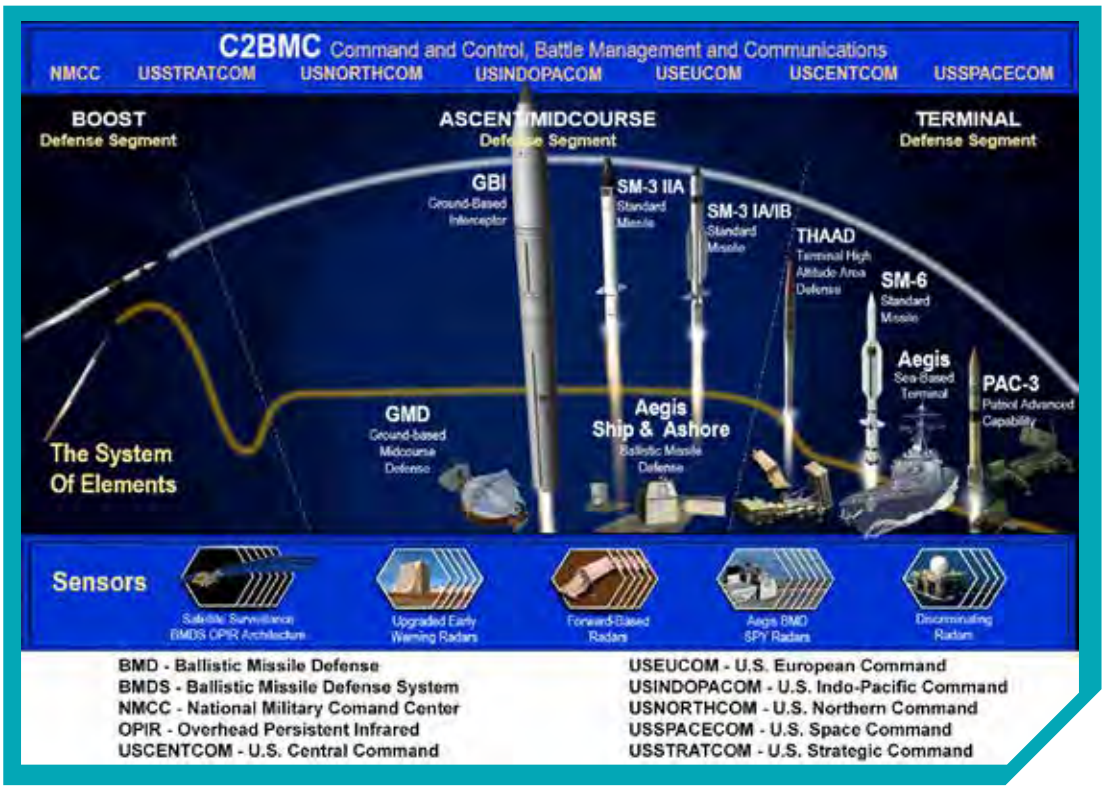
The WAS operational effectiveness, suitability, and survivability assessment is summarized in a classified WAS Beyond Low-Rate Initial Production report published in October 2021.

Recommendation

1. Recommendations are included in the classified WAS Beyond Low-Rate Initial Production report published in October 2021.

Missile Defense System

The Missile Defense System (MDS) has demonstrated a measured capability to defend the United States, deployed forces, and allies from a rogue nation's missile attack.



The Ground-based Midcourse Defense (GMD) weapon system has demonstrated the capability to defend the U.S. Homeland from a small number of ballistic missile threats with ranges greater than 3,000 kilometers and employing simple countermeasures, when supported by the full architecture of Missile Defense System (MDS) sensors. Similarly, the Regional/Theater MDS has demonstrated the capability to defend the U.S. Indo-Pacific Command (USINDOPACOM), U.S. European Command (USEUCOM), and U.S. Central Command (USCENTCOM) areas of responsibility from a small number of medium- or intermediate-range ballistic missile threats with ranges less than 4,000 kilometers, and from representative raids of short-range ballistic missile (SRBM) threats. In FY21, the Missile Defense Agency (MDA) fielded five significant capabilities to the MDS. Additional information and recommendations from each section of this article may be found in the Controlled Unclassified Information edition of this article and the classified DOT&E FY21 Assessment of the MDS report to be published in February 2022.

System Description

The MDA's MDS is a geographically distributed system of systems that relies on element interoperability and warfighter integration for combat capability and efficient use of guided missile/interceptor inventory. The commanders of USNORTHCOM, USINDOPACOM, USEUCOM, and USCENTCOM employ the MDS elements, as available to them, to defend the United States, deployed forces, and allies against ballistic and hypersonic missile threats of all ranges. The MDS consists of six weapon systems, a sensor architecture (terrestrial, maritime, and global sensors), and a command and control element as shown in Table 1.

Table 1. Elements of MDA's Missile Defense System			
Type	**Homeland Defense**	**Global Regional / Theater Defense**	**Hypersonic Defense**
Weapon Systems	**GMD**: Defends the U.S. Homeland against IRBM/ICBM attacks using Ground-Based Interceptors to defeat threat missiles during the midcourse segment of flight. MDA is developing a Next Generation Interceptor to supplement the current Ground-Based Interceptor fleet.	**Aegis BMD**: Both sea- and land-based variants defend U.S. deployed forces and allies from SRBM, MRBM, and IRBM threats. Aegis BMD uses the SM-3 family of guided missiles against exo-atmospheric ballistic missile threats alongside SM-6 guided missiles that are used by the Aegis SBT (Inc 1 and Inc 2 CU) for endo-atmospheric engagements. **THAAD**: Defends U.S. deployed forces and allies from SRBM, MRBM, and IRBM threats using guided interceptors in both the exo- and endo-atmosphere. For extended engagements, THAAD can provide or accept target cues from Aegis BMD or other sensors via C2BMC. THAAD complements the upper-tier Aegis BMD and the lower-tier PAC-3 weapon systems. **PAC-3**[b]: Defends U.S. deployed forces and critical assets from SRBM threats and aircraft attack and defeats enemy air assets. It is a mobile air and missile defense system employing a mix of PAC-3 hit-to-kill interceptors and PAC-2 blast fragmentation warhead interceptors.	**Aegis SBT (Inc 3)**[a]: Aegis SBT provides critical asset protection at sea and for joint forces ashore against ballistic, maneuverable, and hypersonic glide threats in the terminal phase. **GPI**[a]: Provides an additional layer of Hypersonic Defense augmenting Aegis SBT (Inc 3) to increase depth of fire against hypersonic threats. The program is currently in development of prototype interceptors.
Terrestrial and Maritime Sensors	**COBRA DANE Upgrade**[d]: L-band fixed site phased array radar. **UEWRs**[d]: Ultrahigh frequency fixed site phased array radars. **SBX**: X-band mobile phased array radar (XBR) located aboard a self-propelled, ocean-going platform. **LRDR**[a]: S-band two-face fixed site phased array radar.	**AN/SPY-1 Radar**: S-band four-face radar providing Aegis long-range surveillance and track functions in addition to guided missile engagement support. **AN/SPY-6(V)1 Radar**[c]: Being developed to replace the AN/SPY-1 radar on Aegis DDG 51 Flight III destroyers, this S-band four-face radar will extend Aegis threat detection ranges and provide simultaneous ballistic missile and air defense support. **AN/TPY-2 (FBM) Radar**: X-band single-face transportable phased array radar. **LTAMDS**[b]: C-band three-face multi-function, multi-mission radar interfacing with IBCS and supporting interoperability with PAC-3.	Leverages Homeland Defense, Regional/ Theater Defense, and Global sensors.
Global Sensors	**SBIRS**[d]: Satellite constellation of infrared sensors. **BOA**: Element that combines OPIR observations to provide missile event and track reports to C2BMC. **SKA**[a]: Network of space sensors providing interceptor hit assessments. **HBTSS**[a]: Network of space sensors to detect and track both ballistic and hypersonic threats, and provide fire-control quality data to MDS sensors and weapon systems.		
Command and Control	**C2BMC**: Integrating element within the MDS providing deliberate and dynamic planning, situational awareness, sensor track management, engagement support and monitoring, data exchange between elements, and network management. C2BMC also directs sensor tasking for the AN/TPY-2 (FBM) radars and BOA systems.		

[a] Under MDA development. [b] Under Army development. [c] Under Navy development. [d] Under Space Force sustainment/operations.

BMD – Ballistic Missile Defense; BMDS – Ballistic Missile Defense System; BOA – BMDS Overhead Persistent Infrared Architecture; C2BMC – Command and Control, Battle Management, and Communications; CU – Capability Upgrade; FBM – Forward-Based Mode; GMD – Ground-based Midcourse Defense; GPI – Glide Phase Interceptor; HBTSS – Hypersonic and Ballistic Tracking Space Sensor; IAMD – Integrated Air and Missile Defense; IBCS – IAMD Battle Command System; ICBM – Intercontinental Ballistic Missile; Inc – Increment; IRBM – Intermediate-Range Ballistic Missile; LRDR – Long Range Discrimination Radar; LTAMDS – Lower Tier Air and Missile Defense Sensor; MDA – Missile Defense Agency; MDS – Missile Defense System (formerly BMDS); MRBM – Medium-Range Ballistic Missile; OPIR – Overhead Persistent Infrared; PAC – Patriot Advanced Capability; SBIRS – Space-Based Infrared System; SBT – Sea-Based Terminal; SBX – Sea-Based X-band; SKA – Space-based Kill Assessment; SM – Standard Missile; SRBM – Short-Range Ballistic Missile; THAAD – Terminal High Altitude Area Defense; UEWR – Upgraded Early Warning Radar; XBR – X-Band Radar

Program

The MDS is a single Acquisition Category ID program that encompasses five of its six weapon systems, most of its sensor architecture, and its command and control element. In 2002, the Secretary of Defense granted the MDA special acquisition authorities for the MDS, which allowed it to use tailored processes and milestones rather than those specified in the DOD 5000 series of acquisition instructions. The MDA manages the MDS through a series of six program baselines (Schedule, Test, Technical, Resource, Contract, and Operational Capacity) and maintains responsibility for integrating all elements into the MDS whether or not the MDA developed the element. The MDA publishes the Test Baseline twice a year in an Integrated Master Test Plan (IMTP) that corresponds to the MDA Program Objective Memorandum submission to the Department and the President's Budget release to Congress. DOT&E approves each version of the IMTP, the latest of which was dated October 2021.

The Army is managing the PAC-3 and the Lower Tier Air and Missile Defense Sensor (LTAMDS) programs. PAC-3 is an Acquisition Category IC program. DOT&E approved the PAC-3 PDB 8.1 Test and Evaluation Master Plan (TEMP) in FY20.

The LTAMDS is a Middle Tier Rapid Prototyping program expected to be designated an Acquisition Category IC program at its Materiel Development Decision scheduled for FY23. DOT&E approved its initial TEMP in 2019, with an update currently in process.

The Navy is managing the AN/SPY-6(V)1 radar program, an Acquisition Category IC program. Its TEMP is under development, with anticipated DOT&E approval in FY22.

The Space Force sustains and operates three sensor types integrated into the MDS: COBRA DANE Upgrade, five UEWRs, and the SBIRS constellation. The Air Force has completed development and initial operational testing for these sensors.

Major Contractors

Table 2. MDS Major Contractors
The Boeing Company
GMD Integration: Huntsville, Alabama
Lockheed Martin Corporation
Aegis BMD, AAMDS, Aegis SBT, AN/SPY-1 radar, LRDR, and GPI through Phase I: Moorestown, New Jersey C2BMC: Huntsville, Alabama, and Colorado Springs, Colorado NGI AUR through Critical Design Review: Huntsville, Alabama SBIRS: Sunnyvale, California THAAD Weapon System, PAC-3 Command and Launch System, and PAC-3 interceptor variants: Dallas, Texas THAAD Interceptors: Troy, Alabama
Northrop Grumman Corporation
GBI Booster Vehicles: Chandler, Arizona GMD GCN, LMS, and GFC: Huntsville, Alabama NGI AUR through Critical Design Review: Chandler, Arizona BOA: Boulder, Colorado; Colorado Springs, Colorado; and Azusa, California HBTSS through Prototype Demonstration Phase: Redondo Beach, California, and Azusa, California

1. The MDA recently updated the system title to the MDS, dropping "Ballistic," to acknowledge the addition of maneuvering and hypersonic threat missiles to its missile defense charter.

Table 2. MDS Major Contractors
Raytheon Technologies Corporation
GMD EKV, SM-3/6 Interceptors, and LTAMDS: Tucson, Arizona PAC-3 Ground System and PAC-2 interceptor variants, AN/SPY-6(V)1 radar, AN/TPY-2 radar, SBX radar, and UEWRs: Tewksbury, Massachusetts COBRA DANE Radar: Dulles, Virginia
L3 Harris Technologies
GMD IDT: Melbourne, Florida HBTSS through Prototype Demonstration Phase: Fort Wayne, Indiana
Johns Hopkins University, Applied Physics Laboratory
SKA: Laurel, Maryland
AAMDS – Aegis Ashore Missile Defense System; AUR – All-Up Round; BMD – Ballistic Missile Defense; BMDS – Ballistic Missile Defense System; BOA – BMDS Overhead Persistent Infrared Architecture; C2BMC – Command and Control, Battle Management, and Communications; EKV – Exo-atmospheric Kill Vehicle; GCN – GMD Communications Network; GFC – Ground Fire Control; GMD – Ground-based Midcourse Defense; GPI – Glide Phase Interceptor; HBTSS – Hypersonic and Ballistic Tracking Space Sensor; IDT – GMD In-Flight Interceptor Communication System Data Terminals; LMS – Launch Management System; LRDR – Long Range Discrimination Radar; LTAMDS – Lower Tier Air and Missile Defense Sensor; MDS – Missile Defense System (formerly BMDS); NGI – Next Generation Interceptor; PAC – Patriot Advanced Capability; SBIRS – Space-Based Infrared System; SBT – Sea-Based Terminal; SBX – Sea-Based X-band; SKA – Space-based Kill Assessment; SM – Standard Missile; THAAD – Terminal High Altitude Area Defense; UEWR – Upgraded Early Warning Radar

Test Adequacy

The MDA MDS test plan focuses on collecting the flight, ground, and cybersecurity test data needed for contract compliance and operational capability declarations, as well as for the verification, validation, and accreditation of associated M&S. The adequacy assessment of the MDS test plan is based on the: 1) degree of collected data, 2) breadth of tested battlespace, 3) extent of covered threat set, 4) completeness of cybersecurity assessments, and 5) operational realism. The MDA conducted testing in accordance with the DOT&E-approved IMTP as affected by the COVID-19 pandemic. Due to the COVID-19 pandemic, the MDA delayed and modified flight, ground, and cybersecurity test events across the MDS. Table 3 outlines the 17 flight, ground, and cybersecurity test events that the MDA performed in FY21.

Table 3. FY21 Test Events

Date	Test	Mission Area	Description
October 2020	Flight Test Patriot Weapon System-27 Event 1	Global Regional/Theater Defense	The MDA, Army PEO M&S, and Army SMDC exercised the PAC-3 launch-on-remote capability using THAAD AN/TPY-2 (TM) sensor data. This demonstration will support the 2016 NDAA interoperability requirement.
November 2020	Flight Test Aegis Weapon System-44	Homeland Defense	The MDA demonstrated Aegis BMD engage-on-remote capability using a live SM-3 Block IIA guided missile to engage a simple ICBM in a Defense of the Hawaiian Islands scenario. This test fulfilled a 2018 NDAA requirement.

Table 3. FY21 Test Events			
Date	**Test**	**Mission Area**	**Description**
December 2020	Tactical Boost Glide-1	Hypersonic Defense	The MDA and DARPA conducted a joint hypersonic missile phenomenology data collection and tracking exercise to inform future capability development.
December 2020	Sea-Based X-Band Radar Cooperative Vulnerability and Penetration Assessment, and Adversarial Assessment	Homeland Defense	The MDA, BMDS OTA, and the Army's DEVCOM DAC and TSMO performed a limited CVPA and AA on the XBR installed on SBX exploring insider and nearsider threat postures.
March 2021	Ground Test Integrated-21 Sprint 2	Homeland Defense and Global Regional/Theater Defense	The MDA conducted this test to examine MDS performance using different AN/TPY-2 (FBM) radar versions with the C2BMC and GMD elements for the BMD of the Homeland and USINDOPACOM AOR missions.
April 2021	At-Sea Demonstration-1	Global Regional/Theater Defense	The MDA conducted an Aegis AN/SPY 1 radar SDA mission providing sensor tracking of resident space objects. This test informed radar performance and C2BMC/Space C2 interfaces for mission tasking.
May 2021	Formidable Shield 2021	Global Regional/Theater Defense	Eight NATO countries and the United States conducted an exercise integrating in-theater Aegis BMD baselines to support a common tactical picture. Four events were executed including exo- and endo-atmospheric simulated and live-fire engagements with information transfer over USEUCOM/NATO operational networks. These events also supported the acquisition program mandate for SM-3 SLEP data collection every two years.
May 2021	Flight Test Aegis Weapon System-31 Event 1	Global Regional/Theater Defense	The MDA executed an endo-atmospheric engagement using two BMD-configured SM-6 Block IA guided missiles against a single MRBM threat. This demonstration will inform Aegis SBT Increment 2 program.
July 2021	Flight Test Aegis Weapon System-33	Global Regional/Theater Defense	The MDA executed an endo-atmospheric engagement using four BMD-configured SM-6 Block IA guided missiles against a raid of two SRBM threats. This operational test will inform Aegis SBT Increment II program.
July 2021	Hypersonic Air-Breathing Weapon Concept-4	Hypersonic Defense	The MDA and DARPA conducted a joint hypersonic missile phenomenology data collection and tracking exercise to inform future capability development.
July 2021	AN/TPY-2 Radar Hardware-in-the-Loop Cooperative Vulnerability and Penetration Assessment	Global Regional/Theater Defense	The MDA, BMDS OTA, and the Army's DEVCOM DAC performed a limited CVPA on the AN/TPY-2 (FBM) radar using a HWIL laboratory representation. Insider and nearsider threat postures were explored.
August 2021	Aegis Weapon System Controlled Test Vehicle-04	Global Regional/Theater Defense	The MDA demonstrated the upgraded SM-3 Block IIA Guidance Electronics Unit against a simulated target to meet its flight performance requirements.

Table 3. FY21 Test Events			
Date	**Test**	**Mission Area**	**Description**
August 2021	Ground Test Integrated-21 Sprint 1	Homeland Defense and Global Regional/Theater Defense	The MDA conducted this test to assess THAAD capabilities in USINDOPACOM. The test also provided data to support an assessment of AN/TPY-2 (FBM) radar capabilities in USNORTHCOM and USINDOPACOM scenarios, and an assessment of interoperability between the MDS and SBIRS.
September 2021	Ground-based Midcourse Defense Weapon System Booster Vehicle Test-03	Homeland Defense	The MDA conducted a booster vehicle flyout to exercise 2-stage booster capability and 2-/3-stage selectable fire control software. This test was a component-level demonstration within the GMD element.
September 2021	Terminal High Altitude Area Defense Weapon System Controlled Test Vehicle-01	Global Regional/Theater Defense	The MDA attempted to demonstrate THAAD control of two PAC-3 interceptors against a simulated SRBM threat, but the test failed.
September 2021	At-Sea Demonstration-2	Global Regional/Theater Defense	The MDA conducted an Aegis AN/SPY 1 radar SDA mission providing sensor tracking of resident space objects. This test informed radar performance and C2BMC/Space C2 interfaces for mission tasking.
September 2021	Hypersonic Air-Breathing Weapon Concept-5	Hypersonic Defense	The MDA and DARPA conducted a joint hypersonic missile phenomenology data collection and tracking exercise to inform future capability development.

AA – Adversarial Assessment; AOR – Area of Responsibility; BMD – Ballistic Missile Defense; BMDS – Ballistic Missile Defense System; C2 – Command and Control; C2BMC – Command and Control, Battle Management, and Communications; CVPA – Cooperative Vulnerability and Penetration Assessment; DARPA – Defense Advanced Research Project Agency; DEVCOM DAC – Combat Capabilities Development Command Data and Analysis Center; FBM – Forward-Based Mode; FY – Fiscal Year; GMD – Ground-based Midcourse Defense; HWIL – Hardware-in-the-Loop; ICBM – Intercontinental Ballistic Missile; M&S – Modeling and Simulation; MDA – Missile Defense Agency; MDS – Missile Defense System; MRBM – Medium-Range Ballistic Missile; NATO – North Atlantic Treaty Organization; NDAA – National Defense Authorization Act; OTA – Operational Test Agency; PAC – Patriot Advanced Capability; PEO M&S – Program Executive Office-Missiles and Space; SBIRS – Space-Based Infrared System; SBT – Sea-Based Terminal; SBX – Sea-Based X-Band; SDA – Space Domain Awareness; SLEP – Service Life Extension Program; SM – Standard Missile; SMDC – Space and Missile Defense Command; SRBM – Short-Range Ballistic Missile; THAAD – Terminal High Altitude Area Defense; TM – Terminal Mode; TSMO – Threat Systems Management Office; USEUCOM – U.S. European Command; USINDOPACOM – U.S. Indo-Pacific Command; USNORTHCOM – U.S. Northern Command; XBR – X-Band Radar

Performance

The need for additional realistic and emerging threat representations, independently accredited M&S to creditably assess system effectiveness, and system survivability data in a cyber-contested environment present significant challenges for DOT&E in completing a comprehensive assessment of the MDS:

- Realistic and up-to-date representations of threat scenes are critical to the assessment of MDS performance. The rate of adversary threat development is currently faster than the pace of flight test target and ground test threat model development.
- The MDA and the MDS Operational Test Agency (OTA) continued to make progress in FY21 by increasing the number of OTA-accredited models and mitigating model limitations, but gaps remain.
- The MDS is a large system of systems with a potentially extensive cyberattack surface. While the MDA and the MDS OTA made progress in cybersecurity T&E efforts, there is still no standard approach for implementing cybersecurity and cyber-resiliency.

Ballistic Missile Defense for the Homeland

With the support of the full architecture of MDS sensors, the GMD weapon system has demonstrated the capability to defend the U.S. Homeland from a small number of ballistic missile threats employing simple countermeasures and with ranges greater than 3,000 kilometers.

Ballistic Missile Defense for the Global Regional/Theater

The Regional/Theater MDS has demonstrated capability to defend the USINDOPACOM, USEUCOM, and USCENTCOM areas of responsibility from a small number of medium- or intermediate-range ballistic missile threats with ranges less than 4,000 kilometers, and from representative raids against SRBM threats.

Hypersonic Missile Defense

The MDA collected data throughout FY21 to inform future sensors, sensor detection and tracking algorithms, and M&S validation.

Global Sensors and Command and Control

Almost every test conducted by the MDA included global sensors, as well as sensors unique to Homeland and Regional/Theater Defense to acquire, track, and report on observed objects. C2BMC is a force multiplier that globally and regionally integrates and synchronizes autonomous sensors, weapon systems, and operations to optimize MDS effectiveness. C2BMC is an integral part of all system ground and flight tests, which verify and exercise all current and future MDS capabilities. Additional details will be published in a separate classified C2BMC report in FY22.

Recommendations

The MDA should:

1. Increase the rate of target and threat model development to keep pace with the real-world threats.
2. Conduct the required operational cybersecurity assessments on all MDS elements and implement fixes, specifically:
    - Ensure that cybersecurity principles are included in element design, comprehensive cyber T&E plans are created and included in the IMTP, and developmental and operational cyber testing is completed prior to capability delivery to the warfighter.
    - Consider conducting technical working groups with cyber experts and DOT&E before/after each cybersecurity assessment to identify data gaps, review test requirements to focus future testing, ensure post-test analysis is thorough and well documented, and define what constitutes a cyber-secure system.

The Army should:

1. Continue to develop the PAC-3 Battalion Simulation to address current shortfalls in supporting performance assessments.

Cyber Assessment Program

In FY21, DOT&E resourced assessment teams, cyber Red Teams, cyber intelligence support, and other subject matter expertise to plan and conduct 45 assessments of operational networks, systems, and missions during Combatant Command (CCMD) and Service exercises.

FY21 assessments included persistent cyber operations, advanced cyber operations, assessments of emerging cyber technologies, to include offensive cyber capabilities, and special project assessments. Table 1 provides a comprehensive list, with major exercises being Global Thunder 21, Global Lightning 21, Mobility Guardian 21, Pacific Fury 21, Pacific Sentry 21, Judicious Response 21, Combined Command Post Exercise 21-2, Trident 21-3 and 21-4, and Copper Ring 21.

To improve the readiness for these exercise assessments, DOT&E continued to expand Cyber Readiness Campaigns, which are designed to help the Combatant Command (CCMD) or Service improve and assess operational-level cyber operations and decision-making. Cyber Readiness Campaigns use a CCMD exercise as the capstone event to assess cyber warfighting in a realistic mission context. Precursor Cyber Readiness Campaign events include cyber-stimulation events, table-top exercises, range-based exercises, and other events (that include full-spectrum threats) to credibly and comprehensively assess the ability of an adversary to deliver mission effects and impact U.S. operational decision-making. DOT&E works with cyber defenders during these events to identify critical problems and help improve defenders' capabilities.

DOT&E analyzed CCMD and Service exercises from FY14 through FY20 to identify strengths, deficiencies, and trends in DOD defensive capabilities. The analysis resulted in the following observations and recommendations.

There is no cyber defense without cyber defenders. In conflict with an advanced adversary, DOD missions will not succeed without effective cyber defenses. Cybersecurity must be built into system design, and the human defender should be included early on in cyber defense engineering and programmatic priorities for both system usability and training. Cyber defenders can and should include dedicated mission defense teams, system users, response-action teams, commanders, and network operators, all of whom should be trained and equipped to fight though cyberattacks to complete critical missions. DOT&E cyber assessments and operational tests continue to show that where systems or networks are actively defended by well-trained personnel in environments employing Zero Trust concepts, Red Teams emulating cyber actors have difficulty degrading critical DOD missions.

The DOD continues to develop and field cyber technologies, such as endpoint security systems and offensive cyber capabilities, without adequate programmatic support or operationally-realistic threat testing. Current DOD acquisition practices avoid the funding of dedicated program offices; such offices would help ensure the effectiveness of cyber technologies and that cyber operators are prepared with the degree of training commensurate with kinetic warfare operators. Lack of trained and resourced program offices is a root cause of many cybersecurity problems DOT&E discovers in the field, such as insecure system design, inadequate training of cyber defense personnel, and insufficient test planning and conduct. DOD development of cyber defenses continues to lag behind our adversaries' growing offensive capabilities, and critical DOD missions remain at risk of disruption from adversary cyber actions.

With DOD missions at risk, DOT&E recommends that warfighter exercises place increased emphasis on training in contested cyber environments. Although all exercises that DOT&E participates in include a DOT&E-sponsored Red Team, exercise authorities seldom permit warfighters to experience representative adversarial cyber effects because of the risk of degrading other training objectives. The net result of this limitation is a false sense of confidence by warfighters and leadership alike: failure to train in realistic cyber environments leaves warfighter skills and playbooks immature, and they will be unable to quickly detect cyberattacks or perform effective response actions.

DOT&E is engaging with the Joint Staff to promote the inclusion of realistic cyber stresses in every major training exercise. A cyber "fight-through objective" will provide warfighters and network defenders the opportunity to experience the spectrum of cyber threats and effects, and allow them to improve their defenses, detections, and resilience.

DOT&E assesses that DOD cyber concerns increasingly mirror those in the commercial sector due to increasing DOD reliance on commercial products and infrastructure. As a result, cyberattacks and vulnerabilities in the

commercial sector also affect the DOD's cyber posture. The FY21, SolarWinds attackers used novel hacking techniques to gain accesses to commercial networks and erase signs of their presence, enabling months of enduring access for research, exfiltration, and preparations for future operations. The DOD must prepare for these types of attack, and confirm the adequacy of preparations with cyber Red Team assessments.

DOT&E relies on Service-led cyber Red Teams to emulate nation-state threats during exercises and operational tests. DOD Red Teams, however, are stretched thin by high demand, and do not have the resources or personnel needed to routinely emulate sophisticated near-peer attacks. The cyber Red Teams need additional resources, as well as automation capabilities, to ease their workload. DOT&E will continue to urge the DOD to address critical Red Team capability gaps to improve CCMD assessments and cyber operational testing.

The DOD increasingly uses commercial cloud services to store highly sensitive, classified data, but current contracts with cloud vendors do not allow the DOD to independently assess the security of cloud infrastructure owned by the commercial vendor, preventing the DOD from fully assessing the security of commercial clouds. Current and future contracts must provide for threat-realistic, independent security assessments by the DOD of commercial clouds, to ensure critical data is protected.

Advances in artificial intelligence (AI) and machine learning will likely add new warfighter capabilities and cybersecurity challenges. The DOD plans to deploy AI capabilities to the CCMDs in FY22, and DOT&E has begun engagement with the Joint AI Center, the DOD Chief Data Officer, and supporting elements who are part of the AI and Data Accelerator Initiative. DOT&E will expand future assessments to help ensure new AI technologies are secure.

Program Activities

Persistent Cyber Operations

Persistent cyber operations provide cyber Red Teams with longer dwell time on DOD networks to probe selected areas and portray more advanced adversaries. As opposed to one- to two- week exercises or tests, long-duration activities offer Red Teams time for stealthier cyber reconnaissance to identify cybersecurity weaknesses and access points that might otherwise go undetected. After obtaining accesses, Red Teams can continue more stealthy operations to move laterally or escalate privileges. These activities may identify subtler and more pervasive vulnerabilities, and provide more realistic training for cyber defenders.

In FY21, DOT&E resourced such operations at six CCMDs, but due to the limited availability of planners and operators, these operations were more "part-time" than persistent. Requests for such activities expanded at the end of the fiscal year, to include networks supporting Ballistic Missile Defense and the global Department of Defense Information Network (DODIN); persistent cyber operations resources will have to continue to grow to adequately evaluate the DOD cybersecurity posture.

Advanced Cyber Operation Team

DOT&E resourced an advanced cyber operations team to augment cyber Red Teams with specialized cyber expertise and assist in the portrayal of more advanced adversaries. The advanced cyber operations team supported persistent cyber operations activities and the development of new cyber tools and tactics, techniques, and procedures (TTPs). During FY21, the advanced cyber operations team supported:

- Cybersecurity testing of the F-35
- Assessments of offensive cyber operations capabilities
- Assessment of Zero Trust architectures in Microsoft Software-as-a-Service environments
- Assessments of military aircraft transponders and critical aircraft systems
- Assessments of industrial control systems

- Development of enhanced Red Team capabilities
- Stand-up of a new Red Team location in Maryland
- Expansion of Red Team accesses via persistent cyber operations
- Review of evolving cybersecurity architectures and defensive measures

Demand for advanced cyber operations support continued to grow in FY21, and DOT&E expects requests for this support to continue into FY22, with efforts subject to available cyber expertise.

Assessment of Offensive Cyber Capabilities

DOT&E continued collaboration with offensive cyber capability developers and testers, helping to integrate more operationally realistic elements into assessments of these capabilities, including more representative environments, systematic variation of operational conditions, and inclusion of a thinking opposing force. Programs often overlook these critical elements because they focus on expediting development and delivery without completing rigorous OT&E.

Engagement with the Intelligence Community

DOT&E's collaboration and integration with the Defense Intelligence Agency continues to prove critical to our CCMD-focused assessments and OT&E events, and will remain so in the coming year. We continue to face challenges in conducting threat-representative cyber assessments, due in part to information-sharing challenges originating from multiple communities within the Department.

Special Project Assessments

DOT&E performed the following special assessments in FY21 in collaboration with USCYBERCOM, the DOD Chief Information Officer (CIO), Joint Forces Headquarters DOD Information Network (JFHQ-DODIN), the Defense Information Systems Agency (DISA), the Defense Threat Reduction Agency, and the Department of Energy Sandia National Labs:

- Zero Trust architectures in software-as-a-service environments
- DOD Office 365
- Usability of mid-tier defensive cyber operations tools
- DISA Internet Access Point that connects the DOD Information Networks to the commercial Internet
- Internet Protocol version 6 implementation
- Nuclear command, control, and communications

Special assessment methodologies and outcomes were shared with requesting organizations and will inform the broader CCMD and Service Cyber Readiness Campaigns, as well as cybersecurity OT&E of acquisition programs.

Assessment

The DOD continues to develop and field cybersecurity technologies, such as endpoint security systems and network monitoring tools, without adequate programmatic support or operationally-realistic threat testing. DOD Components often fail to provide dedicated program offices and adequate funding to support the development and fielding of cybersecurity technologies. The lack of trained and resourced program offices is a root cause of many cybersecurity problems DOT&E discovers in the field, such as insecure system design, inadequate training of cyber defense personnel, and insufficient test planning and conduct. In order to improve its cybersecurity posture and avoid costly cybersecurity technology failures, which DOT&E too-often encounters during our cyber assessments, the DOD must ensure that cybersecurity technology development is always conducted by well-resourced program offices; this should include cyber engineering expertise and cyber defense expertise of

the highest caliber. Moreover, training for cyber operators should be commensurate with the degree of training provided to kinetic warfare operators, and should include routine exercises against realistic cyber threats.

There is no Cyber Defense without Cyber Defenders

DOT&E analyzed CCMD and Service exercises from FY14 through FY20 to identify strengths, deficiencies, and trends in DOD defensive capabilities. The analysis showed the importance of defending each phase of a cyberattack, especially the phase during which an adversary maneuvers within a network or system to find their objective. DOT&E found that this phase presents unique detection challenges for cyber defenders. DOT&E also assessed emerging technologies that promise to increase defender visibility to such attacks. These include DOD's Office365 cloud-based environment and the Zero Trust Architecture model, discussed below.

Zero Trust Validation Events

In FY21, DOT&E took part in the DOD's implementation of Office365 and executed 15 cybersecurity assessments to inform decisions by senior leaders in DOD CIO, DISA, and U.S. Cyber Command on various aspects, options, and risks associated with the DOD's O365 employment. These assessments indicated that a data-centric security model implementing Zero Trust principles improves protection of DOD data. Furthermore, given the proper tools, manning, and training, the Zero Trust model can help cyber defenders actively defend mission-critical cyber terrain and enable improved cybersecurity over traditional perimeter-based defenses.

Remote Assessment of Security Stack Usability

DOT&E, in collaboration with a DOD Security Operations Center, conducted a usability assessment of the NIPRNET Joint Regional Security Stacks in FY21. For this project, DOT&E developed a methodology to remotely collect usability information from DOD network defenders. DOT&E intends to share this methodology with the test community to promote more rigorous and routine collection of usability information on fielded systems.

Collaboration with Commercial Sector to Assess Cybersecurity of Infrastructure Supporting DOD Operations

DOT&E observed increasing instances in FY21 where critical elements or even the whole of a DOD capability reside in networks or infrastructure deemed proprietary by the commercial sector, such as commercial clouds. Contractual language often prevents adequate operational test and evaluation of commercial networks and infrastructure within the scope of OT&E, resulting in incomplete evaluations. In the case of cybersecurity testing, independent assessments by DOD Red Teams are essential to assessing the security of DOD's data within the commercial infrastructure; contracts need to permit such assessments for the DOD to be able to understand how well critical mission data is protected.

Several major defense and commercial contractors have recently indicated willingness to allow DOT&E and select DOD Red Team personnel to collaborate with their contractor Red Teams on joint assessments of key elements residing on commercial networks and infrastructure. While not equivalent to independent OT&E, these collaborations represent positive first steps to remedy the current barriers to more complete OT&E and assessment of the myriad networks and capabilities that support all DOD missions.

DOD Ability to Portray Advanced Cyber Threats

In FY21, DOT&E conducted an assessment highlighting the gaps between the cyber capability of advanced threats, as reported by the intelligence community, and the existing DOD ability to emulate such capabilities during cybersecurity exercises and assessments. The most frequent gaps included insufficient time on network for cyber aggressors, limited toolsets, deficiencies in TTPs, unrealistic rules of engagement, and lack of end-to-end planning for a coherent cyber threat campaign. DOD Red Teams do not have the capacity or automation tools to routinely emulate sophisticated near-peer attacks. Such limitations preclude an ability to

stress systems, networks, and warfighters during CCMD exercise assessments and during OT&E to the extent expected in a real-world conflict.

Internet Access Points

Internet Access Points (IAPs) are intended to provide a protected security boundary between the Internet and NIPRNET. DOT&E supported a JFHQ-DODIN assessment of the DISA IAPs, sponsoring a DOD Cyber Red Team to conduct operationally realistic attacks against the IAPs to assess their cybersecurity capabilities. DOT&E provided findings and recommendations, and DISA is developing an implementation plan for a number of the recommendations.

Aircraft Combat Identification

DOT&E, with the Commander, Operational Test and Evaluation Force, analyzed the mission effects from degraded Transponder Combat Identification (T-CID) at the Northern Edge 2021 exercise. Working with DOT&E, the Air Force Life Cycle Management Center conducted a cybersecurity risk-reduction of Mode 5 Level-2 to demonstrate capabilities and effects from an adversary manipulating T-CID messages, and the Air Force Joint Test and Evaluation Program Office assessed air surveillance mission risk from T-CID-based capabilities and developed corresponding TTPs.

Artificial Intelligence

Advances in AI and machine learning will likely add new warfighter capabilities and cybersecurity challenges. During FY21, DOT&E led a team of cyber analysts at the request of the DOD CIO to develop machine learning tools and TTPs for the analysis of DOD network traffic data. The DOT&E team analyzed extremely large data sets using these techniques, allowing a deeper review of the technical data than previously possible using only human capabilities. These tools supported unique cybersecurity analyses and the identification of previously undetected problems. DOT&E briefed the results to the Office of the Secretary of Defense, the DOD CIO, and mission partners.

Assessments of Offensive Cyber Capabilities

The DOD continues to develop offensive cyber capabilities without formal operational testing to ensure such capabilities will work when used against an adversary. Although DOT&E's Cyber Assessment Program is conducting operationally realistic testing against a small subset of critical offensive cyber capabilities, there are many more offensive cyber capabilities being developed in multiple DOD Components with no such testing. This risks such capabilities failing to work when needed, and lowers commanders' confidence in the capabilities. The DOD should ensure offensive cyber capabilities are always operationally tested prior to their fielding.

Endpoint Security Tools

Endpoint security is a critical component of cyber defense-in-depth. For enterprise endpoints, the selection of the endpoint tools has been mandated through DOD CIO policy (e.g., Host Based Security System) with the DOD Components needing exceptions to policy to adopt alternative solutions for their networks.

In FY21, DOT&E conducted an assessment of Microsoft's Defender for Endpoint (MDE) as part of the U.S. Navy's proposed architecture for the enterprise Office365. The positive cybersecurity results of this assessment informed the DOD's decision to use MDE on all Navy endpoints.

Way Ahead and Recommendations

DOT&E will continue to increase the realism of our assessments to accurately assess the warfighter's ability to sustain missions in environments contested and degraded by an advanced cyber adversary. Ready access to a talented cyber workforce and advanced tools remain essential, and DOT&E will continue to advocate that the DOD

establish a well-resourced pipeline of cyber talent from academia, federally funded research and development centers, national labs, and the commercial sector. Overarching recommendations and assessment objectives for FY22 are discussed in the following subsections.

Increase Emphasis on Defenders

The DOD should refocus its cybersecurity efforts on cyber defender personnel, instead of focusing primarily on the technology associated with cyber tools, networks, and systems. Such a focus necessarily encompasses not only the technology, but the doctrine, organization, and training needed to ensure cyber defenders can effectively use technology to thwart cyber adversaries' attempts to disrupt DOD missions. All personnel performing DOD missions – including commanders and system and network operators – should be trained and equipped to recognize and help fight through cyberattacks commensurate with the degree of training provided to kinetic warfare operators. This will require the development of, and training for, new technologies capable of identifying potential cyberattacks to system operators and mission commanders. Such "cyberattack warning" technologies must be developed in order to identify and react to cyberattacks on mobile platforms such as aircraft, ships, and combat vehicles. Critical DOD missions should always be supported by trained teams dedicated to providing cyber defense for those missions.

Independent Assessment of Cloud Infrastructure

DOT&E will continue engagement to improve collaboration with commercial cloud providers in understanding and identifying the cyber risks from commercial cloud infrastructure to DOD critical missions, and ways to mitigate these risks.

The DOD should renegotiate contracts and establish requirements for future contracts with commercial cloud providers that enable the DOD to perform independent and threat-representative cybersecurity assessments of cloud infrastructure which hosts critical DOD capabilities.

Operational Testing of Cyber Tools

The DOD should operationally test cyber capabilities, such as endpoint security tools, prior to their wide-scale deployment to assess their cyber vulnerabilities, operational effectiveness, usability, and interoperability with other tools. The DOD should also assess the effectiveness and usability of existing endpoint security tools to help understand current returns on investment.

Adequate testing of cyber capabilities will require operational environments for both on-premises and cloud-based architectures, with up-to-date catalogs of threats and malware, fielded versions of the endpoint systems, and well-planned tests. Rigorous testing would allow the use of new malware with existing software to determine how well a current defensive cyber tool reacts to zero-day vulnerabilities. Such an infrastructure would also allow for DOD Cyber Red Teams to aggress candidate systems to discover unknown vulnerabilities, defensive cyber experts to fine-tune configurations, and cyber instructors to develop training materials and approved TTPs for selected systems.

Implementing Presidential Directive on Zero Trust

DOT&E will continue supporting Zero Trust efforts with rigorous assessments across the DOD as the Federal Government responds to the May 2021 Presidential Directive to adopt Zero Trust architectures.

Cyber Assessment Support to the ADA Initiative

In May 2021, the Deputy Secretary of Defense launched the Artificial Intelligence and Data Acceleration (ADA) Initiative to expedite deployment of AI-enabled technologies to the CCMDs, starting at the end of FY21. In FY22, DOT&E will proactively work with these teams to identify opportunities to assess the cybersecurity of these technologies in conjunction with the assessment activities that DOT&E already performs at the CCMDs.

Increase Assessment Realism for Offensive Cyber Operations (OCO) Capabilities

DOT&E has placed the Joint Cyber Warfighting Architecture on the DOT&E oversight list. OT&E of the Joint Cyber Warfighting Architecture will provide the opportunity to assess many smaller OCO capabilities not on oversight. DOT&E will coordinate with U.S. Cyber Command and the Service developers of OCO capabilities to increase involvement and test the realism of OCO capabilities and tools not covered under formal OT&E.

Full-Spectrum Cyber Assessments

Cyber operations increasingly involve interactions with the other warfighting domains (air, land, sea, space) and electromagnetic spectrum operations. DOT&E will increase focus on the following during CCMD and Service assessments:

- Cyber-physical systems such as industrial control systems and aircraft transponders
- Cyber-electromagnetic spectrum operations that use the radio frequency itself to cause cyber effects
- Cyber operations at tactical levels for better integration into military maneuvers in other domains

Evolve Persistent Cyber Operations to Campaign Mindset

DOT&E plans to evolve and mature persistent cyber operations to a campaign mindset conducted by a team of specialists to better capture the evolution of cyber actors, from criminal groups to nation-state adversaries. By integrating a campaign-planning element that integrates intelligence and other support components into persistent cyber operations, DOT&E plans to strengthen the persistent cyber operations concept to better portray advanced cyber threats and expand persistent cyber operations to additional CCMDs, as resources permit. DOT&E is developing a cyber campaign pilot partnership with the Air Force.

Mission Assurance Assessments via Wargames

DOT&E intends to offer cyber wargames to the CCMDs and Services as a complementary approach to assessing their cyberspace capabilities and processes. DOT&E will tailor each wargame using the applicable cyberspace terrain, participating cyber units, adversarial objectives and tactics, and overall scenario to enable stakeholders to explore cyberspace decisions and their relationship to improved mission assurance.

Table 1. Cybersecurity Assessments in FY21	
Event Type	**Acquisition Program or Type of Event**
Cyber Assessment Program Events	**Physical Security Assessment (2 Events)** USSPACECOM, USTRANSCOM
	Cooperative Network Vulnerability Assessments (3 Events) USINDOPACOM, USNORTHCOM, USTRANSCOM
	Assessments of Network Security, Stimulation Exercises, and Table Top Exercises (10 Events) USAFRICOM (2), USCENTCOM (3), USEUCOM (2), USSOUTHCOM (2), USSTRATCOM
	Assessment of Mission Effects during Exercises (12 Events) USAFRICOM (2), USINDOPACOM, USSOCOM (2), USSPACECOM, USTRATCOM (2), US Air Force, US Navy (2), USFK
	Assessment of Cyber Fires Processes for Offensive Cyber Operations (4 Events) USINDOPACOM
	Assessment of Special Capabilities and Projects (8 Events) Cyber Red Team Tools, SME Case Studies, DOD O365, DOD SOC Usability Study, USCC ZT Pilots, and USN MDE Assessment
	Assessments Employing Persistent Cyber Operations (6 Efforts) USCENTCOM, USEUCOM, USINDOPACOM, USNORTHCOM, USSTRATCOM, U.S. Air Force
USAFRICOM – U.S. Africa Command; USCENTCOM – U.S. Central Command; USCYBERCOM – U.S. Cyber Command; USEUCOM – U.S. European Command; USFK – U.S. Forces Korea; USINDOPACOM – U.S. Indo-Pacific Command; USNORTHCOM – U.S. Northern Command; USSOCOM – U.S. Special Operations Command; USSOUTHCOM – U.S. Southern Command; USSPACECOM – U.S. Space Command; USSTRATCOM – U.S. Strategic Command; USTRANSCOM – U.S. Transportation Command	

Center for Countermeasures

The Center for Countermeasures (CCM) executes testing of the operational effectiveness of countermeasures (CM) employed by a range of U.S. DOD and foreign weapon systems.

The Center for Countermeasures (CCM) accomplishes its mission by operating and deploying mobile test equipment capable of simulating an array of adversarial threats throughout the country. The transportability of CCM test tools and personnel provides the requisite test agility and efficiency for the DOD to develop and field warfighting capability at operationally-relevant speeds. It minimizes the deployment of aircraft and Program Office staff to test locations, preserving their schedules and resources. In FY21, CCM: 1) executed 30 test events supporting the successful evaluation and deployment of upgraded missile warning systems and CMs to combat theaters, 2) provided high threat environments for pre-deployment training, 3) equipped DOD test ranges with joint instrumentation required to expedite the development and fielding of directed energy weapons (DEWs), including directed energy (DE)-based CMs, and 4) leveraged project arrangements with Allies to advance the testing and evaluation of countermeasures.

CCM Expedites the Development and Fielding of Countermeasure Systems

In FY21, to keep pace with the advancing threat and expedite testing, development, and fielding of countermeasures needed to dominate and survive in an increasingly complex, multi-domain environment, CCM continued to upgrade the following test infrastructure and capabilities:

- **The Joint Mobile Infrared Countermeasure Test System and Multi-Spectral Sea and Land Target Simulator** – dual-band, infrared (IR), and ultraviolet (UV) simulator emitters used to replicate threat missile plumes. Upgrades to missile simulator emitters include improved bandwidth and processing capabilities to adequately represent the threat and evaluate advanced missile warning sensor (MWS) systems and directed infrared countermeasures (DIRCMs). The first upgraded simulator is expected in FY22.
- **The Towed Airborne Plume Simulator (TAPS)** – an airborne-towed body that generates a plume to simulate the IR temporal characteristics of a threat missile approaching an aircraft. It can also approximate the spectral and spatial behavior of threat missiles, simulating the movement of a threat in different backgrounds to more adequately evaluate aircraft MWS. CCM is executing the following TAPS projects to support the use of this capability for rotorcraft testing and further increase its capabilities:
  - The Phase 1 TAPS-Helicopter (TAPS-Helo) project to test the TAPS towing stability under various flight conditions and verify that the tow payload had no adverse effects on aircraft operation. Development of the TAPS-Helo is expected in FY23.
  - The Towed Optical Plume Simulator (TOPS) project focused on replacing the pyrophoric, fuel-based burner subsystem of the current TAPS with solid-state, optical emitter sources to simultaneously emit energy in two independently-controlled IR bands and one UV band. The Critical Design Review was completed in September 2021.
- **The Joint Standard Instrumentation Suite (JSIS)** – a suite of instrumentation used to collect missile plume and hostile fire threat signatures, and Time-Space-Position Information data during live fire events. These data are used to improve threat signature models developed by the Missile Space and Intelligence Center used to support MWS and CM development and evaluation. The JSIS baseline was developed from FY13 – FY18. JSIS 2.0 began in FY19 to add the capability to collect missile attitude data by FY23, needed to increase the fidelity of common threat models. JSIS Final Operational Capability Block 1, currently in progress, will provide additional radiometric imagers in emerging electromagnetic spectrum bands that the current JSIS baseline does not contain. It will improve the capability of measuring IR radiation generated from the missile throughout flight and is expected to be completed by February 2022. JSIS Blocks 2 and 3 intend to provide all remaining JSIS instrumentation equipment requirements, including radiometers, spectrometers, and tracked imagery to complete the JSIS suite. CCM continues to generate threat missile plume signatures required for open-air missile simulator testing and validation of signature models.
- **The High Power Portable Range Threat Simulator** – a ruggedized, deployable, ground-based, open-loop radio frequency (RF) threat radar simulator designed to provide open space emulation of threat radar signals and full threat modulations. It currently utilizes a legacy signal generator that CCM is upgrading to replicate new, high-fidelity threat radar signals. Upgrades are expected to take effect in FY22.

In FY21, CCM used unique capabilities, generating more than 17,000 missile plume signatures, to execute 19 total tests that supported the expedited development and fielding of eight Quick Reaction Capability, Urgent Operational Needs Statement, and Joint Urgent Operational Needs Statement CM programs as well as 11 tests that supported hardware and software upgrades of fielded systems against single and multiple IR-guided threats. Testing included the following:

- Advanced Threat Warner (ATW) and Common Infrared Countermeasures installed on Army rotary wing aircraft, demonstrating readiness for fielding
- Large Aircraft IR Countermeasures (LAIRCM) Next Generation System Processor Replacement (LSPR), in direct support of ongoing Navy efforts to improve aircraft survivability of fixed-wing aircraft
- Department of the Navy LAIRCM ATW Processor Upgrade Flight Test, as an initial evaluation of the software performance capabilities
- Common Missile Warning System and Common Infrared Countermeasures as integrated on the AH-64E and UH-60M, to evaluate their effects on aircraft survivability
- Limited Interim Missile Warning System, to determine its effectiveness in support of a fielding decision intended to increase the survivability of the UH-60M, CH-47F, and AH-64E
- Distributed Aperture Infrared Countermeasure, in direct support of ongoing Air Force efforts to improve the survivability of tactical HH-60G rotorcraft
- LAIRCM system upgrade performance, in direct support of ongoing Air Force Life Cycle Management Center efforts to improve survivability of C-5M and C-130J strategic transport platforms

CCM Provides the Threat Environment for Pre-Deployment Training

In FY21, CCM provided its unique test capability – a missile plume simulator, an instrumented man-portable air defense surrogate system, and the Portable Range Threat Simulator – to support the following two training exercises by providing data to the trainers to develop and refine their tactics, techniques, and procedures, enhancing their survivability potential in a combat environment:

- U.S. Army Special Operations Aviation Command Validation Exercise, where the aircrews executed electronic warfare (EW) threat identification, CM deployment, and evasive maneuvers. CCM helped validate the combat capabilities of the Battalion staff and aircrews.
- Joint interoperability training exercise (Neptune Falcon), designed to evaluate aircrews' CM employment capabilities in a realistic threat environment. This joint interoperability large-force exercise was conducted by aircrew planners and staff in a realistic, contested, and near-peer environment. The training included combat search and rescue activities for the A-10 Combat Air Force and the CV-22 Air Force Special Operations Command aircrews with the latest IRCM technology on a high-fidelity electronic combat range.

CCM Enables Credible T&E of Directed Energy-based CMs

DEWs have been emerging as a capability that could be integrated with kinetic fires to counter more advanced adversaries. In FY21, CCM made significant progress in equipping the DOD with tools and methods needed to adequately test and evaluate the effectiveness and lethality of DEWs and DE-based CMs. Specifically, CCM:

- Supported the development of a credible Mobile High Energy Laser Measurement system, in partnership with the Test Resource Management Center and the High Energy Laser Systems Test Facility, White Sands Missile Range (WSMR), New Mexico, intended to evaluate the lethal effects of DEWs. Specific advances include:
    - Target boards capable of directly measuring the High Energy Laser's (HEL) performance while stationary and while mounted on an inflight, operationally-representative cruise missile and small unmanned aerial systems.
    - Diagnostic suites capable of imaging, characterizing, and measuring the HEL as it is propagated in an open-air environment.

- Led the development of the HEL Remote Target Scoring (HRTS) system, in coordination with the Program Executive Office for Simulation, Training, and Instrumentation, to enable the tracking and scoring of a variety of targets during HEL engagements, including light boats, rocket-artillery-mortars, unmanned aircraft systems, and subsonic and supersonic cruise missiles. The HRTS system will extend CCM and WSMR testing capabilities with two such systems by FY22.
- Introduced four interim instrumentation suites in FY21 to support DEW rapid acquisition programs. These instrumentation suites were developed to collect the necessary data to adequately characterize the HEL beam, track target trajectory, collect environmental atmospheric conditions, and provide calibrated target imagery to determine HEL lethality against aerial munitions in both land and maritime conditions. CCM conducted various tests in FY21 that successfully demonstrated the instrumentation suites' capabilities. Further development of instrumentation to complement these capabilities are ongoing and expected to be completed by FY22.
- Supported DE High Power Microwave (HPM) effectiveness testing in collaboration with the WSMR Survivability, Vulnerability, and Assessment Directorate. CCM operated the HPM threat simulators and supported the effectiveness of ground combat vehicle assessment in the presence of congested electromagnetic spectrum environments.
- Participated in nine DE and Counter-Small Unmanned Aircraft Systems test events.

CCM Leverages Allies' Support to Advance T&E of IR and RF Threat CMs

In FY21, CCM supported the execution of the Australia, Canada, Great Britain, and U.S. Airborne EW Cooperative T&E Project Arrangement intended to advance EW T&E capabilities, resulting in:

- An exchange of RF CM modeling & simulation (M&S) plans between the four member nations.
- Advances in plans to execute a demonstration of integrated aircraft survivability equipment T&E methodologies using the Redstone Test Center Aviation Systems Test and Integration Laboratory, including a man-in-the-loop flight simulator.
- Advances in the development of M&S evaluation capabilities required for combat aircraft survivability assessment within complex threat environments. This work focused on the four nations' joint development of a core architecture, the System of Systems Architecture Design, which allows the integration of multiple evaluation tools and provides a larger scale (battlespace-wide) synthetic evaluation capability. Specifically:
    - The nations will develop and integrate complex Airborne EW scene generation tools. Significant progress has been made both with the System of Systems Architecture Design integration of a Canadian-developed electro-optical scene generator, as well as the development and integration of a parallel, complex RF scene generator.
    - The United Kingdom will execute a series of tests for the development of two new Airborne EW T&E M&S capabilities in FY22, with remote participation by the other three nations. It will deliver a combined electro-optical and RF synthetic test at a high-level fidelity.
    - Canada will execute a series of tests to demonstrate an improved level of electro-optical/IR and RF fidelity in Airborne EW system of systems M&S, with remote participation by the other three nations.
    - The U.S. will lead development and testing of multiple new Airborne EW T&E capabilities, incorporating inputs from the other three nations. Starting in FY22, the U.S. will hold a series of annual tests focusing on the requirements, capabilities, and tools needed for RF CM technique evaluation at the system of systems level.

International Test and Evaluation Program

The International Test and Evaluation Program (ITEP) enables bilateral and multilateral agreements between U.S. forces and Allies which are critical for expediting the development and fielding of advanced warfighting technologies, and supporting T&E infrastructure and capabilities.

Bilateral and multilateral agreements between U.S. forces and Allies enable the planning and execution of cooperative T&E projects, transfer of necessary test equipment and materials, exchange of T&E-relevant information through working groups, and reciprocal use of test facilities.

The United States continues to hold 11 bilateral agreements, as well as 2 multilateral agreements, to include the Multinational Test and Evaluation Program (MTEP) Memorandum of Understanding with Australia, Canada, New Zealand, and the United Kingdom, and the Transatlantic MTEP Memorandum of Understanding with France, Germany, Italy, and the United Kingdom, signed in January 2021. The addition of other NATO partners to the Transatlantic MTEP is under discussion. During FY21, discussions also continued with two other prospective international partners to establish new bilateral agreements with those nations.

In FY21, in support of the International Test and Evaluation Program (ITEP) mission, DOT&E reviewed and approved 14 agreements/memoranda, summarized in Table 1. Table 1 lists all agreements/memoranda signed in FY21, and if applicable, the time and location of associated test plans or events.

Table 1. IT&E Documents in Effect in FY21

IT&E Projects	Entry into Force/Effect Date	Test Dates	Test Activity Locations
The Transatlantic Multinational Test and Evaluation Program Memorandum of Understanding (MOU)	Jan 20, 2021	MOU will expire Jan 19, 2046	Test activities will be detailed in projects under the MOU
Advanced Distributed Modular Acquisition System (ADMAS) Instrumentation Equipment and Material Transfer Arrangement (E&MTA)	Oct 26, 2020	Equipment transfer planned in FY22	Koblenz, Germany
Sky Sabre System Reciprocal Use of Test Facilities (RUTF) Project Arrangement (PA)*	Nov 20, 2020	Jun 14-Jul 9, 2021	White Sands Missile Range, New Mexico
Flight Test Working Group Terms of Reference, Amendment One	Dec 1, 2020	Activity continuing through 2023	
Heterogeneous Multiphase Reactive Blast Cooperative T&E Cooperative T&E Project Arrangement	Dec 4, 2020	Ongoing	Suffield Research Centre, Ralston, Alberta, Canada
28th Engineers Regiment Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Tactics, Techniques, and Procedures (TTPs) RUTF PA and Annex A*	Jan 14, 2021	Jan 18-Feb 12, 2021	Dugway Proving Ground, Utah
Annex B to the RUTF Concerning 28th Engineers CBRNE Defense TTPs RUTF PA*	Apr 26, 2021	May 3-21, 2021	Dugway Proving Ground, Utah
Flight Test Aegis Weapon Systems-31 RUTF PA	Mar 29, 2021	May 20, 2021	Pacific Missile Range Facility, Hawaii
Electronic Warfare Operational Test 2016 RUTF PA, Amendment Three	May 7, 2021	Testing was delayed due to the coronavirus (COVID-19) pandemic and is expected to continue in 2022	Naval Research Lab, Washington DC or Norfolk, Virginia, Marine Corps Base Hawaii, Oahu, Hawaii
CF-18 Software Upgrade T&E RUTF PA*	Jun 14, 2021	Jul 1-Aug 5, 2021	Naval Air Warfare Center, China Lake, California
T&E of the German Bundeswehr CBRNE Defense TTPs RUTF PA*	Jun 16, 2021	Jun 28-Jul 16, 2021	Dugway Proving Ground, Utah

Table 1. IT&E Documents in Effect in FY21			
IT&E Projects	**Entry into Force/Effect Date**	**Test Dates**	**Test Activity Locations**
T&E of the Australian Special Operations Engineer Regiment CBRNE Defense and Explosive Ordnance Disposal TTPs RUTF PA and Annex A	Sep 21, 2021	Sep 28-Oct 15, 2021	Dugway Proving Ground, Utah
High Intensity Radiation Field Testing on the CC-295 Kingfisher RUTF PA	Sep 20, 2021	Sep 30 – Nov 5, 2021	Naval Air Warfare Center Aircraft Division, Patuxent River, Maryland
Approval in Principle for the Strategic Development Planning and Experimentation for National Advanced Surface-to-Air Missile System Experimentation RUTF PA	Sep 16, 2021	The Project Agreement remains to be negotiated. Consequently, the test start date has yet to be determined.	Andoya Test Range Facility, Norway

The Transatlantic Multinational Test and Evaluation Program Memorandum of Understanding

The Transatlantic MTEP Memorandum of Understanding was signed in January 2020 to prescribe the general provisions that will apply to the initiation, conduct, and management of TEP activities detailed in separate Project Agreements, Equipment and Material Transfer Agreements (E&MTA), and Working Groups Terms of Reference. These TEP activities will be between participants, authorized in accordance with the national policies and procedures, from France, Germany, Italy, and/or the United Kingdom.

Advanced Distributed Modular Acquisition System (ADMAS) Instrumentation E&MTA

The ADMAS E&MTA between the U.S. and Germany enables the Army's T&E Command to transfer the ADMAS instrumentation and software tools to the Bundeswehr Head of Robotics R&D at Koblenz. The transfer is valid for three years, and will enable Germany to standardize test procedures, data analysis techniques, and T&E methodology for the testing of autonomous robotic vehicles and associated technology. Due to the global coronavirus pandemic, the Army was not able to initiate the transfer of the equipment or personnel in FY21, as planned.

Sky Sabre System RUTF Project Agreement

The Sky Sabre System project agreement allowed the United Kingdom's Ministry of Defence (UK MOD) to leverage U.S. Army personnel and facilities at White Sands Missile Range to test the vertically-launched Sky Sabre integrated Ground Based Air Defence system prior to declaring its Initial Operating Capability. Through this agreement, the UK MOD received data on threat detection, threat prioritization, weapon allocation, and threat engagement, as well as post-launch analytical support to evaluate the system's capability (Figure 1).

Figure 1. American and UK personnel setting up the Sky Sabre system for testing at White Sands Missile Range.

Flight Test Working Group Terms of Reference

The Flight Test Working Group was established to identify and study future collaborative efforts intended to increase the effectiveness of joint weapons systems T&E through the harmonization of T&E requirements, investment strategies, and activities on specific T&E issues of mutual interest. Specifically, the Flight Test Working Group focuses upon the adoption and establishment of interoperable flight test instrumentation architecture to allow contributing participants to collaborate on flight test programs.

Heterogeneous Multiphase Reactive Blast Cooperative T&E Project Agreement

The Heterogeneous Multiphase Reactive Blast Cooperative T&E project agreement between the U.S. and Canada supports a series of tests over a three-year period between the U.S. and Canada at the Suffield Research Center, Alberta, Canada. The purpose of this agreement is to develop, test, and deploy diagnostics developed for heterogeneous multiphase reactive blast based on a series of explosive charges.

28th Engineers CBRNE TTPs RUTF Project Agreement

This project agreement with the UK enabled the development and testing of the partner defense TTPs against CBRNE threats. The U.S. Army Dugway Proving Ground, Utah hosted the tests, providing threat-representative scenarios to support the evaluation of the operational effectiveness of new detectors, Personal Protective Equipment, and decontamination equipment in an operationally representative environment. Tests also included the firing of various weapons by soldiers in protective clothing to evaluate their potential effects on mission effectiveness.

Annex B of the 28th Engineers CBRNE Defense TTPs RUTF Project Agreement

Under this Annex to the aforementioned project agreement, the UK sought to enhance and improve current TTPs and develop additional TTPs for operational gaps identified by the 28th Engineer Regiment during previous testing.

Flight Test Aegis Weapon Systems-31 (FTM-31) RUTF Project Agreement

A High-Power Phased Array Radar was employed at the Pacific Missile Range Facility to observe the target vehicle for the Missile Defense Agency's (MDA) FTM-31 flight test. The radar successfully tracked the target vehicle as planned. Resultant data will support and improve threat characterization.

Electronic Warfare Operational Test 2016 RUTF Project Agreement

The Electronic Warfare Operational Test 2016 enables the United States and Canada to continue the at-sea T&E of the electronic warfare suites fitted in Canadian Navy ships. This testing was postponed due to the global coronavirus pandemic and is expected to be conducted in Hawaii, where the U.S. will simulate anti-ship missiles to validate the Canadian Softkill System.

CF-18 Software Upgrade T&E RUTF Project Agreement

The CF-18 Software Upgrade agreement enabled Canada to test the upgrades to their CF-18 Hornets at the U.S. Naval Warfare Center, China Lake, California in July and August 2021. This T&E validated and verified the upgraded software and the CF-18's ability to intercept radar signals, identify signal sources, prioritize emitters, and provide defensive action against threat weapon systems.

T&E of the German Bundeswehr CBRNE Defense TTPs RUTF Project Agreement

This agreement enabled the German Bundeswehr to develop and test their defense TTPs against CBRNE threats. The U.S. Army Dugway Proving Ground, Utah hosted the tests, providing threat representative scenarios to support the evaluation of the operational effectiveness of new detectors, to include mass spectrometers, multi-gas measuring devices, radiation detection devices, Personal Protective Equipment, and decontamination equipment in an operationally representative environment (Figure 2). Tests also included the firing of weapons with soldiers in protective clothing to evaluate their effects on mission effectiveness. Tests also assessed post attack reconnaissance after an Improvised Explosive Device attack and testing of new radios and communications equipment.

Figure 2. German Bundeswehr CBRNE Testing at Dugway Proving Ground, Utah

T&E of the Australian Special Operations Engineer Regiment (SOER) CBRNE Defense and Explosive Ordnance Disposal TTPs RUTF Project Agreement

This agreement allows the Australian SOER to conduct a full range of evaluated CBRNE mission requirements at multiple Dugway Proving Ground, Utah locations. Execution of TTPs will address Australian DOD SOER tactical operational needs and management of situations involving CBRNE threats and home-made explosives. The goal is to enhance and improve current TTPs, as well as develop additional TTPs for operational gaps identified during this T&E effort.

High Intensity Radiation Field Testing on the CC-295 Kingfisher RUTF Project Arrangement

The Naval Air Warfare Center, Aircraft Division, Patuxent River, Maryland will provide High Intensity Radiated Field T&E support to Canada's Department of National Defense. This will include use of test facilities, set-up and operation of test equipment, and data collection, to include equipment readings, pictures, and video. This will be a five-week full-scale test.

Approval in Principle for the Strategic Development Planning and Experimentation (SDPE) National Advanced Surface-to-Air Missile System (NASAMS) Experimentation RUTF Project Agreement

This Approval in Principle will allow the U.S. Air Force SDPE office to implement an experimentation effort with the following primary objectives: 1) examine the utility of the NASAMS to provide a layered-defense capability for Base Defense against cruise missile threats, and 2) demonstrate the ability of the NASAMS to be integrated in U.S. armed forces Battle Management Command and Control systems for Base Defense missions.

Airborne Electronic Warfare Cooperative T&E Project Agreement

This agreement was established under the MTEP Memorandum of Understanding in 2016 and is therefore not listed in the annual FY21 Table 1, but this important multinational effort is ongoing, and is expected to continue

through at least 2026. FY21 activities and plans for the coming year under this agreement are described in detail in the Center of Countermeasures section of this annual report.

Integrated Air and Missile Defense (IAMD) Testing RUTF Project Agreement

This major project agreement was signed in 2016, and is therefore not included in the annual table above. However, test events under the IAMD RUTF occur every two years, to include the most recent Formidable Shield 21. The IAMD project agreement allowed the U.S. Navy to test its maritime IAMD system in the Formidable Shield 21 exercise at the UK's Hebrides Test Range that included 11 nations and 16 ships. This testing included employment of ground-launched supersonic low altitude targets and ballistic missiles. Formidable Shield 21 witnessed the first ever use of a Pathfinder Zombie short range ballistic missile target (Figure 3), provided by the Missile Defense Agency. Additionally, the U.S. provided two Medium Range Ballistic Missile Target presentations. These tests demonstrated the potential for conducting launch on remote engagements wherein target data are passed from one ship to another. The Formidable Shield exercise series provides the most comprehensive opportunity to evaluate IAMD capability in the Atlantic area of operations. This year's event was the most complex IAMD testing yet conducted in the Formidable Shield series. It is anticipated that future events will continue to increase in complexity.

Figure 3. U.S. MDA-provided Pathfinder Zombie short range ballistic target launch from the UK MOD Hebrides range.

Joint Aircraft Survivability Program

The Joint Aircraft Survivability Program (JASP) develops cross-Service aircraft survivability solutions and evaluation methods needed to dominate the multi-domain battlefield and mitigate U.S. aircraft losses in combat.

JASP products support: 1) weapons tactics schools, air operations, and training, 2) operational and live fire test and evaluation of aircraft systems, 3) aircraft combat damage reporting, and 4) transition of technologies to the battlefield intended to improve aircraft survivability and force protection.

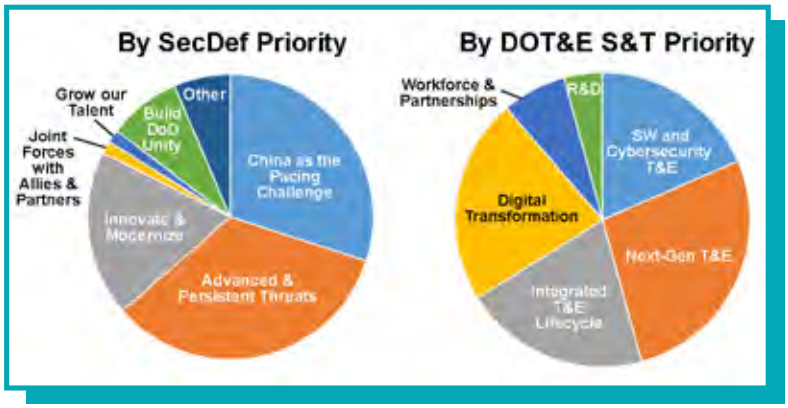


Figure 1. JASP FY21 funding by SECDEF and DOT&E S&T priorities

Specifically, JASP:

- Advances the capability and credibility of joint aircraft combat effectiveness tools used in combat mission planning, training, and weapon schools to support the development of air combat tactics, techniques, and procedures (TTPs).
- Manages enterprise-level modeling and simulation (M&S) tools required for credible evaluation of aircraft effectiveness and survivability.
- Supports the Joint Combat Assessment Team, which collects and analyzes U.S. aircraft combat damage and losses to develop the requirements for joint aircraft survivability solutions that provide force protection and remedy operational shortfalls.
- Leverages advances in science and technology to develop innovative survivability enhancement features.

JASP Advances the Capability and Credibility of Joint Aircraft Combat Effectiveness Tools

In coordination with the Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME), JASP develops and maintains the Air Combat Effects Library that serves as a joint suite of Service-based data and models used for modeling air-to-air, surface-to-air, and air-to-surface engagements and the resulting aircraft survivability and lethality. JASP supports this library with the delivery of data and models, to include shooter detection, target tracking, aircraft performance/kinematics (threat and friendly), weapon trajectory/shot logic, pilot logic, and standardized threat models.

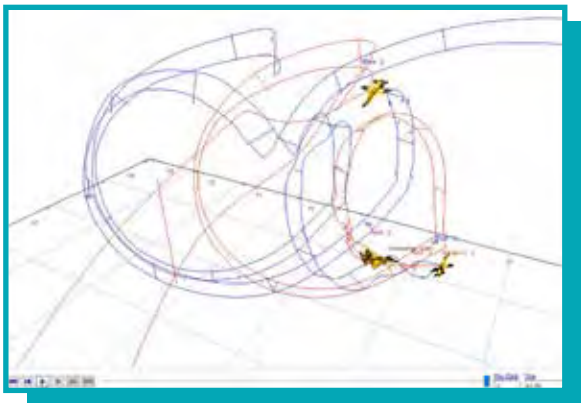


Figure 2. JAAM Dog Fight Example

JASP also supports the development the Joint–Anti-air Combat Effectiveness (J-ACE) tool used to conduct combat effectiveness analyses, which underpin air combat TTP development and training. J-ACE is an umbrella product consisting of models such as the Joint Anti-Air Model (JAAM), the output of which is shown in Figure 2. JAAM simulates the kinematic engagement of multiple U.S. (blue) and enemy (red) platforms, including their missiles and weapons. The aero-performance of the blue and red aircraft is calculated by BlueMax. The resulting damage effects analysis is conducted using the Endgame Manager to generate probability of kill estimates. J-ACE connects to test and training debrief tools through the use of an Application Program Interface. In FY21, the Joint Technical Coordinating Group for Munitions Effectiveness, in coordination with JASP, completed the J-ACE v5.4, adding or updating several aircraft and threat inputs, updating Endgame Manager, and adding the TSPI P5e format. Work continued on the next generation of J-ACE v6.0, which will fully implement the Air Combat Effects Library.

SLATE (Survivability and Lethality of Aircraft in Tactical Environments) is another notable model that provides J-ACE with capabilities to assess weapons effects in an advanced, contested environment. SLATE also provides the acquisition and RDT&E community the capability to assess aircraft survivability against the full spectrum of threats, including surface-to-air missile systems (SAMS), air defense artillery (ADA), and air-to-air missiles (AAMs). In FY21, JASP advanced SLATE by maturing aero performance and radar modeling of rotary wing aircraft, air defense artillery gun modeling, and environment modeling as shown in Figure 3. The initial version of SLATE will be fielded in early FY22.

Figure 3. SLATE Helicopter, ADA Gun, and Low Altitude Environment Modeling Example

JASP Manages Enterprise-level M&S Tools Required for Credible Evaluation of Aircraft Effectiveness and Survivability

Through Tri-service configuration control boards, JASP continues the management of major M&S tools used to estimate air combat effectiveness and survivability against an array of operationally representative kinetic threats. The toolsets include the air-to-air combat simulation Brawler, the surface-to-air engagement model Enhanced Surface-to-Air Missile Simulation (ESAMS), SLATE, and the vulnerability analysis code Computation of Vulnerable Area Tool (COVART), along with its supporting penetration and fire prediction codes Projectile Penetration (ProjPen), Fast Air Target Encounter Penetration (FATEPEN), and the Next Generation Fire Model (NGFM).

In collaboration with the Intelligence Community, JASP continues to improve the representation of the contested environment for these tools. Through work conducted under JASP efforts, the Intelligence Community developed a means to evaluate radio-frequency countermeasure effects under their Threat Modeling and Analysis Program that will be released in SLATE once validated by the intelligence center .

In FY21, JASP initiated the Machine Assisted Exploitability Simulation for Testing Resilient Operations (MAESTRO) project to improve the survivability evaluation of U.S. aircraft against cyber threats. This effort, in collaboration with the Air Force, Army, and Navy aviation cyber survivability communities, will provide M&S tools and data standardization to develop and evaluate aircraft survivability in a cyber-contested environment.

JASP Supports the Joint Combat Assessment Team to Collect and Analyze U.S. Aircraft Combat Damage and Losses

In FY21, JASP continued to enable aircraft combat damage incident reporting and aviation combat injury analyses through the Joint Combat Assessment Team and the U.S. Army Aeromedical Research Laboratory (USAARL). In FY21, the Joint Combat Assessment Team completed combat damage assessments supporting operational forces. The USAARL supported the related analysis of aircraft combat injuries and documented all reported CH-47 Chinook combat injuries in Operation Iraqi Freedom and Operation Enduring Freedom. USAARL also completed analysis of combat injury trends across the UH-60 Black Hawk, AH-64 Apache, and CH-47 Chinook helicopters to guide future personnel survivability investments.

To enable combat incident reporting and data sharing across the DOD, Services, and Combatant Commands, JASP transitioned the Combat Damage Incident Reporting System to the National Ground Intelligence Center for hosting. To support future aircraft combat incident reporting, in coordination with the Naval Air Systems Command, JASP demonstrated automatic collection of time-sensitive threat incident and engagement data to

improve combat incident reporting. Table 1 details DOT&E oversight programs by acquisition program type supported by JASP tools.

Table 1. DOT&E Oversight Programs Supported by JASP Tools

Acquisition Program Type	ACAT/ BCAT	BRAWLER	ESAMS	SLATE	COVART	NGFM
Bomber Aircraft	-	1	1		1	1
Fighter Aircraft	ID, IC, II	5	5		4	1
Rotary-Wing Aircraft	IB, IC		3	3	2	2
Transport/Tanker Aircraft	IC		1		2	1
Special Use Aircraft	ID, III		1		2	2
Weapons	IC	1				
Oversight Programs Supported Totals		7	11	3	11	7

JASP Leverages Advances in Science and Technology to Deliver Innovative Survivability Enhancement Features

Threat Detection and Countermeasures

In collaboration with the OSD and Service organizations, JASP develops countermeasure techniques and matures technologies to defeat advanced electro-optical/infrared and radio frequency guided threat systems, the distribution of which is shown in Figure 4.

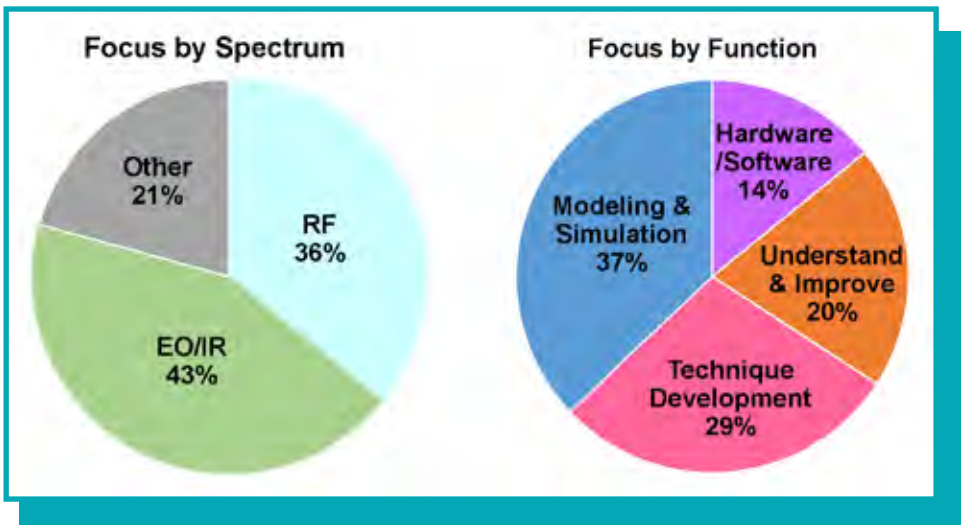


Figure 4. JASP FY21 Susceptibility Assessment and Reduction Projects by Spectrum and Function

Electro-Optical/Infrared Spectrum

In FY21, JASP assessed the current U.S. countermeasure effectiveness against a high priority electro-optical/infrared guided threat system. The Navy and the Army are using these data to inform future system requirements and countermeasure technique optimization. JASP also finished the development of a specific man-portable, air-defense system digital model to facilitate a more comprehensive operational and live fire test and evaluation of U.S. countermeasures against this category of threats.

In FY21, JASP also initiated two projects to improve aircraft situational awareness using electro-optical/infrared sensors against advanced missile threats by an innovative use of missile warning sensors in a non-standard operational scenario, and advanced machine learning algorithms to improve missile warning sensor detection and classification of specific threats.

Radio Frequency Spectrum

In FY21, JASP continued the development and demonstration of electronic attack (EA) technologies. Specifically, JASP completed the initial hardware-in-the-loop demonstration. Concurrently, JASP adapted these technologies/techniques to a different category of advanced radio frequency threats and completed test planning for a FY22 flight test. In coordination with the Intelligence Community, JASP also completed integration of an electronic attack capability into a particular threat system model, which provides the Services a unique capability for development of countermeasure techniques.

In FY21, JASP completed a three-year collaboration with the Army to advance a low size, weight and power (SWaP) modular antenna needed to keep pace with advanced electronic attack techniques. JASP advanced this technology to a technology readiness level of 5, positioning it to transition to a program of record.

Force Protection

In FY21, JASP continued to develop and test technologies that improve the protection of aircraft aircrew and passengers against persistent and emerging threats. These efforts also collected the prerequisite test data needed to develop and validate vulnerability and lethality M&S tools. Specifically, JASP:

- Developed a fire-mitigating mist control additive for Polyalphaolefin Oil avionics cooling fluid to reduce the vulnerability of aircraft to onboard fires. Testing to validate the additive's effectiveness is ongoing. If proven effective, JASP will investigate the possibility of applying the technology for other common aircraft flammable fluids..
- Continued the development of a methodology to optimize self-sealing fuel bladder fabric design for crashworthiness and revised fuel bladder qualification procedures (and test fixtures) to improve fuel cell test quality and assessment credibility. The self-sealing and crashworthiness capability of fuel cell bladders commonly used to improve rotorcraft safety and survivability are a continuing tri-service concern.
- Assessed the effect of high energy laser effects on baseline and hardened aircraft components, identified the most promising hardening solutions for maturation, and quantified the mission impacts and benefits. This effort also provided data enabling a more credible survivability assessment of U.S. aircraft against high energy lasers.
- Tested a new armor, demonstrating its capability to stop a projectile at up to 40 percent reduction in area density over the legacy armor for the same significant, unguided threat to aircraft and occupants, particularly in low altitude operations. This innovative technology considerably improves the options available to programs and commanders to protect personnel and flight critical components.
- Constructed a test setup that will provide validation of composite joint shear analysis under threat-induced hydrodynamic loading. JASP also continued validation of a rapid structural vulnerability assessment tool providing a new capability to evaluate structural vulnerability earlier in the aircraft development lifecycle.

USSOCOM Collaboration

In FY21, JASP partnered with the United States Special Operations Command (USSOCOM) Program Executive Office – Fixed Wing (PEO-FW) to synchronize the efforts and support the PEO-FW mission through cross-Service awareness and collaboration on aircraft survivability technologies and methodologies. This cooperation led to several technical developments with the potential for future transition, including reduced weight armors, advanced missile warning sensors, and radio frequency and infrared countermeasures.

Joint Technical Coordinating Group for Munitions Effectiveness

The Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) program develops validated weaponeering tools derived from the policy-approved Joint Munition Effectiveness Manuals (JMEMs).

Combatant Command strike authorities rely on weaponeering tools developed by The Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) program to estimate and optimize the type and number of U.S. weapons required to achieve the desired lethal effect against a range of strategic or tactical targets while mitigating risk for collateral damage, to include civilian casualties. Current Joint Munition Effectiveness Manual (JMEM) products include:

1. The Digital Imagery Exploitation Engine (DIEE) tool, used to geographically locate and characterize the target, weaponeer the target using JMEM Weaponeering Software, and then estimate collateral damage effects using the Digital Precision Strike Suite Collateral Damage Estimation (DCiDE) tool.
2. Weaponeering tools capable of estimating lethal effects for directed energy weapons (DEW), cyber, and electromagnetic spectrum (EMS) fires.
3. The Joint Anti-Air Combat Effectiveness (J-ACE) tool used in combat mission planning, training, and in weapon schools to support the development of air combat tactics, techniques, and procedures (discussed in the Joint Aircraft Survivability section of this report).

In FY21, the JTCG/ME program assumed the management role of the Joint Live Fire (JLF) program to facilitate the development of adequate LFT&E tools, methods, and infrastructure required for credible development of both, JMEM products and LFT&E programs. Examples include: 1) development of new test data collection methods, 2) advancement of verification, validation, and accreditation of modeling and simulation (M&S) tools, 3) advancement of the use of machine learning to automate T&E, 4) development of a survivability and lethality data management strategy, 5) advancement of survivability/lethality analysis in a contested maritime environment.

Combatant Command Strike Authorities Require Credible Weaponeering Tools

JMEMs are used daily by the warfighters in direct support of operations, mission planning, and training. The user base includes approximately 26,000 spanning all Services across tactical, operational, and strategic objectives, as detailed in Figure 1.

Figure 1. User Community

- An example of the use of weaponeering tools can be seen in Figure 2, which demonstrates the lethal effects of U.S. strikes against targets of interest. To achieve such lethal effects, JMEM products were used to characterize the target and determine the type and number of weapons required to achieve such an effect.

Figure 2. U.S. Airstrike – Pre and Post Strike

Specifically, the DIEE is the tool that enables users to plan and execute this type of event by seamlessly performing the following Advanced Target Development steps: 1) geographically locate and characterize the target, 2)

weaponeer the target using JMEM Weaponeering Software and perform target coordinate mensuration, and 3) estimate collateral damage effects using the DCiDE tool. In FY21, JTCG/ME updated DIEE to further improve the accuracy and efficiency of all three steps:

- In collaboration with Office of the Under Secretary of Defense for Intelligence and Security and Joint Staff J2 Targets, JTCG/ME enhanced the Joint Targeting Intelligence process by developing, enhancing, and standardizing the intelligence database in support of the Joint Targeting Cycle.
- Incorporated new user interfaces to increase JMEM Weaponeering Software tool usability, which provides a series of weapon system characteristics, delivery accuracy, and target vulnerability data needed to estimate the final aimpoint, delivery conditions, and number of rounds on target to achieve the desired lethal effects. JTCG/ME included new weapon and trajectory data to keep pace with technology development by accounting for enhanced capabilities for target defeat, and implemented an approved software development environment for continuous JMEM evolution. To maintain consistency with the latest National Geospatial-Intelligence Agency mensuration methods, JTCG/ME updated both Mensuration Services Program and Common Geopositioning Services.
- Enabled data-based updates to the authenticated collateral effects radii tables, reducing their error margins, advanced the collateral effects library mitigation tool to increase the efficiency of collateral effects analysis, enhanced risk estimate distances calculations used by DCiDE to determine friendly force risk estimates, and provided assistance with reachback support for current operations. DCiDE complies with the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) and provides lethal radii graphics to aid in the decision-making for strike approval authority.

JTCG/ME Advances the Capability and Accuracy of Weaponeering Tools

JTCG/ME continues to advance the capability and accuracy of weaponeering tools to respond to Combatant Command needs as they are challenged with the increased complexity and dynamics of the multi-domain operational environment. JTCG/ME upgraded existing capabilities to increase the effectiveness of kinetic strikes and developed new capabilities to enable deliberate and dynamic strikes using cyber, EMS, and DEW.

Increasing the Effectiveness of Kinetic Strikes

Figure 3. Buried Soil Test

Kinetic threat lethal effects are complex phenomena that need to be adequately characterized to credibly predict their effect on the target of interest. Similarly, targets of interest are complex and the lethal effect predictions largely depend on our understanding of the target vulnerabilities. In FY21, JTCG/ME made progress in improving the ability of the DOD to accurately characterize the lethal effects of U.S. weapons. Specifically, JTCG/ME leveraged the multi-year, Enhanced Weaponeering and Collateral Damage Effects (CDE) test program initiated by the JLF program to quantify the lethal effects of weapon burial and building debris. Figure 3 demonstrates the effects of a munitions buried within the ground, while Figure 4 demonstrates the lethal effects of munitions detonated inside structures. These and similar data sets are used to verify and validate high fidelity M&S tools being utilized to predict building debris mass and velocity distributions from structures along with crater ejecta, ground shock, and blast pressure for various soil configurations. These predictions must be credible since they are the foundation of fast running engineering models used by DIEE and DCiDE

Figure 4. Structure Test

to estimate weapon lethal effects and collateral damage, and to refine CDE tables. In FY21, under the Enhanced Weaponeering and CDE test program, JTCG/ME conducted several tests to further the understanding of bomb burial and building debris effects on noncombatant personnel.

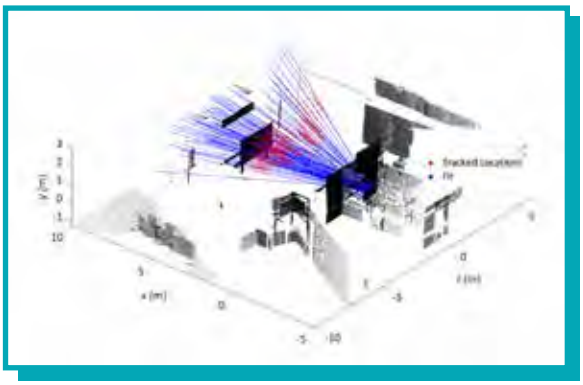


Figure 5. Fragment tracking data overlaid on laser scanned test set-up

JTCG/ME also leveraged the Advanced Warhead Characterization project and the Small-Scale Blast program initiated by the JLF program to improve the pedigree of weapons data. Specifically, in FY21, the program explored advances in science and technology and utilized emerging diagnostics tools (computed tomography imaging, digital image correlation, x-ray, photon doppler velocimetry, pressure measurements, and optical fragment tracking) to support efficient data collections and high-fidelity model validation for multiple munitions. Figure 5 shows optical tracking data overlaid on laser scan data for visualization of fragment distribution tests at Sandia National Labs.

In addition, JTCG/ME leveraged the small-scale blast test program initiated by the JLF program to provide a tailorable scale target model (shown in Figure 6) that will be used to efficiently collect larger volume and higher fidelity lethality data. In FY21, the Air Force Research Laboratory completed the design and fabrication of a scaled structure that will be used to update, verify, and validate the blast effects (BlastX) M&S.

Figure 6. Small Scale Blast Test Structure

In FY21, the JLF program initiated the Multiphase Blast Explosive (MBX) weapon system test program to update methodology for MBX lethal effect estimates used in low-collateral-damage munitions. In coordination with JTCG/ME, enhancements to enable optical characterization of fragment dispersion in flight tests are being developed to adequately evaluate emerging hypersonic weapons.

In FY21, JTCG/ME identified an opportunity to enhance the DOD weaponeering tools and their ability to support the warfighter with credible and timely lethal effects estimates against adversary maritime (surface and subsurface) targets. Current weaponeering capabilities and data sets are either insufficient or non-existent for conventional surface, subsurface, and unconventional small-boat threats, which are capable of conducting attacks against U.S. and partner ships in the competition phase, or major combat operations. To provide an initial response, JTCG/ME leveraged the Maritime Survivability and Lethality Test program initiated by JLF to pursue a cohesive, enterprise-wide strategy that seeks to improve efficiency, collaboration, knowledge sharing, and analytical techniques across maritime organizations. With additional funds, the program could plan collaborative test programs that procure data to fill those gaps and improve current analytical tools and methods required to support the delivery and fielding of such weaponeering tools. This effort will not only increase weapons systems' lethality against foreign maritime platforms but also deliver the capability that will support the delivery of more survivable ships and submarines to the U.S. Navy.

The most comprehensive effort used to verify, validate, and advance the effectiveness of weaponeering tools is tied to a multi-year effort intended to improve the Battle Damage Assessment (BDA), initiated by JTCG/ME. The primary benefit of the BDA program is to enable credible post-strike analysis to ensure Commander's intent has been achieved in accordance with Chairman of the Joint Chiefs of Staff Manual. To meet this intent, JTCG/ME continued to collect all BDA data to not only analyze strikes and inform reachback support, but also to support weaponeering tool verification and validation, training, and expenditure analysis. Specifically, in FY21, the BDA team developed automated data collection tools and collected data products for thousands of strikes.

As part of the IL6 Microsoft Azure Cloud architecture development, the BDA team took their first steps in the development of virtual machines to provide efficient scalability and agility to enhance processing performance.

The BDA effort also offers a foundation for advancement of the T&E data management strategy that will support not only weaponeering tools, but also the acquisition community. In FY21, the JLF program funded an effort to evaluate a framework capable of consolidating available and future LFT&E data in support of a range of data mining and data analytics intended to more effectively inform requirements, performance evaluations, and development of evaluation/test tools. The DEVCOM Data Analysis Center performed a requirements analysis through stakeholder surveys and interviews in the development of a requirements definition document. A potential course of action is to utilize the Cloud Hybrid Edge-to-Enterprise Evaluation and Test Analysis Suite as a prototype data storage capability. Access to a comprehensive data storage capability is important to the success of artificial intelligence (AI)/machine learning efforts requiring large formatted data sets. An example of this has been demonstrated through another JLF initiated program: the machine learning to optimize armor/anti-armor performance. Effort is focused on leveraging AI and machine learning to optimize armor system designs and the evaluation of their effectiveness against a range of kinetic energy threats. Research laboratories and T&E centers continue to create robust scalable armor performance databases for use by future developed trained algorithms. These future algorithms will predict kinetic threat engagement solutions and optimize armor /anti-armor solutions at a fraction of the cost of full-scale live-fire tests.

Enabling Multi-Domain Superiority with Directed Energy Weapons, Cyber, and Electromagnetic Spectrum Strikes

JTCG/ME has made significant progress in supporting the warfighter with weaponeering tools intended to integrate kinetic and non-kinetic fires for optimized mission and lethal effects while mitigating collateral effects to both noncombatants, infrastructure, facility and equipment. While JTCG/ME has focused on the development and fielding of separate weaponeering tools that can account for DEW, cyberattacks, and EMS fires, it has also initiated the plans to provide an architecture for a single JMEM capable of estimating the appropriate number and types of both kinetic and non-kinetic weapon required to achieve superiority in a multi-domain operational environment.

Directed Energy Weapons

In FY21, JTCG/ME has continued the development of validated Joint Laser Weaponeering Software (JLaWS) and High-Power Microwave (HPM) Weaponeering Software (HPMWS) tools designed to enable the Combatant Commands to estimate lethal effects on the target of interest using DEW (either high energy lasers (HEL) or HPM). Specifically, JTCG/ME conducted solid state laser weapon demonstrator testing against various targets to collect critical data that were used to verify and validate JLaWS. This tool was provided to users (shown in Figure 7) to obtain HEL operator feedback that will be used to further advance JLaWS utility, establish HEL reachback support, and continue to advance the development of collateral risk tools for HEL. As a result, JTCG/ME supplied operators with JLaWS-developed target cards.

Figure 7. Testing a Solid State Laser

To advance the development and fielding of HPMWS systems, (example system shown in Figure 8), JTCG/ME developed HPM lethal effects data standards and analytical

Figure 8. Navy HPM System

tools required to characterize target vulnerability, M&S tools required to estimate lethality and collateral damage effects, and probabilistic risk assessment tools. While DEW tools are being developed in parallel with kinetic tools, they are still leveraging existing JMEM architecture to enable future integration of these capabilities.

Cyber

In FY21, JTCG/ME continued the development and fielding of JMEM tools intended to estimate cyber effects. The Cyberspace Operations Lethality and Effectiveness (COLE) tool is the foundational product, which enables commander operations decisions through advanced analytics used to adequately visualize, plan, evaluate, and assess the full spectrum of cyberspace activities (Figure 9). In FY21, major contributions included fielding across multiple security domains, supplying probability of effects of cyberattacks while accounting for target configuration uncertainty and data gaps, enabling characterization and visualization of weapons and targets in a dynamic operational environment, and providing access to intelligence data support. These COLE efforts were used to deliver the Machine Assisted Exploitability Simulation and Testing for Resilient Operations (MAESTRO) tool used for assessment of fielded U.S. platforms in a cyber-contested environment. MAESTRO enables automated early discovery of system vulnerabilities that can be used to inform and refine cybersecurity T&E. Additionally, JLF initiated the Cyber Automated threat Discovery and Vulnerability Evaluation Reinforcement (CADAVER) tool, also underpinned by COLE methodology. It is intended to leverage AI/machine learning to allow identification of potential vulnerabilities to mitigate cyberattack access points through automated/semi-automated means. Combined, these programs ensure warfighters have the necessary tools to assess cyber effectiveness/vulnerability using tri-service approved data standards and streams. Leveraging technology and lessons learned of these three programs provide consistent, credible data and methodology for both offensive and defensive cyberspace operations.

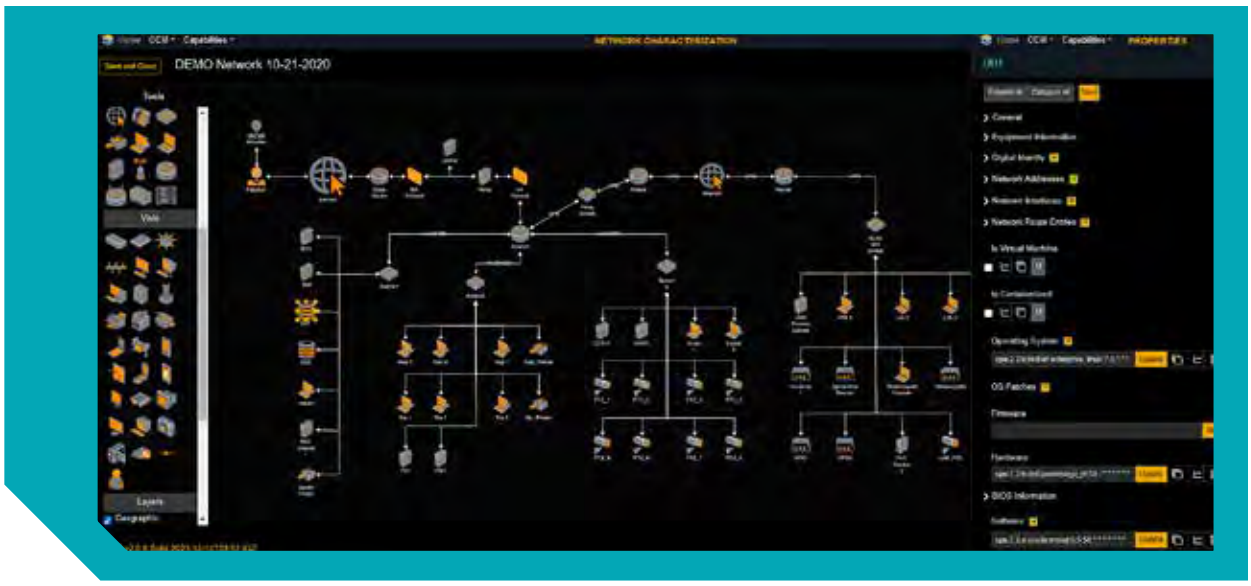


Figure 9. COLE Network Characterization – Notional Data

Electromagnetic Spectrum Fires

Combined with DEW and Cyber JMEM, EMS Fires JMEM enables targeteers and mission planners to adequately respond in a multi-domain operational environment. EMS JMEM will estimate electronic attack (EA) effects and the ability of the warfighter to effectively prosecute adversary targets in contested EMS environments. An illustration of EMS representing range of radiation frequencies used to transmit information wirelessly is shown in Figure 10. EMS JMEM will allow mission planners to assess weapon and combat effectiveness in the presence of adversary

Figure 10. Depiction of EMS deployment

EA (i.e., GPS denial and its effect on kinetic weapon guidance systems). It will also estimate the effects of friendly EA capabilities against adversary targets (e.g., jamming). In FY21, the EMS JMEM development efforts resulted in an initial weaponeering guide, development of data standards, mission area analysis for EA effectiveness, and the review of the Mission Planning GPS Analysis Services model.

Weaponeering Tools Support Interoperability with U.S. Allies and Partners

In FY21, JTCG/ME supported the delivery of weaponeering tools, data sets, and training to coalition partners in support of current operations under Foreign Military Sales agreements. This included the release of weapon effectiveness tables, collateral effects radii tables, and advanced target development capabilities to coalition partners to minimize collateral damage and reduce civilian casualties. These efforts directly supported the Presidential Conventional Arms Control Policy to build partner capacity and prevent civilian casualties. A second effort supported information exchange forums via information exchange annexes with coalition partners. These exchanges facilitate collaboration on methodologies and efforts of mutual interest in the area of weapons effectiveness and collateral damage estimation. A final effort supported standardization of weapon characteristics and interoperability by providing coalition partners with the updated JTCG/ME weapon test information to augment international test operation procedures.

Joint Test and Evaluation

The Joint Test and Evaluation (JT&E) Program enables planning and execution of joint tests to support the future fight.

The Joint Test and Evaluation (JT&E) Program considers emerging technologies and the increasingly complex and dynamic, joint, multi-domain operational environment to develop solutions intended to enhance the United States' operational effectiveness, suitability, and survivability in combat. The Services and Combatant Commands (CCMD) help identify critical challenges that need to be addressed in their areas of responsibility to maintain superiority across joint, multi-domain operations. The JT&E Program provides operational test and evaluation management and expertise to develop, test, and validate joint solutions, including agile warfighting tactics, techniques, and procedures (TTP), concepts of employment (CONEMP), and concepts of operations (CONOPS). In turn, Services and CCMDs provide leadership and support to the planning and execution of JT&E projects and their successful transition to the warfighter. The JT&E Program focuses on joint requirements that cannot be economically or effectively maintained within each of the individual Services and CCMDs. Given the increased integration and dependencies of platform, network, and command and control solutions across the domains, JT&E's mission and unique focus on system of systems testing is becoming increasingly critical to the Department's strategic objectives, to include modernization. JT&E test techniques, workforce talents, and reach-back are essential to the adequate evaluation of the effectiveness of operational plans across the CCMDs.

In FY21, the JT&E Program managed 3 Joint Tests and 10 Quick Reaction Tests (QRT). A Joint Test averages about two years in duration and is preceded by a six-month Joint Feasibility Study. QRTs provide a quicker response to urgent joint needs but must focus their objectives to execute within the shortened, one-year schedule. The JT&E Program also managed one Special Project that was fully resourced by the CCMD sponsor.

Joint Tests

Joint Integrated Fire Control – Directed Energy Weapons for Air Defense (JIFC-DAD)

The advancement of adversaries' ballistic and cruise missiles continue to threaten U.S. interests. U.S. Indo-Pacific Command (USINDOPACOM) J8 recognized the benefits of emerging technologies, specifically directed energy weapons (DEW), in improving air defense capabilities against such threats for U.S. joint forces and coalition partners. When employed with existing kinetic systems, DEW may enhance area air defense capabilities and enable commanders to effectively, affordably, and rapidly defeat massed attacks. In January 2021, JT&E initiated the JIFC-DAD Joint Test to deliver a validated CONEMP that optimizes the integration of DEW with kinetic weapon systems and provides a layered defense of critical assets against a mix of wartime air threats. The first field test is scheduled for early 2022.

Joint Interoperability through Data Centricity (JI-DC)

CCMDs utilize more than 40 independent, mission partner networks in current daily operations, requiring significant resources and complexity to manage multiple computer systems, networks, and associated infrastructure. The DOD Chief Information Officer and U.S. Central Command J6 recognized the benefit of having a data-centric environment that can consolidate operations with coalition and multi-national partners onto a single network. In February 2019, JT&E initiated the JI-DC Joint Test to optimize, test, and evaluate the effectiveness of such a data-centric network currently developed by U.S. Central Command. The joint field tests focused on the ability of U.S. and coalition warfighters to effectively employ data-centric procedures and share information with authorized targeteers in the development of targeting packages. The procedures developed within the JI-DC project are expected to be implemented across multiple CCMDs and adapted for the Joint Staff Joint All Domain Command and Control concept. The JI-DC project should demonstrate that data can be effectively, efficiently, and securely shared using a data-centric network. It should also provide warfighters with confidence that the data are accessible to authorized recipients only.

Recovery Enhanced by Synchronizing Capabilities to Unify Effects (RESCUE)

Personnel recovery operations will face a challenge in the increasingly complex multi-domain, anti-access/area denial environment. The Joint Personnel Recovery Agency recognized that current doctrine and TTPs need to be updated to deploy, assemble, and operate joint forces with acceptable risk in a contested environment so as to provide effective and timely support to personnel recovery. In January 2021, JT&E initiated the RESCUE Joint Test to develop new TTPs that integrate and synchronize information-related capabilities with traditional kinetic fires. Specifically, such TTPs leverage information operations, military deception, public affairs engagement, the use of national assets, interagency coordination, and space-related capabilities. The RESCUE TTP demonstrated the benefit of integrating these capabilities into the joint planning processes during a risk reduction event at Marine Forces Special Operations Command Raven Exercise in October 2021. The primary field test to demonstrate the execution of personnel recovery using the updated TTPs is scheduled for Keen Edge Exercise at USINDOPACOM in January 2022.

Quick Reaction Tests

Assessment of Joint Maritime Mining on USINDOPACOM Operational Plans (AMMO)

Maritime mining is a low-cost and effective means to deny an adversary access to geographic locations and delay their action. U.S. adversaries have advanced their integrated air defense systems and substantially increased risk to the warfighter when deploying mines. USINDOPACOM J8 recognized the need to develop, test, and validate a joint CONEMP to maximize the wartime effect of both legacy and advanced maritime mines, given the increased risk in their deployment. In April 2021, JT&E initiated the AMMO QRT that will utilize advanced modeling and simulation to develop a CONEMP for near-term and legacy mine capabilities intended to maximize operational and strategic effect within USINDOPACOM operational plans and minimize risk to U.S. forces and coalition partners. The AMMO QRT is scheduled to complete the first table top exercise in January 2022, while the second is planned for Spring 2022. The AMMO QRT will provide critical updates to the Office of the Chief of Naval Operations N81 Capabilities Based Analysis for Maritime Mining.

Integration of Joint Optimization for Electromagnetic Spectrum (EMS) Superiority (I-JOES)

Joint forces are critically dependent on the electromagnetic spectrum (EMS) across all domains and functions. To achieve EMS superiority, USINDOPACOM J8 recognized the need for validated cross-functional TTPs that integrate intelligence, electromagnetic warfare, and spectrum management at the component level. In April 2021, JT&E initiated the I-JOES QRT to develop component-level TTPs that: 1) incorporate EMS targets and collection requirements into joint targeting or collection cycles, 2) integrate EMS operations into the joint air tasking cycle, and 3) develop component EMS operations plans to feed the CCMD and Joint Task Force Joint Electromagnetic Spectrum Operations. The I-JOES QRT will complete the first field test during the Keen Edge Exercise in January 2022.

Joint Basin-Scale Communications (J-BASC)

U.S. Strategic Command (USSTRATCOM) recognized an emerging communications technology that could be integrated within the existing architecture to meet a critical joint force need. In April 2021, JT&E initiated the J-BASC QRT to develop, test, and evaluate the new communications CONOPS that considers this technology. Planning is underway for field test activities scheduled in January and May 2022. Details are classified.

Joint Discreet Adversary Strategy Defeat (J-DASD)

USSTRATCOM J8 recognized the need to apply tailored deterrent strategies for specific adversaries by integrating the full spectrum of U.S. military capabilities, both nuclear and conventional, with elements of U.S. national power. In April 2021, JT&E initiated the J-DASD QRT to develop and test CONOPS that specifically addresses the following areas: 1) integration of strategic deterrence action, 2) development of deterrence options, 3) degrading potential impact of threat actors, 4) executing deterrence operations in a timely manner, and 5) reducing the risk of deterrence failure. The J-DASD QRT will conduct two field test events during USSTRATCOM exercises to collect measurements for the entire messaging processes.

Joint Integrated Network – Korea (JIN-K)

U.S. Forces Korea are updating their near real-time, joint/coalition integrated air-ground common operational picture. The update will enhance integration and distribution of sensor and targeting data to mobile and command post sites throughout the theater of operations. Joint Staff J6 recognized the need to develop new TTPs that optimize the benefits of this update and deliver the required joint capabilities within the Multi-Domain Resilient Air-Ground Operations Network. In January 2021, JT&E initiated the JIN-K QRT to develop, test, and validate such TTPs. The JIN-K QRT will conduct field tests in Spring 2022. The validated TTP will enable warfighters to effectively utilize available data within a common operational picture and retain real-time situational awareness from the tactical through strategic levels. Further, the TTP will reduce bandwidth consumption and directly contribute to projection of combat power.

Joint Interagency – 5G Radar Altimeter Interference (JI-FRAI)

In March 2020, the Federal Communications Commission reallocated the 3.7 to 3.98 GHz frequency spectrum to 5G C-Band applications. The Office of the Under Secretary of Defense for Acquisition and Sustainment and U.S. Transportation Command recognized the need to determine the effects of 5G C-Band interference on military, U.S. Coast Guard, U.S. Customs and Border Protection, and Civil Reserve Air Fleet-partner aircraft radar altimeters (RADALT). In April 2021, JT&E initiated the JI-FRAI QRT to provide an initial assessment of 5G interference on selected military RADALT systems. The initiative is using military RADALT as a use case to support current and future operational avionics testing, mitigations, and standards development. The JI-FRAI QRT will assess 5G interference risks, mitigations, standards, conditions, and future test resource requirements by leveraging Service-funded bench test results and conducting improved operator-in-the-loop bench testing, over-the-air testing, and operationally realistic 5G interference flight tests. The initial phase of testing commenced with enhanced bench testing scheduled for December 2021. The final two phases of testing are scheduled to occur in FY22 and will deliver a Combined Test Methodology with procedures for evaluating 5G interference on RADALTs and other avionics.

Joint/Interagency – Ground/Air Transponder Operational Risk Reduction (JI-GATOR)

Multiple transponder systems (across aviation and ground-based services) broadcast data such that commercial services can collect and display those data to any end user. Aviation is dependent on broadcast modes such as Automatic Dependent Surveillance-Broadcast for navigation, air traffic control, and flight safety. Headquarters, U.S. Air Force A3, and North American Aerospace Defense Command – U.S. Northern Command recognized that the open, unencrypted design of Automatic Dependent Surveillance-Broadcast could create operational security issues for military, U.S. Coast Guard, and U.S. Customs and Border Protection aircraft and introduce vulnerabilities affecting air surveillance accuracy and air surveillance system availability. In June 2019, JT&E initiated the JI-GATOR QRT to develop, test, and validate joint and interagency TTPs intended to mitigate vulnerabilities in aviation transponder data confidentiality, integrity, and availability. JT&E completed the field tests in May and July 2020. TTPs enabled operators to configure their systems to restrict unwanted transponder emissions/tracks and interpret the data in the air traffic control environment, improving operational security, air traffic control, and air surveillance. These TTPs accounted for the differences between air traffic

control system hardware configurations in the DOD and interagency aircraft across a range of air traffic control environments.

Joint Interagency Net-Centric Cross-Domain Risk to Operational Cyber Systems (JINX ROCS)

The Eastern Air Defense Sector and Western Air Defense Sector rely on a range of transponders and associated datalinks that underpin air defense awareness and control in support of the homeland defense mission. DOT&E recognized the need to evaluate the cyber risks to the Eastern Air Defense Sector/Western Air Defense Sector architecture, system, and information. In April 2021, JT&E initiated the JINX ROCS QRT to develop, test, and validate time-critical TTPs to detect, respond to, and recover from cyber interference within the data stream and architecture, as well as a means to optimize available sensors to support these activities. The first field test series began at Eastern Air Defense Sector Headquarters in December 2021, with completion scheduled in February 2022. The JINX ROCS QRT is scheduled to conduct the second field test at Arctic Edge in April 2022. Testing will validate the TTPs needed for air defense sector operators to maintain battlespace situational awareness in a cyber-contested environment.

Joint Littoral Fire Support Coordination (J-LIFE)

The joint warfighter requires doctrine to deconflict, coordinate, and integrate attacks that include newly fielded capabilities and emerging technologies. USINDOPACOM J8 recognized the need for an effective doctrine that minimizes the risk of fratricide, reduces duplication of effort, and assists in shaping the operating environment for land-based fires into the maritime domain. In January 2021, JT&E initiated the J-LIFE QRT to develop and validate TTPs to update existing joint and Service doctrine in support of the U.S. Marine Corps' Expeditionary Advanced Base Operations and U.S. Army's Multi-Domain Task Force. To meet these objectives, the J-LIFE QRT conducted an observation event at Project Convergence in October 2021 and is scheduled to utilize a U.S. Pacific Fleet Battle Problem exercise to conduct the first field test in January 2022.

Joint Sustainment in the Littorals – Fuel and Water Distribution (JSL-FWD)

Expeditionary Advanced Base Operations require forces to continue to distribute fuel and water in an evolving anti-access/area denial environment. USINDOPACOM J8 recognized the need for joint CONOPS to enable flexible and resilient logistical supply and sustainment to maintain operations in such an increasingly complex and dynamic environment. In January 2021, JT&E initiated the JSL-FWD QRT to develop, test, and validate a joint CONOPS for agile, scalable, and expeditionary fuel and water distribution that connects existing tactical fuel and water distribution systems ashore to locations beyond the high water mark via an over-the-shore connection. The JSL-FWD QRT is scheduled to conduct field tests in early 2022.

Special Projects

Joint – Rapid Alerting for Survivability and Endurability (J-RASE)

Electromagnetic pulse is an evolving threat to critical U.S. infrastructure, including strategic command, control, and communications (C3) systems, requiring the need for timely notification and protective procedures to prevent damage to such systems. USSTRATCOM recognized the need for an enterprise solution to endure and sustain operations that support the deterrent capability of the joint force. In October 2019, JT&E initiated the J-RASE Special Project to develop, test, and validate TTPs focused on improving C3 system and logistics survivability during an electromagnetic pulse alert notification. The J-RASE team completed two field tests demonstrating the effectiveness of the operationally realistic processes for rapid notification of forces and supporting agencies to initiate actions to enhance the survivability of their C3 systems and manage their units'

capability to endure and sustain operations in a degraded, contested communications environment. The J-RASE TTP improves the joint warfighters' ability to rapidly prepare for an attack, initiate protective measures, recover quickly, sustain, and endure while continuing to meet current operational requirements.

Test and Evaluation Threat Resource Activity

Test and Evaluation Threat Resource Activity (TETRA) is a joint duty activity between DOT&E and the Defense Intelligence Agency (DIA) established in 2000 to ensure that OT&E and LFT&E programs and warfighter training are adequately informed by the latest and emerging intelligence data.

Test and Evaluation Threat Resource Activity (TETRA) is comprised of Defense Intelligence Agency (DIA) analysts responsible for supplying authoritative and timely intelligence assessments of the current and emerging multi-domain threat environment. Specifically, TETRA: 1) generates products that include intelligence-based analysis of current and emerging threats, 2) facilitates the acquisition of foreign materiel needed for testing or development of threat surrogates, 3) oversees threat surrogate verification and validation to include threat modeling and simulation (M&S), and 4) leverages emerging science and technologies to project expected threat capabilities.

TETRA Executes Intelligence Analysis to Support Credible OT&E and LFT&E

In coordination with the DIA and the Services Intelligence Production Centers, TETRA conducts independent intelligence research and analysis to generate products required to adequately define scenarios for the evaluation of U.S. weapon systems against operationally representative threats and targets. Most notable products include assessments of order of battle, threat Concept of Operations, and tactics, techniques, and procedures (TTPs) to be used against U.S. systems. TETRA also supplies the T&E community with threat and target signatures and characteristics, as well as the status (availability, verification and validation) of threat surrogates required for an adequate OT&E or LFT&E program. For example, in FY21, TETRA:

- Updated emerging technology threats and changing adversaries' TTPs of tactical, operational, and strategic significance to our U.S. ground forces and programs under oversight
- Defined small boat design characteristics, operational performance, signatures, order of battle, technology trends, and swarm attack tactics against multiple naval air and surface programs to enable adequate evaluation of the operational effectiveness of naval strike warfare
- Supplied intelligence assessments of ballistic missile and counter-space threats to inform testing of ballistic, hypersonic, and cruise missile defense systems
- Collected and analyzed event data and open source intelligence to supply cyber threat-specific data and cyber threat intelligence support

TETRA Facilitates Acquisition of Actual Foreign Threats

OT&E and LFT&E programs rely on the availability of actual, foreign material, threat systems to either test our systems against the real threat/target or reverse engineer the threat/target to support the development of threat/target surrogates (either physical or models). In the absence of the actual threat, TETRA supplies the best available intelligence data on the threat/target characteristics and capabilities critical to the development of target/threat surrogates.

To secure actual systems for intelligence analysis and use in operational testing, TETRA works directly with the Joint Foreign Materiel Program Office, overseen by the Office of the Under Secretary of Defense for Intelligence. In coordination with the OT&E and LFT&E community, TETRA supplies a prioritized and coordinated list of foreign materiel required for upcoming operational and live fire tests to inform Intelligence Community collection opportunities. The Joint Foreign Materiel Program is a critical link between the T&E community, Defense Intelligence Agency, and the Department of State that increases the visibility of T&E requirements in support of operationally representative testing and warfighter training. Foreign materiel requirements span all warfare areas, and TETRA is currently monitoring and coordinating over 100 acquisition efforts. The demand for a wide array of foreign man-portable air-defense systems (MANPADS) continues to be high for: 1) the development of MANPADS surrogates to enable adequate testing of countermeasures (as discussed in the Center for Countermeasures section of this report), 2) representative missile seekers and software for use in hardware-in-the-loop laboratories, and 3) LFT&E to test the vulnerability of U.S. weapon systems when engaged by such a threat. Foreign anti-tank guided missiles have also been in high demand to support the testing of the evolving Active Protection System employed by ground combat vehicles. GPS jammers have been in demand for testing of GPS-guided weapons, and very high frequency (VHF) radars have been required for programs such as the F-35 due to longer acquisition range and low probability of intercept.

While TETRA works with the T&E community to develop the foreign materiel priorities for T&E programs, there is a critical need to advance the acquisition process of foreign materiel when they become available. Foreign materiel acquisitions are usually lengthy and unpredictable, making it difficult to identify appropriate year funding, resulting in missed opportunities to acquire such systems when they do become available. A no-year or non-expiring dedicated funding line for foreign materiel acquisitions would mitigate this shortfall.

TETRA Supplies Accredited Threat and Target Models and Surrogates

In the absence of actual, foreign threats, which could be difficult to acquire, TETRA supports the T&E community with intelligence data and analytical expertise required to develop and accredit threat and target surrogates, either physical replicates or M&S. In accordance with DOD Instruction 5000.61, and in coordination with Intelligence Production Centers, TETRA leads DOT&E's Integrated Technical Evaluation and Analysis of Multiple Sources (ITEAMS) projects that evaluate options to build threat-representative simulators and models from intelligence, open source, and industry data. TETRA also develops and continues to maintain the Threat Systems Database, which catalogs threat assets available for the T&E community. ITEAMS projects are critical to adequate OT&E and LFT&E.

TETRA is also responsible for the threat surrogate verification and validation process to assess the uncertainties of the threat surrogate compared to the actual threat system that the warfighter would encounter in combat. To accomplish this, TETRA leads the Threat M&S Working Group Enterprise development of common and authoritative threat models, delivering a threat surrogate verification and validation report, documenting the comparison of the threat representation to intelligence data, noting the differences, and explaining the potential effect of those differences on test adequacy. Threat model development efforts are often stove-piped, proprietary, and single use. TETRA ensures threat M&S is based on an enterprise management process that provides developmental and interoperability standards to enable data correlation with threat models across the T&E spectrum.

In FY21, TETRA provided threat intelligence, validation expertise, and oversight for more than 17 Joint and Service threat representation validation efforts, including the Navy's Integrated Digital Acquisition Radar Environment—Upgrade; the Next-Generation Jammer to develop a method to validate and certify the radar electronic attack countermeasure tool; and the M&S gaps and verification, validation, and accreditation in support of Ballistic Missile Defense System ground testing. TETRA also continued the development, validation, and delivery of 10 radio frequency and 10 infrared high-priority threat models, as well as two high-fidelity, closed-loop, electronic warfare-capable, emulative threat models: 1) Laboratory Intelligence Validated Emulators (LIVE) and 2) Common High-Assurance Internet Protocol Encryptor Interoperable Manager for Efficient Remote Administration (CHIMERA).

TETRA is also managing the Advanced Satellite Navigation Receiver effort intended to develop a next-generation, six degrees of freedom, Time-Space-Position Information Satellite Navigation Receiver test kit that provides high-fidelity and accurate GPS and inertial measurement unit instrumentation characteristics that operate in a highly dynamic environment. This effort meets the needs of new and upcoming near-peer missile autopilots, guidance, and M&S requirements identified in intelligence community and T&E reviews.

TETRA Keeps Pace with Emerging Threats and Targets

TETRA focuses on projections of future technology and intelligence mission data availability to create the most adequate representation of threat system characteristics and performance. Artificial intelligence, machine learning, deep learning, and neural network capabilities are toolsets that TETRA intends to pursue and use to analyze variances in the threat characteristics to quickly identify design space parameters responsible for variances in weapon performance. This approach is necessary to enable the DOD to meet the challenges outlined in the 2018 National Defense Strategy given the emergence of the contested space environment and technologies such as cognitive electronic warfare (EW) systems.

DOD cognitive EW systems are rapidly developing and will soon become intrinsic to DOD air, land, sea, and space combat systems, supplying advanced EW self-protection and electronic attack capabilities to next generation DOD platforms. DOD cognitive EW systems will heavily rely on artificial intelligence and machine learning techniques with the cognitive capability required to defeat advanced threat systems. Adversary threat systems are also projected to increasingly use cognitive capability. TETRA has been charged with leading the effort of identifying cognitive EW system T&E challenges and recognizing the need for a standardized, reusable cognitive test environment, U.S. and foreign cognitive threat models, and common cognitive tool sets that can be used across a range of developmental and operational T&E activities. These efforts will significantly affect test capability by providing a radically increased adoption of M&S early in the developmental test cycle, which will be a necessity for operational testing of complex cognitive systems.

Appendix

Oversight List
DOT&E Activities
SASC Statement for the Record
HASC Statement for the Record
Service Secretary Comments
Index of Programs

II Oversight List

DOT&E Oversight List as of September 30, 2021

- 120mm Advanced Multi-Purpose (AMP), XM1147, High Explosive Multi-Purpose with Tracer (HEMP-T)
- 30mm Multi-Function Munition (MFM)
- 7.62mm Advanced Armor Piercing (ADVAP), M1158
- Abrams M1A1 SA; M1A2 SEP; APS
- AC-130J
- Acoustic Rapid COTS Insertion for SONAR
- Advanced Airborne Sensor
- Advanced Anti-Radiation Guided Missile - Extended Range
- Advanced Arresting Gear
- Advanced Field Artillery Tactical Data System (AFATDS) Version 7
- Advanced Pilot Trainer
- Advanced Threat Detection System
- AEGIS Modernization (Baseline Upgrades)
- AEHF - Advanced Extremely High Frequency (AEHF) Satellite Program
- Aerosol and Vapor Chemical Agent Detector
- AGM-114L LONGBOW HELLFIRE Air to Ground Missile
- AH-64E Apache Remanufacture/New Build
- AIM-120 Advanced Medium Range Air-to-Air Missile
- AIM-260A Joint Advanced Tactical Missile
- AIM-9X Block II Sidewinder
- Air and Missile Defense Radar (AMDR) / AN/SPY-6
- Air Force Integrated Personnel and Pay System (AF-IPPS)
- Air Force Intercontinental Ballistic Missile Fuze Modernization
- Air Force Maintenance, Repair and Overhaul Initiative (MROi)
- Air Force Next Generation Air Dominance
- Air Operations Center Weapon System Modifications
- Air Warfare Ship Self Defense Enterprise
- Air-Launched Rapid Response Weapon
- Amphibious Combat Vehicle (ACV) Family of Vehicles (FoV)
- AN/AQS-20X Minehunting Sonar and Tow Vehicle (all variants)
- AN/TPQ-53 Counterfire Target Acquisition Radar
- Armored Multipurpose Vehicle (AMPV)
- Armored Truck - Heavy Equipment Transporter (HET)
- Army Contract Writing System
- Army Mobile Wheeled Howitzer (AMWH)
- Assault Breaching System Coastal Battlefield Reconnaissance and Analysis System (all variants)
- Assured Positioning, Navigation, and Timing
- B-21 Long Range Strike Bomber
- B-52 Commercial Engine Replacement Program (CERP)
- B-52 Radar Modernization Program (RMP)
- B61 Mod 12 Life Extension Program Tailkit Assembly
- Ballistic Missile Defense System
- Barracuda Mine Neutralization System
- Big Sky
- Bradley ECP; MOD; APS
- Cannon Delivered Area Effects Munitions (C-DAEM) Armor (Inc 1)
- Cannon-Delivered Area Effects Munitions (C-DAEM) Dual Purpose Improved Conventional Munition (DPICM) Replacement (Inc 2)
- Capability Set 21 Integrated Tactical Network - Rapid Fielding
- CH-47F Modernized Cargo Helicopter
- CH-53K King Stallion

DOT&E Oversight List as of September 30, 2021

- CMV-22 Joint Services Advanced Vertical Lift Aircraft - Osprey -- Carrier Onboard Delivery (COD)
- ***Columbia*** Class SSBN - including all supporting PARMs
- Command Post Computing Environment/Tactical Services Infrastructure
- Common Infrared Countermeasures (CIRCM)
- Consolidated Afloat Networks and Enterprise Services
- Cooperative Engagement Capability (CEC)
- CVN 78 - ***Gerald R. Ford***-Class Nuclear Aircraft Carrier
- DDG 1000 – ***Zumwalt***-Class Destroyer and associated PARMs
- DDG 51 Flight III and associated PARMS
- Deep Space Advanced Radar Capability
- Defense Enterprise Accounting & Management System
- Defense Enterprise Office Solution (DEOS)
- Defense Medical Information Exchange (DMIX)
- Defense Security Assistance Management System (DSAMS BLK III)
- Deliberate and Crisis Action Planning and Execution Segments (DCAPES) Inc. 2B
- Digital Modernization Strategy (DMS) – Related Enterprise Information Technology Initiatives
- Distributed Aperture Infrared Countermeasure
- Distributed Common Ground System - Army (DCGS-A)
- Distributed Common Ground System - Navy (DCGS-N)
- DoD Healthcare Management System Modernization (DHMSM)
- E-2D Advanced Hawkeye
- Electro-Magnetic Aircraft Launching System
- Electronic Warfare Planning and Management Tool (EWPMT)
- Enhanced Polar System
- Enterprise Air Surveillance Radar
- Evolved Sea Sparrow Missile Block 2
- Evolved Strategic Satellite Communications
- Extended Range Cannon Artillery (ERCA)
- EXTRA LARGE UNMANNED UNDERSEA VEHICLE (XLUUV)
- F/A-18E/F Super Hornet Aircraft
- F-15 Eagle Passive Active Warning Survivability System
- F-15 Infrared Search and Track
- F-15EX
- F-16 Radar Modernization Program
- F-22 - RAPTOR Advanced Tactical Fighter Aircraft
- F-22 Capability Pipeline
- F-35 - Lightning II Joint Strike Fighter (JSF) Program
- Family of Advanced Beyond Line-of-Sight Terminals
- Family of Advanced Beyond Line-of-Sight Terminals Force Element Terminal
- Family of Medium Tactical Vehicles A2 (FMTV A2)
- FFG(62) Guided Missile Frigate
- Future Long Range Assault Aircraft MTA
- Future Operationally Resilient Ground Evolution Rapid Prototype
- Future Vertical Lift (FVL) Future Unmanned Aircraft System (FUAS)
- Geosynchronous Space Situational Awareness Program
- Global Command & Control System - Joint (GCCS-J)
- Global Positioning System (GPS) Enterprise Oversight
- Global Positioning System III
- GPS III Follow-on Production
- GPS Next Generation Operational Control System Block 3F

DOT&E Oversight List as of September 30, 2021

- Ground Based Strategic Deterrent
- Ground/Air Task Oriented Radar
- Guided Multiple Launch Rocket System Family of Munitions Including Alternative Warhead (AW); Unitary; Extended Range (ER)
- Hammerhead Encapsulated Effector Program
- Handheld, Man pack, and Small Form Fit (including Handheld and Manpack components)
- Heavy Dump Truck
- HH-60W Jolly Green II
- High Mobility Artillery Rocket System (HIMARS)
- Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs) - AF
- Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs) - Army
- Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs) - Navy
- Improved High Explosive Dual Purpose 40mm Cartridge
- Improved Turbine Engine Program (ITEP)
- Indirect Fire Protection Capability Increment 2 - Intercept (IFPC Inc 2-I)
- Infantry Squad Vehicle (ISV)
- Infrared Search and Track
- Integrated Air and Missile Defense
- Integrated Personnel and Pay System-Army Increment 2
- Integrated Strategic Planning and Analysis Network Increment 5
- Integrated Tactical Network (ITN) - Rapid Prototyping
- Integrated Visual Augmentation System (IVAS) Rapid Prototyping
- Integrated Visual Augmentation System Rapid Fielding
- Javelin Antitank Missile System - Medium
- Joint Air-to-Ground Missile (JAGM)
- Joint Air-to-Surface Standoff Missile
- Joint Assault Bridge (JAB)
- Joint Battle Command Platform (JBC-P)
- Joint Biological Tactical Detection System
- Joint Cyber Warfighting Architecture - Joint Cyber Command and Control
- Joint Cyber Warfighting Architecture - Unified Platform
- Joint Light Tactical Vehicle Family of Vehicles
- Joint Operational Medicine Information Systems
- Joint Regional Security Stack (JRSS)
- KC-46A Tanker Modernization
- Key Management Infrastructure (KMI)
- Large Displacement Unmanned Undersea Vehicle (LDUUV)
- LAV (NAVY)
- LHA 6 Flt 0 and associated PARMs
- LHA 8 Flt I and associated PARMs
- Light Amphibious Warship
- Limited Interim Missile Warning System
- Littoral Combat Ship (LCS) Anti-submarine Warfare (ASW) Mission Package
- Littoral Combat Ship (LCS) Mine-countermeasures (MCM) Mission Package
- Littoral Combat Ship (LCS) Surface Warfare (SUW) Mission Package
- Littoral Combat Ship (LCS), ***Freedom*** and ***Independence*** Variant Seaframes
- Logistics Modernization Program (Restructured)
- Long Range Hypersonic Weapon (LRHW)
- Long Range Stand Off Weapon
- Lower Tier Air and Missile Defense Sensor
- LPD 17 Flt II
- M88A2 Heavy Equipment Recovery Combat Utility Lift Evacuation System
- Maneuver-Short Range Air Defense
- Massive Ordnance Penetrator Modification
- MH-139A Grey Wolf

DOT&E Oversight List as of September 30, 2021

- milCloud
- Military Global Positioning System (GPS) User Equipment Increment 1
- Military GPS User Equipment Increment 2 Miniature Serial Interface
- Military Personnel Data System
- MINIATURE AIR LAUNCHED DECOY-NAVY
- Mission Partner Environment (MPE)
- MK 48 ADCAP COMMON BROADBAND ADVANCED SONAR SYSTEM
- Mk 54 torpedo/MK - 54 VLA/MK 54 Upgrades Including High Altitude ASW Weapon Capability (HAAWC)
- Mk21A Reentry Vehicle
- Mobile / Handheld Computing Environment (M/HCE)
- Mobile Protected Firepower
- Mobile User Objective System
- Mounted Mission Command - Software
- MQ-25 Stingray
- MQ-4C Triton
- MQ-8 Fire Scout Unmanned Aircraft System
- Multi-Function Electronic Warfare
- Multi-Functional Information Distribution System
- Multiple Launch Rocket 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 Conventional Prompt Strike
- Navy Maritime Maintenance Enterprise Solution - Technical Refresh
- Navy Personnel and Pay System
- Nett Warrior
- Next Generation Jammer - Mid-Band
- Next Generation Jammer Low Band
- Next Generation Operational Control System
- Next Generation Overhead Persistent Infrared Space
- Next Generation Squad Weapons - Fire Control Rapid Fielding (NGSW FC RF)
- Nuclear Planning and Execution System
- Offensive Anti-Surface Warfare Increment 1 (Long Range Anti-Ship Missile)
- Offensive Anti-Surface Warfare, Increment 2 (Air and Surface Launch)
- Optionally Manned Fighting Vehicle
- Over The Horizon Weapon System
- Paladin/FASSV Integrated Management (PIM)
- Patriot Advanced Capability 3
- Precision Guidance Kit Family of Fuzes
- Precision Strike Missile (PrSM)
- Presidential and National Voice Conferencing Integrator
- Protected Tactical Enterprise Service
- Protected Tactical SATCOM
- Public Key Infrastructure (PKI) Inc. 2
- Rolling Airframe Missile Block 2
- RQ-7B Shadow Tactical Unmanned Aircraft System
- SBIRS - Space-Based Infrared System Program
- SF - Space Fence
- Ship Self Defense System (SSDS)
- Ship to Shore Connector
- Small Diameter Bomb Increment II
- SOCOM Dry Combat Submersible Medium (DCSM)
- Soldier Protection System
- Space Based Infrared System (SBIRS) Survivable and Endurable Evolution (S2E2)
- Space Command and Control System
- Stand In Attack Weapon
- Standard Missile 2 (SM-2) including all mods

DOT&E Oversight List as of September 30, 2021

- Standard Missile -6 Block IB
- Standard Missile-6
- Stryker Family of Vehicles to include all variants (including NBCRV)
- Submarine Torpedo Defense System (Sub TDS) including Next Generation Countermeasure System (NGCM)
- Surface Electronic Warfare Improvement Program Block 2
- Surface Electronic Warfare Improvement Program Block 3
- Surface Mine Countermeasures Unmanned Undersea Vehicle (SMCM UUV)
- Survivable Airborne Operations Center E-4B Recap
- Tactical Tomahawk Modernization and Enhanced Tactical Tomahawk (Maritime Strike) (includes changes to planning and weapon control system)
- T-AO 205 ***John Lewis*** Class Fleet Replenishment Oiler
- Teleport, Generation III
- Terrain Shaping Obstacles (TSO)
- Theater Medical Information Program - Joint Increment 2
- Third Generation FLIR
- Three-Dimensional Expeditionary Long-Range Radar
- Tranche 1 Transport Layer
- Trident II (D-5) Sea-Launched Ballistic Missile
- UH-60M Black Hawk Helicopter
- UH-60V Black Hawk Digital Cockpit
- Unmanned Influence Sweep System (UISS) include Unmanned Surface Vessel (USV) and Unmanned Surface Sweep System (US3)
- VC-25B
- VH-92A Presidential Helicopter
- ***Virginia*** Class SSN 774 and associated PARMS
- Weather Satellite Follow-on (WSF)
- Wide Area Surveillance
- XM1170 30x173mm Armor Piercing, Fin Stabilized, Discarding Sabot with Trace

II DOT&E Activities

Table 1. FY21 DOT&E Reports to Congress	
Program	**Date**
Early Fielding Report	
Family of Beyond Line of Sight Terminals (FAB-T) Early Fielding Report	December 2020
Follow-on Operational Test and Evaluation Reports	
Acoustic Rapid COTS Insertion for SONAR (ARC-I) APB-15 FOT&E Interim Report	May 2021
AIM-9X Block II OFS 9.410 FOT&E Report	September 2021
Bradley M2A4/M7A4 Follow-on Operational Test and Evaluation (FOT&E) Report	June 2021
Military Health System (MHS) GENESIS Follow-On Test and Evaluation Cybersecurity Assessment Report	August 2021
RQ-7Bv2 Shadow Block III FOT&E II Report	May 2021
Stryker ATGM Follow on Test and Evaluation (FOT&E) Report	May 2021
USG - 3B Cooperative Engagement Capability Follow-on Operational Test and Evaluation Report	November 2020
Initial Operational Test and Evaluation Reports	
Amphibious Combat Vehicle (ACV) Combined Initial Operational Test and Evaluation (IOT&E) and Live Fire Test and Evaluation (LFT&E) Report	November 2020
Handheld, Manpack, and Small-Form Fit Leader Radio and Manpack (HMS) Initial Operational Test and Evaluation (IOT&E) Report	July 2021
High Altitude Anti-Submarine (ASW) Weapon Capability (HAAWC) IOT&E Report	June 2021
Initial Operational Test and Evaluation (IOT&E) Report with classified annex for the VH-92A Presidential Helicopter Replacement Program	September 2021
Joint Assault Bridge (JAB) Initial Operational Test and Evaluation (IOT&E) 2 Report and Classified Survivability Annex	March 2021
Operational Assessment Reports	
Initial Maneuver, Short-Range Air Defense (IM-SHORAD) Operational Assessment	August 2021
Integrated Visual Augmentation System (IVAS) Capability Set 3 Soldier Touchpoint 3 Report (OA Report)	March 2021
Integrated Visual Augmentation System (IVAS) Capability Set 4 Operational Assessment	September 2021
LHA 8 Operational Assessment (OA) Report	September 2021
Operational Test and Evaluation Report	
Flight Test Aegis Weapon System (FTM-44) Test Report	June 2021
Live Fire Test and Evaluation Reports	
Abrams M1A2 System Enhancement Package Version 3	December 2020
M917A3 Heavy Dump Truck (HDT) Live Fire Test and Evaluation Report	September 2021
Special Reports	
MHS GENESIS Change Management Strategies and Training Programs Evaluation Results Brief	March 2021
DOT&E Certification and Risk Assessment of Test Strategies for Air Force, Army, Navy and United States Special Operations Command Middle Tier Acquisition (MTA) (804) and Accelerated Acquisition Programs	May 2021
Ballistic Missile Defense System Report	
2020 DOT&E Assessment of the Ballistic Missile Defense System	February 2021

Table 2. FY21 DOT&E Reports not sent to Congress	
Program	**Date**
Follow-on Operational Test and Evaluation Report	
Public Key Infrastructure (PKI) Inc. 2 FOT&E Report and Test Interference Memo	September 2021
Operational Assessment Reports	
F-15 Eagle Passive Active Warning System (EPAWSS) Milestone C Decision Point 1 Report	October 2020
Army's Integrated Air and Missile Defense (AIAMD) System Increment II Operational Assessment Report	November 2020

Table 3. FY21 DOT&E TEMPs and Test Strategy Documents Approved[1]	
Program	**LF**
Advanced Anti-Radiation Guided Missile (AARGM) Extended Range Test and Evaluation Master Plan for Milestone C - Approval	*
Advanced Multi-Purpose (AMP) Cartridge XM1147 Test and Evaluation Master Plan (TEMP)	*
Amphibious Combat Vehicle (ACV) Test and Evaluation Master Plan (TEMP) Full-Rate Production (FRP) Update	*
Approval of Test and Evaluation Master Plan Number 1736, Revision B for the Infrared Search and Track System (IRST)	
Approval of the Air Force Depot Maintenance, Repair and Overhaul Initiative Test and Evaluation Master Plan	
Armored Multi-Purpose Vehicle (AMPV) Test and Evaluation Master Plan (TEMP)	*
B-52 Radar Modernization Program (RMP) MS B TEMP Approval	
Ballistic Missile Defense Systems (BMDS) Integrated Master Test Plan (IMTP), v22.1	*
Electronic Warfare Planning and Management Tool (EWPMT) Increment I Simplified Acquisition Master Plan (SAMP)	
F/A-18E/F SCS H16 TEMP	
GPS Enterprise Test & Evaluation Master Plan (E-TEMP) Revision C	
Infantry Squad Vehicle (ISV) Test and Evaluation Master Plan (TEMP)	
Integrated Personnel and Pay System – Army (IPPS-A), PART VI: UPDATED Annex 2 of the IPPS-A Increment II Post-Milestone B Test and Evaluation Master Plan (TEMP) for Release 3 Version 2.0, 15 March 2020 (Contract Option Decision)	
Integrated Strategic Planning and Analysis Network (ISPAN) Increment 5 (Inc 5) Mission Planning and Analysis System (MPAS) Test and Evaluation Master Plan (TEMP)	
Next Generation Jammer - Low Band test and Evaluation Master Plan TEIN 1829	
Next Generation Jammer- Mid Band Test and Evaluation Master Plan (TEMP) TEIN 1824	
Nuclear Planning and Execution System (NPES) Recapitalization Test and Evaluation Master Plan (TEMP) and Agile Operational Test Master Test Plan (Decision Point TBD)	
Official Submission: IM-SHORAD Master Test Document	*
Official Submission: Precision Strike Missile (PrSM) Increment 1 Test and Evaluation Master Plan (TEMP) supporting Milestone (MS) B	*
Presidential Network Voice Conferencing (PNVC) Test and Evaluation Master Plan (TEMP) Approval	
Stryker 30mm Lethality Engineering Change Proposal (ECP) Test and Evaluation Master Plan (TEMP) Annex: Testing Strategy for the Stryker 30mm Lethality ECP in Support of Conditional/Full Material Release (CMR/FMR)	*

Table 3. FY21 DOT&E TEMPs and Test Strategy Documents Approved[1]	
Program	**LF**
Surface Ship Undersea Warfare (USW) Combat System (AN/SQQ-89(V)15) Test and Evaluation Master Plan (TEMP) Update Approval	
T-AO 205 Test and Evaluation Master Plan (TEMP) Rev 1	*
Test and Evaluation Master Plan Supporting Milestone C Decision for the Joint Biological Tactical Detection System (JBTDS), ACAT II, 4 June 2020	
Update to 3rd Generation Forward Looking Infrared (3GEN FLIR) Milestone B (MS B) Test and Evaluation Master Plan (TEMP)	
Weather Satellite Follow-on Microwave (WSF-M) Milestone B (MS B) Test and Evaluation Master Plan (TEMP)	
1. Live Fire test strategies marked with *	

Table 4. DOT&E Live Fire Test and Evaluation Strategies/ Management Plans Approved
Live Fire Test and Evaluation Strategy for the Joint Multiple Effects Weapon System (JMEWS)
Penetrating Counter Air Alternate Live-Fire Test Plan Approval

Table 5. DOT&E Test Plans Approved
AAS FOT&E Test Plan & Decision Brief
Advanced Tracking and Launch Analysis System (ATLAS) Operational Utility Evaluation (OUE) Plan Approval (Test starts in Dec 2020)
Adversarial Assessment (AA) Test Plan (TP) for the AN/TPQ-53 Counter Fire Target Acquisition Radar
Adversarial Assessment (AA) Test Plan (TP) for the Stryker Common Remotely Operated Weapon Station - Javelin (CROWS-J) Engineering Change Proposal (ECP)
Aegis Advanced Capability Build 16 (ACB 16) Baseline 9.2.2 Integrated Test C3B3 Data Collection Plan (DCP)
Aerosol Vapor Chemical Agent Detector (AVCAD) Chemical Biological Radiological Contamination Survivability Detailed Test Plan
Approval of the MQ-8C Surface Warfare Increment/Radar Follow-on Operational Test and Evaluation Test Plan COMOPTEVFOR 3980 (1593-OT-D1) Ser 00/022, dated 1 April 2021
Armored Multipurpose Vehicle (AMPV) Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan
Army Contract Writing System (ACWS) Cooperative Vulnerability and Penetration Assessment (CVPA) Plan Approval
Ballistic Missile Defense Systems (BMDS) Integrated Master Test Plan (IMTP), v22.1
CH-53K Initial Operational Test and Evaluation (IOT&E) test plan for approval
CMV-22B Adversarial Assessment (AA) and Cooperative Vulnerability and Penetration Assessment (CVPA) test plan
Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan (TP) for the AN/TPQ-53 Counter Fire Target Acquisition Radar System
Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan (TP) for Joint Biological Tactical Detection System (JBTDS)
Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan (TP) for the Command Post Computing Environment Increment 1
Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan (TP) for the Electronic Warfare Planning and Management Tool (EWPMT)
Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan (TP) for the CH-47F Cargo Helicopter (Block II)
Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan (TP) for the Stryker Common Remotely Operated Weapon Station - Javelin (CROWS-J) Engineering Change Proposal (ECP)

Table 5. DOT&E Test Plans Approved
Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan (TP) for the Javelin G-Model (Spiral 3) Missile and Lightweight Command Launch Unit
Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan (TP) for the Integrated Visual Augmentation System (IVAS)
Cooperative Vulnerability and Penetration Assessment (CVPS) Test Plan (TP) for the Integrated Personnel and Pay System - Army (IPPS-A) Release 3
Cooperative Vulnerability Penetration Assessment (CVPA) Test Plan (TP) for the Close Terrain Shaping Obstacle (CTSO), XM204 Top Attack (TA) System
Cooperative Vulnerability Penetration Assessment (CVPA) Test Plan for the Army Integrated Air and Missile Defense (IAMD) System
Detailed Test Plan for the Live Agent Aerosol Test Developmental Test/Operational Test (DT/OT) of the Joint Biological Tactical Detection System (JBTDS) U.S. Army Test and Evaluation Command Project Number 2021-DT-DPG-JBTDS-H8471
Detailed Test Plan for the Operational Assessment of the Stryker Common Remotely Operated Weapon Station - Javelin (CROWS-J) Engineering Change Proposal)ECP), U.S. Army Test and Evaluation Command Project No. 2019-DT-ATC-CRWSJ-H0708
Distributed Common Ground System - Navy (DCGS-N) Cybersecurity Test Plan
Dry Combat Submersible (DCS) Cyber Survivability Test Plan
Dry Combat Submersible (DCS) Initial Operational Test and Evaluation (IOT&E) Test Plan
Evolved Sea Sparrow Missile (ESSM) Block 2 Initial Operational Test and Evaluation Phase 1 Test Plan
F/A-18E/F Software Configuration Set (SCS) H16 Test Plan Approval
F-22 Integrated Maintenance Information System Test Cooperative Vulnerability and Penetration Assessment Test Plan
KC-46A: Cybersecurity Test Plan AA-1
LHA (R) Verification of Correction of Deficiency (VCD) Test Plan Approval
Operational Test Plan (OTP) for the 120-mm XM1147 Advanced Multipurpose Advanced Multipurpose (AMP IOT) 2021-OT-MTD-AMPOO-H7534
Operational Test Plan (OTP) for the Dismounted Assured Positioning, Navigation, and Timing System Operational Assessment (DAPS OA) 2021-CF-IEW-CDAPS-H3500
Operational Test Plan (OTP) for the Electronic Warfare Planning and Management Tool Initial Operational Test Operational Test (EWPMT IOT) 2021-OT-IEW-EWPMT-H2421
Operational Test Plan (OTP) for the Infantry Squad Vehicle Initial Operational Test (ISV IOT) 2021-OT-MTD-ISV01-H4559
Operational Test Plan (OTP) for the Infantry Squad Vehicle Limited User (ISV LUT) U.S. Army Test and Evaluation Command (ATEC)
Operational Test Plan (OTP) for the Initial Maneuver Short Range Air Defense System Operational Assessment (IM-SHORAD OA) 2020-DO-AMD-SHORAH2152 and Adversarial Assessment (AA) Test Plan (TP)
Operational Test Plan (OTP) for the Integrated Personnel and Pay System-Army (IPPS-A) Increment II Release 3.0 Limited User Test 3
Operational Test Plan (OTP) for the Joint Biological Tactical Detection System Operational Assessment (JBTDS OA) 2021-OE-MSS-JBTDS-H4054
Operational Test Plan (OTP) for the Joint Light Tactical Vehicle Fires Developmental Test/Operational Test (JLTV DT/OT) 2021-DO-MSS-JLTVX-H4218
Operational Test Plan (OTP) for the Mounted Assured Positioning, Navigation, and Timing (PNT) System Limited User Test
Operational Test Plan (OTP) Official Submission for Mobile Protected Firepower (MPF) Limited User Test (LUT)
Operational Test Plan for THAAD Software Version 4.0 Cybersecurity Assessment
Operational Test Plan for the Command Post Computing Environment Increment 1
Operational Test Plan Lead Radio/Manpack Radio Initial Operational Test
Public Key Infrastructure (PKI) Increment 2 FOT&E Plan Approval
Surface Electronic Warfare Improvement Program (SEWIP) Block 2 FOT&E test plan
Test Plan for the Developmental Test/Operational Test (DT/OT) of the Joint Biological Tactical Detection System (JBTDS)

Table 5. DOT&E Test Plans Approved
Tomahawk OT-D-12 Cybersecurity Test Plan
Unmanned Influence Sweep System (UISS) Cyber Survivability Test Plan
Unmanned Influence Sweep System (UISS) Test Plan (Test begins 30 November)
US Operational Test Team F-35 Modernization Block 4 Suitability Test Plan and Data Management and Analysis Plan Approval
USS ***Gerald R. Ford*** Shock Trial Plan Approval
Warp Core Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan

Acting Director Dr. Raymond O’Toole SASC Statement for the Record

STATEMENT

BY

RAYMOND D. O'TOOLE, JR.

ACTING DIRECTOR, OPERATIONAL TEST AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

READINESS SUBCOMMITTEE

APRIL 28, 2021

Raymond D. O'Toole, Jr.

Acting Director, Operational Test and Evaluation (DOT&E)

Office of the Secretary of Defense

Chairman Kaine, Ranking Member Sullivan, and distinguished Members of the Committee –

Thank you for this opportunity to discuss the performance of Department of Defense (DOD) acquisition programs and acquisition reform. This is my first appearance before this Committee and it is an honor to be here to testify with Ms. Stacy Cummings, who is performing the duties of the Undersecretary of Defense for Acquisition and Sustainment, and Ms. Shelby Oakley from the Government Accountability Office.

DOT&E's Role and Perspective

As specified in Title 10 of the U.S. Code, DOT&E provides independent oversight of operational and live fire test and evaluation of DOD acquisition programs. Test and evaluation (T&E) is critical to the acquisition process: It assesses a system's operational performance and identifies system issues, offering program leads the opportunity to correct them before the final acquisition or fielding decision is made.

DOT&E is tracking 234 acquisition programs across the Department, which does not account for highly classified programs. Among the competing priorities of program cost, schedule, and performance, DOT&E is focused on delivering an authoritative assessment of system performance in combat. To do this, we ensure that the test is conducted in operationally realistic and representative conditions with trained operators, in

a mission-ready system configuration, and with representative threats; and that the test is comprehensive enough to capture the factors that may affect credible assessment of operational effectiveness, suitability, survivability, and/or lethality in theater. Our findings inform acquisition decisions and help our military forces understand good and bad aspects of their system's performance so that they can plan and execute their mission within that context. For programs under DOT&E oversight, we provide our assessment of the results of operational testing to the Secretary of Defense and Congress, in accordance with Title 10.

Attributes and Practices That Promote Program Success

Every acquisition program is unique but some key attributes can help influence whether a program succeeds, including technical complexity and maturity, resource availability, contract strategy, and the skills of the government and contractor personnel associated with the program. Based on DOT&E's evaluations of a wide range of DOD programs, I offer three insights on how acquisition program managers can achieve better outcomes and provide timely delivery of the required capability. Program managers should understand: (1) the value of T&E, which is critical to determining mission performance; (2) the value of integrating developmental and operational T&E, which enables earlier discovery of problems; and (3) the value of credible modeling and simulation (M&S) to augment and enhance, and in some cases replace, traditional "live" testing. I will illustrate these insights with a few examples from acquisition programs that have either embraced these principles or set them aside.

Understanding the Value of T&E

A good program must start with a realistic baseline of cost, schedule, and performance to ensure enough margin to adapt as the program evolves. In this balancing act, operationally realistic T&E is essential to understand the performance of the unit equipped with that system. T&E is the only way to demonstrate system performance, to include mission effectiveness, suitability, survivability, and lethality, prior to fielding. When conducted early in a program's development and when adequately resourced across the acquisition cycle, operationally realistic T&E offers a unique opportunity for the program office to not only identify but also solve problems before the system matures. Early problem discovery may allow the program to better manage cost and schedule later in the process, when retrofits and problem solutions become more complex, expensive, and time-consuming to implement. Most importantly "fixing" problems early in the T&E process mitigates the risk of discoveries in operational test, the field, or, worse, combat.

The Amphibious Combat Vehicle program serves as a good example of prudent planning and the benefits of early, operationally realistic testing. The program office understood that T&E would identify problems, provided the resources required to solve those problems, and was well-positioned to respond to problems discovered in early, developmental and limited user tests that supported a successful Milestone C acquisition decision. Early understanding and correction of deficiencies led to improved operational performance, demonstrated in a successful Initial Operational Test and Evaluation, which supported an informed full-rate production decision.

On the other hand, the KC-46A aerial refueling tanker program was years late in delivering test aircraft to the Air Force due to several reasons, including inadequate schedule margin for early identification of deficiencies through T&E, followed by failure to rapidly develop and demonstrate deficiency solutions. Fortunately, the KC-46A program has improved. Last year, the vendor shifted from a position of "what's good enough" to "what's the best we can do", spurring development of a new remote visual system design critical for unrestricted air refueling. So far, it appears that the new subsystem – which is based on significant research and excellent technologies – will contribute to the tanker's eventually fulfilling its primary mission.

As cybersecurity threats become more ubiquitous and sophisticated, DOD's acquisition and T&E communities need to address cybersecurity more comprehensively. Unfortunately, some programs do not properly plan for cybersecurity assessments. More critically, due to poor system hardening against dynamic cyber threats, driven by lack of workforce cyber capacity, talent and tools within the program offices, virtually none of the programs assessed in FY20 were survivable against relevant cyber threats.

A good example of recognizing the importance of cybersecurity is the Ground-Based Strategic Deterrent (GBSD) program, which is the replacement for the Minuteman III Intercontinental Ballistic Missile program. To ensure an effective cyber defense for GBSD, the program manager is funding an integrated Mission Defense Team to provide overall security for the program, including cybersecurity, physical security, and nuclear safety. The program manager started building this team in parallel with early development of the rest of the program. This early cybersecurity capability, coupled with early cybersecurity testing, increases the likelihood that cyber defenses will be ready to protect the GBSD program when it is deployed, although future GBSD cybersecurity testing will demonstrate the effectiveness and any potential shortfalls of this approach.

Understanding the Value of Integrated Test and Evaluation

Integrated test and evaluation (IT&E) begins with collaborative developmental, live fire and operational test planning and execution during early phases of the acquisition program. Involving operational testers and the intended system users in the earliest stages of program development and test planning helps to set the conditions for a successful operational test, to discover mission-relevant problems early, and to reduce the cost of fixing problems. When adequately planned and resourced, integrated T&E can increase T&E efficiency by eliminating unnecessary test redundancies, and enable leveraging of data and lessons learned across the acquisition cycle.

The AIM-120D Advanced Medium-Range Air-to-Air Missile program has directly benefited from early developmental and operational test integration. The test teams ensured AIM-120D test shots were relevant and useful for both developmental and operational test, shortening test timelines and mitigating the possibility of transferring undiscovered operational utility risk to the user. Despite initial delays due to technical challenges, the AIM-120D team has established an efficient and collaborative test battle rhythm that has generated significant improvements, accelerating the fielding of better capabilities to the warfighter.

While integrated testing continues to produce T&E efficiencies, it currently represents only a small portion of overall T&E activities within DOD. Moreover, much of the success of integrated testing is attributed to individual programs' establishment of integrated test teams. DOT&E has been working with USD(R&E) to advance the integrated T&E concepts, policy, and guidance needed to further leverage the potential benefits; additional changes may be necessary to fully support integrated T&E implementation. For example, effective integrated T&E requires mission-relevant, testable requirements that can be assessed in the context of mission outcomes throughout the acquisition cycle, rather than just technical specification requirements. Integrated T&E also requires sharing T&E-relevant data across the acquisition cycle; to do so, DOD must improve data collection processes, instrumentation, access to contractor data, and data storage approaches. While current collection and storage practices do not routinely facilitate such sharing of data, to include advanced data analysis and analytics, many programs achieve this in a more ad hoc fashion.

The Armored Multi-Purpose Vehicle (AMPV) program exemplifies the value of data sharing, even in its current manual instantiation. Data sharing between the test teams and the program office has been exceptional AMPV's testers understood the performance requirements and their rationale early, which allowed them to scope the test early; as a result, the final contract included test assets necessary to support all phases of testing. The exchange of data during operational tests also enabled the program to understand the

significance of the problems identified by the Army Operational Test Center and DOT&E in earlier operational T&E, which they were then more inclined to fix.

Understanding the Value of Credible Modeling and Simulation

Modeling and simulation (M&S) is necessary for development, integration, and mission-level evaluation due to the complexity of the systems DOD is acquiring, the increasing importance and difficulty of representing complex operating environments, and the growing sophistication of our adversaries' weapon systems. To have confidence in M&S-based evaluations, we must ensure that each M&S environment is supported by an independent and agile verification, validation, and accreditation (VV&A) process that uses credible and relevant data for accreditation.

The Tomahawk Weapon System (TWS) program recognized the value of adequately validated M&S and developed an M&S representation of the shipboard TWS computer and communication architecture. The program office committed to recurring validation of this M&S capability with live flight data, allowing M&S to be used to evaluate operational performance with high confidence. This resulted in the reduction of flight time and associated resource expenditures, which translated to significant cost savings compared to a test program that would have employed only live testing.

In some cases, independently accredited M&S provides critical supplemental data to evaluate a system's performance. For example, safety limitations preclude testing manned Navy surface ships' self-defense capability against some anti-ship cruise missiles. An adequate test campaign to evaluate various combat, radar, and weapon systems against these threats requires live test data, a capable unmanned asset to support this live testing, and accredited M&S. The Navy currently does not have a well-defined strategy or funding to provide any of these three capabilities, creating an unacceptable risk in our ability to evaluate the operational effectiveness and survivability of future ships in combat.

Adaptive Acquisition Framework

The Adaptive Acquisition Framework consists of six Acquisition Pathways recently developed by USD(A&S) for use by DOD program managers. DOT&E, in coordination with USD(R&E), is developing the T&E guidance for the Adaptive Acquisition Framework to enable the T&E community to support the six Acquisition Pathways effectively without compromising the ability to characterize effectiveness, suitability, survivability, and lethality of our weapon systems.

My assessment of the effectiveness of the Adaptive Acquisition Framework is based on Middle Tier of Acquisition (MTA) and Software Acquisition Pathway programs. The MTA Pathway has been widely adopted by program managers and DOT&E currently oversees 28 MTA programs. Per the explanatory statement accompanying the FY21 appropriations act, USD(A&S) and the Service acquisition executives have approved certain acquisition programs to use "prototyping or accelerated acquisition authorities." In accordance with the same legislation, DOT&E is assessing the available test strategies for these programs for appropriateness and risk to test execution.

The Services use the MTA Pathway for a wide range of systems and warfighting capabilities. In some cases, the MTA programs modestly upgrade an existing system. In other cases, MTA programs, such as the Future Long-Range Assault Aircraft and the ORCA (Extra Large Unmanned Undersea Vehicle/XLUUV), provide advanced new capabilities via emerging technologies. Approximately 75 percent of MTA programs are used for rapid prototyping while others are used for rapid fielding.

The agile acquisition approach utilized by some MTA programs exacerbates some existing acquisition challenges. For example, MTA test strategies frequently lack well-defined resources to plan and execute

operational testing, or to train operators, maintainers, and cyber defenders. Some lack the rigor typically required to demonstrate operational effectiveness, suitability, survivability, and lethality. Certain MTA programs have wisely incorporated integrated test approaches with rapid test-fix-test cycles but doing so has begun to stress the Service operational test agencies and developmental test organizations, to include relevant oversight organizations, which currently are not resourced, staffed, or trained for the continuous level of effort and reporting required by such approaches.

While DOT&E fully supports the MTA concept of faster acquisition and fielding in order to get capability to warfighters more quickly, MTA programs still need to be positioned to assess and demonstrate operational performance – what the system can and cannot do, and whether employment and unit tactics, techniques, and procedures can remediate system shortcomings. An adequate operational demonstration, or an otherwise tailored operational test, must be executed to provide an opportunity to "fly before you buy" – with the operational user behind the proverbial wheel – before the initial production or fielding decision is made in order to mitigate risk to the user. Any increase in tolerance for performance risk in pursuit of acquiring emerging technologies must be characterized, if not quantified, in the context of the actual capability delivered to warfighters and their ability to win and survive wars.

Test and Evaluation Authorities, Responsibilities, and Capabilities

It is important that the same rigorous oversight DOT&E provides be applied to the earlier developmental T&E phases of a program. Certain acquisition programs have a strong DOT&E presence, with DOT&E providing oversight for 234 acknowledged programs. In contrast, USD(A&S) is the Milestone Decision Authority for 11 programs, providing oversight across the entire acquisition cycle. USD(R&E) provides Developmental Test, Evaluation and Assessment oversight of 11 programs, in accordance with previous Deputy Secretary of Defense guidance. Because initial operational testing represents a fraction of the overarching T&E program, and tends to occur at the end of a system's development cycle, there is an opportunity for A&S and R&E to provide more and earlier T&E oversight. This is especially true if we expect to take full advantage of adaptive acquisition, integrated testing, and early deficiency discovery and remediation, all of which can lead to faster and less costly development of more effective and survivable systems.

Program offices, in an effort to balance cost, schedule, and performance, are sometimes drawn to truncating developmental test efforts to maintain schedule or cost objectives. Developmental testing may be cut short, or problems that developmental testing uncovers may be left unaddressed in order to keep the program moving forward. This recently occurred in the Bradley A4 Engineering Change Proposal program. Developmental testing had discovered indications that the system was overcharging turret batteries but the Army did not identify this as a fault or safety hazard and did not address it. Later in the program, operational testing identified a significant safety issue; the system overcharged the turret batteries and released hazardous toxic fumes into the crew compartments. Improved oversight of developmental testing likely would have prevented this problem from persisting until soldiers were exposed to a safety hazard during operational testing.

As discussed above, acquisition outcomes could be improved if the T&E community were positioned to more effectively leverage the benefits of integrated T&E. To support that, contracts should be negotiated to require operationally relevant, mission-level goals during developmental test, rather than focusing only on technical specification compliance. In addition, as the use of integrated T&E expands, it would be helpful to codify in the law, and otherwise enable inclusion of, operational test representatives in decisions regarding execution of developmental and integrated test events. On several occasions, DOT&E had intended to obtain data via integrated T&E or simply to use developmental test data, only to see the test event canceled without input from the operational test community.

The T&E community plays a large role in assuring test adequacy and shepherding programs to operational test success and, ultimately, fielding. As a result, the T&E community needs to be equipped with state-of-the art tools and capabilities to meet emerging needs and the needs of the future. Earlier this year, DOT&E laid out a Science and Technology Strategy to provide a basic framework to guide T&E modernization and to keep up with changing weapon system capabilities – both ours and that of our adversaries. The strategy comprises five focus areas.

The first focus area is software and cybersecurity T&E. We are finding cyber issues and vulnerabilities in nearly every program we oversee. Given the volume and complexity of cybersecurity and software testing, it is clear that people-centric T&E approaches are not sufficient. Instead, the T&E community needs automated solutions for both testing and continuous monitoring of system cybersecurity and software. This needs to be fortified by a workforce trained and equipped to combat cybersecurity threats.

The second focus area is next-generation T&E capabilities. The quality of T&E – and ultimately warfighting capability – depends on the quality of T&E tools, infrastructure, and processes. DOD's T&E enterprise must be able to adequately assess emerging capabilities and threats, such as systems using artificial intelligence, space-based systems, and directed-energy and hypersonics programs – and must mirror real-world environments and scenarios. DOT&E recently commissioned the National Academies of Sciences, Engineering and Medicine (NASEM) to assess DOD's T&E capabilities and capacity, and to provide actionable recommendations to shape the Department's investment strategy over the next five to 10 years.

The third focus area is more widely instituting the integrated T&E lifecycle. DOD can make T&E more effective, and likely more efficient, by mitigating the adverse effects of traditional contractor, developmental, and operational test silos. The segregated, serial approach should be replaced with a process that integrates all test phases -from contractor testing to developmental testing to operational testing - within a mission construct. This will require advanced tools and methods for designing test events that collect data that satisfy both developmental and operational needs across the acquisition cycle. As part of the integrated T&E lifecycle, we also must institutionalize inclusion of the intended users and testers in development of system specifications and contract requirements to ensure that they are operationally relevant and testable.

The fourth focus area is digital transformation. T&E must respond to industry's and adversaries' adoption of digital technologies and capabilities. T&E needs automated, even AI-enabled, data collection and analysis tools. We also must build easily shared – yet cybersecure – data repositories for better data analysis and analytics. In addition, more programs should incorporate credible digital twinning in their design and testing efforts. We need to prioritize the development of sophisticated modeling environments that undergo constant refresh and continuous agile verification, validation, and accreditation, as well.

The final focus area is workforce expertise and partnerships. T&E of complex technologies requires cutting-edge expertise. The ability to attract more talent to government service and to obtain consistent, on-demand access to experts from academia and industry is key. Equally important are more structured, rigorous, and continuous training programs to help the acquisition and T&E workforce meet future needs.

I appreciate the invitation to be here today and I would welcome the opportunity to meet in person or virtually with any member of the committee or your staff to talk further about the value of operational testing to the DOD acquisition process.

Acting Director Dr. Raymond O'Toole HASC Statement for the Record

STATEMENT

BY

RAYMOND D. O'TOOLE, JR.

ACTING DIRECTOR, OPERATIONAL TEST AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

TACTICAL AIR AND LAND FORCES SUBCOMMITTEE

JULY 13, 2021

ON

FISCAL YEAR 2022 BUDGET REQUEST OF THE DEPARTMENT OF DEFENSE FOR FIXED-WING TACTICAL AND TRAINING AIRCRAFT PROGRAMS

Raymond D. O'Toole, Jr.

Acting Director, Operational Test and Evaluation (DOT&E)

Office of the Secretary of Defense

Chairman Norcross, Ranking Member Hartzler and distinguished Members of the Committee, I appreciate the opportunity to provide an update regarding ongoing F-35 operational test and evaluation activities and relevant test and evaluation infrastructure and resource challenges. As requested, I will also provide an overview of my role, participation, and actions during formulation of the fiscal year (FY) 2022 President's Budget.

The Department of Defense conducts operational test and evaluation in order to determine a system's operational effectiveness, including lethality, operational suitability, and survivability. The objective is to inform warfighters and decision-makers of a system's capabilities and limitations prior to its use in the field. DOT&E provides independent, unbiased oversight of operational test and evaluation to ensure that it is adequate and realistic, and that credible conclusions are drawn from OT&E data.

F-35 Initial Operational Test and Evaluation (IOT&E)

Testing Completed To Date

The F-35 is nearing the end of a multi-year initial operational test and evaluation (IOT&E) program. To date, the test team has completed: cold-weather trials; actual weapons employment, which included bombs and missiles; cybersecurity testing of air vehicle components and the Autonomic Logistics Information System (ALIS); deployments to ships and austere environments; and testing that compared F-35 performance to that of fourth-generation fighters against traditional and more contemporary threats currently used by our adversaries. Open-air test missions evaluated the roles of offensive and defensive counter-air, including: cruise missile defense; suppression/destruction of enemy air defenses (S/DEAD); offensive counter air; reconnaissance; electronic attack; close air support; forward air control-airborne; strike control and armed reconnaissance; combat search and rescue; anti-surface warfare; and air-to-surface attack, in higher-threat environments, in two-, four- and eight-aircraft missions. During the S/DEAD trials, the F-35 faced robust, realistic surface-to-air threats represented by Radar Signal Emulators (RSEs).

The only remaining element of the IOT&E program is 64 trials in the Joint Simulation Environment at Naval Air Station Patuxent River, Maryland. These trials will include all three variants.

The Joint Simulation Environment (JSE)

As I noted earlier, the purpose of OT&E is to determine operational effectiveness, suitability and survivability. The JSE is essential to assessing these factors for the F-35 because there are no other means, other than actual combat against peer adversaries, to test it against the dense, modern, surface and air threats we expect it to face. For a variety of reasons, open-air testing is not feasible for this mission set and these operational scenarios, which are fundamental to achieving a credible, comprehensive, accurate evaluation of the F-35.

Constructing the F-35 JSE has proven to be a significant challenge. The JSE team is making steady progress in developing this complex simulation venue, and I am heartened by the independent technical assessment, completed by Johns Hopkins Applied Physics Laboratory, the Carnegie Mellon University Software Engineering Institute and the Georgia Tech Research Institute in May 2021. This independent report concluded that the JSE is feasible as envisioned. The keys to bringing the JSE to fruition are sufficient financial and human resources and strong support from all stakeholders. From the DOT&E perspective, it is essential that the JSE undergo a rigorous verification, validation and accreditation process that, among other elements, utilizes data collected during open-air flight testing. We must be able to trust that JSE results are truly representative.

Effectiveness

As IOT&E is ongoing, DOT&E has no formal information to share at this time. However, I would be happy to meet with members of the committee and your staff, in an appropriate venue, to discuss our classified preliminary observations.

Suitability

In calendar year 2020, several key suitability metrics continued to show signs of slow improvement. Yet, operational suitability of the F-35 fleet remains below Joint Strike Fighter Operational Requirements Document (ORD) thresholds in some areas. Maintenance data gathered through February 2021 from the U.S. fleet of all three variants show that the F-35A is not meeting, and the F-35B and F-35C are not projected to meet, the full set of ORD reliability and maintainability requirements for mature aircraft. The F-35A has accumulated the flight hours designated for maturity (75,000 hours) and therefore DOT&E assessed it against the full ORD requirement. However, the F-35B and F-35C have not yet reached their thresholds (75,000 and 50,000 hours, respectively) and thus were assessed against interim goals.

Fleet availability also continues to fall short of program goals. Data gathered through the end of May 2021 show that the 12-month fleet average availability is below the program goal. DOT&E found that mission capability rates for the U.S. fleet fell just short of the target value, while full-mission-capable rates were short of the target.

Survivability

The program has collected all live-fire and electronic attack survivability data needed to complete IOT&E. Other aspects of survivability will be assessed through the JSE trials.

As with all platforms, cybersecurity is a critical factor in F-35 survivability. The JSF Operational Test Team and other supporting test teams have conducted several cybersecurity test events on the Autonomic Logistics Information System (ALIS), F-35 training systems, integration and reprogramming labs, and actual air vehicle components. Cyber test teams conducted enterprise-wide testing on the latest release of ALIS available at the time, version 3.5.0, in July and October 2020; the final cyber tests of air vehicle components were completed in April 2020. The results show that some vulnerabilities identified during earlier testing periods have not yet been adequately mitigated.

F-35 IOT&E Report

IOT&E findings will be summarized in the beyond low-rate initial production (BLRIP) report, which DOT&E will deliver after testing in the JSE is completed. The report will include the F-35A and A-10C comparative evaluation results, which detail F-35A capabilities in close air support, combat search and rescue, and forward air controller-airborne missions. As I already noted, IOT&E results are classified; DOT&E would be happy to discuss our final conclusions with you in the right venue when the BLRIP report is finished.

Other Topics

F-35 Block 4

The current F-35 Block 4 development process, referred to as Continuous Capability Development and Delivery, or C2D2, is not delivering capability as scheduled. The Joint Program Office intended for C2D2 to field a new software increment, known as a "minimum viable product" (MVP), every six months. To date, the process has not worked well. The first version of each increment has frequently been deficient. As a result, each increment has required more extensive developmental flight testing and multiple subsequent iterations to fix deficiencies. This, in turn, has reduced the time available to conduct adequate operational testing. Additionally, software changes intended to introduce new capabilities or fix deficiencies instead introduced stability problems that adversely affected certain existing F-35 functionality.

DOT&E has concluded that the six-month C2D2 cycle is not sound. Each MVP increment comprises mission planning software, mission data, ALIS, joint technical data, flight series data, training simulators, and other support capabilities. While individual components are tested, a final MVP configuration receives minimal, if any, testing as a complete package prior to fielding. As a result, significant problems are being discovered during OT events, which often are not in sync with the six-month C2D2 cycle, and in the field. To ensure platform effectiveness and pilot safety, DOT&E believes dedicated OT of each final MVP package is necessary prior to installation on the F-35.

To improve the quality and timeliness of software development, in November 2020, the Assistant Undersecretary of Defense for Acquisition and the Director of Defense Research and Engineering jointly chartered a Systems Engineering Tiger Team (SETT) focused on generating corrective action recommendations to manage F-35 program risk, schedule, cost, progress, and outcome expectations. DOT&E contributed to this effort, with a rigorous, technical evaluation of the status of current laboratories and modeling and simulation (M&S)

capabilities required for the C2D2 effort. In parallel, F-35 program executive leadership requested an independent software review, which recommended steps for improving the overall software quality and delivery timeliness. DOT&E expects these initiatives will provide a more stable software product for operational test and evaluation and fully supports them.

Remaining F-35 deficiencies and modeling and simulation (M&S) plans also are a concern. Initial Block 4 development focused on addressing deficiencies that the F-35 program has carried since before the System Development and Demonstration (SDD) phase was completed in April 2018. The Block 4 plan calls for remedying deficiencies while simultaneously developing new capabilities. The overall number of open deficiencies -- more than 800, to include eight Category I deficiencies -- has not changed significantly since SDD because testing continues to discover new issues. The program intends to depend more heavily on M&S in Block 4, compared to the SDD phase. Unless the program establishes rigorous internal processes, provides funding, and drives contractual performance to support development and enhancement of required M&S capabilities, this reliance on M&S likely will negatively impact efforts to resolve the deficiency backlog.

DOT&E remains concerned about the availability of the test infrastructure and resources required to execute the approved Block 4 test and evaluation programs, as well. The Services and F-35 JPO OT representatives have developed a tail-by-tail accounting of current and future OT aircraft, and identified the necessary modifications to OT aircraft and the required instrumentation. Additional work and funding are required to address these and other test-enabling and infrastructure requirements, such as the U.S. Reprogramming Lab for mission data, data sharing networks and storage systems for the test teams, and JSE upgrades. Currently, these requirements are not fully funded, programmed, or scheduled to be completed in time to support Block 4's DT, integrated DT/OT, and dedicated OT activities.

Adequate Block 4 operational testing will also require mission-level evaluations, which will rely on Open Air Battle Shaping (OABS) instrumentation, threat radar emulators, and updates to the JSE. As proven during F-35 IOT&E, the OABS capability is essential to assess accurately complex mission trials. Updated threat radar emulators that match modern air defense radars are necessary to evaluate warfighting capability. While the Department has provided some funding to acquire new emulators, more resources are needed to upgrade current emulators, procure additional new radars, continue funding OABS systems, and expand JSE for each Block 4 capability release. All of these capabilities also will be required to test a range of other emerging DOD programs and to train our warfighters.

DOT&E expects F-35 sustainment and modernization to be a challenge. The F-35 fleet will comprise multiple hardware and software configurations, all of which will require continuous updates and continuous testing to ensure operational effectiveness, suitability and survivability. The department's already stressed T&E infrastructure and personnel will be strained even further. Already, development and testing of the currently fielded hardware and software system-of-systems that comprise ALIS have been hampered by software immaturity and inadequate test infrastructure. This type of problem could become more common without sufficient T&E capacity and capability investments. The transition to Operational Data Integrated Network (ODIN) is not expected to address this concern as initially ALIS software is to be used on ODIN.

Next-Generation T&E Capabilities

Our tactical air warfighting capability largely depends on the quality of the T&E tools, infrastructure, and processes used to identify and mitigate any performance shortfalls prior to employment in combat. DOD's T&E enterprise must be able to assess adequately emerging capabilities and replicate threats, such as artificial intelligence-enabled systems, advanced sensors and shooters, space-based systems, and directed-energy and hypersonic weapons – all of which contribute to the complex, dynamic multi-domain operational picture on which commanders and warfighters rely. Improvements to both the live and synthetic domains that support operational T&E and training are therefore imperative for mission success and national security. We must

modernize our ranges to enable operationally relevant testing of fourth-, fifth-, and, eventually, sixth-generation platforms in operationally representative environments. This may include expanding the Navy's Fallon Range Training Complex, and other facilities, to support both test and training requirements. It certainly will require greater investment in T&E instrumentation, data storage and analysis tools, threat replication, and human expertise. In 2020, DOT&E commissioned the National Academies of Sciences to assess the adequacy of ranges, infrastructure, and tools to accommodate future technologies anticipated to arrive between now and 2035. When those reports are ready, DOT&E will share them with Congress and the Secretary of Defense to help inform investment decisions.

Fiscal Year 2022 Budget Request

In accordance with the FY21 Defense Appropriations Act, DOT&E worked with the Deputy Secretary of Defense and the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer (OUSD(C)) to budget appropriately for greater oversight of programs using Section 804 acquisition authorities or rapid prototyping authorities. As you know, the FY22 budget request included $12 Million for DOT&E's Section 804 oversight activities. The department intends to review the resources necessary to support this congressional oversight mandate when it builds the FY23 budget and Future Years Defense Program. DOT&E will continue to work with all DOD stakeholders to fund this effort appropriately in the future, in accordance with H.R. 133-119.

DOT&E participated in the review of the FY22 President Budget's led by the Office of the Director of Cost Assessment and Program Evaluation (CAPE) and OUSD(C). The process re-evaluated existing decisions with a focus on a very small number of issues, none of which directly affected the responsibilities of this office.

Moving forward, it is important that the Department continue to emphasize the critical role of test and evaluation in delivering warfighting capability. Operational and live-fire test and evaluation assess a system's operational capability and identify performance issues, offering programs the opportunity to correct them before the final acquisition or fielding decision is made. The Department needs to continue to enable adequate T&E, which requires additional resources to modernize T&E ranges, laboratories, virtual and M&S environments, tools, infrastructure, and methods. In coordination with the Office of the Under Secretary of Defense for Research and Engineering, DOT&E has identified several T&E infrastructure gaps that warrant the Department's attention. Notable shortfalls exist in the areas of space; electromagnetic spectrum; hypersonic, nuclear and directed-energy weapons and threats/targets; modeling and simulation; autonomous and artificial intelligence-enabled systems; and digital modernization. Some of these gaps have been partially addressed in the FY22 budget request but many shortcomings remain. Also, we must ensure that programs have the right amount of resources and time to prioritize and execute robust T&E, then apply and test all necessary fixes prior to deployment.

Unfortunately, unlike our adversaries, who continue to make strong investments in their T&E infrastructure, in some instances we are moving in the opposite direction. For example, smaller dedicated test squadrons would introduce risk to adequate evaluation of weapon systems in operationally relevant environments; that, in turn, poses risk to the warfighter and DOD's mission success. DOT&E urges the Committee to continue to emphasize the value of T&E and allocation of the resources necessary to deliver combat-credible weapons at the speed of relevance.

Again, I appreciate the invitation to be here today. I would welcome the opportunity to meet in person or virtually with any member of the committee or your staff to talk further about the F-35 and next-generation tactical air test and evaluation requirements and challenges.

Service Secretary Comments

SECRETARY OF THE ARMY
WASHINGTON
JAN 18 2022

MEMORANDUM FOR Director, Operational Test and Evaluation, 1700 Defense Pentagon, Washington, DC 20301-1700

SUBJECT: Army Response to Fiscal Year 2021 Director, Operational Test and Evaluation Annual Report

1. Thank you for the opportunity to include the Army's comments in the Director, Operational Test and Evaluation (DOT&E) Fiscal Year 2021 Annual Report. This is the Department of the Army response.

2. I appreciate the thoroughness of the DOT&E report as well as the coordination between DOT&E and the Army. There has been significant progress in addressing many of the system level issues contained in the report. Additionally, the Army provides the below insights from the Service-level.

a. The Army is actively modernizing to ensure we continue to provide a threat-informed most capable Army to the Joint Force. Correspondingly, the Army remains focused on ensuring that effective capabilities are employed to test and evaluate emerging technologies. The Army's Test and Evaluation (T&E) community has already initiated actions to provide our workforce with more advanced skills, modernize test capabilities, and invest in future capabilities to address many of the technologies identified in this report.

b. The Army acknowledges the importance of the oversight role of the Office of the Secretary of Defense activities; however, the Army believes the management and execution of test capabilities to address new technology challenges is best retained at the Service level thereby appropriately aligning authority responsibility, and resources. For emerging capabilities such as Artificial Intelligence/Machine Learning and Robotics, we look forward to DOT&E level policy to enable Service level execution of T&E.

c. The Army is very pleased with the Department's recognition of the T&E challenges for Chemical and Biological Defense (CBD). The Army would like to emphasize that adequate and predictable funding continues to remain an additional challenge for CBD T&E modernization.

SUBJECT: Army Response to Fiscal Year 2021 Director, Operational Test and Evaluation Annual Report

4. We look forward to working with your office on implementing the recommendations at the Service level to ensure we continue to provide effective capabilities to our Soldiers in support of the Joint Force. Thank you for your continued support of Army programs and our Soldiers.

5. My point of contact for this action is Ms. Laura Pegher, 571-256-9438 or laura.i.pegher.civ@army.mil.

Christine E. Wormuth

Christine E. Wormuth

2

DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

24 JAN 2022

MEMORANDUM FOR DIRECTOR, OPERATIONAL TEST AND EVALUATION

SUBJECT: Department of the Navy Comments on the Fiscal Year 2021 DOT&E Annual Report

Pursuant to your e-mail dated December 14, 2021 requesting Department of the Navy comments on the FY2021 DOT&E Annual Report, the following is provided:

- Littoral Combat Ship (LCS): The report notes low reliability and availability due to propulsion issues. The Navy is addressing LCS Freedom variant propulsion issues through Combining Gear (CG) redesign, installation and performance verification. After the successful performance verification of the CG, LCS 21 was accepted and delivered to the Navy in November. LCS Independence variant propulsion reliability is being addressed by Strike Team systems engineering and logistics efforts. Improvements to maintenance, and design have been implemented resulting in increased availability on recent deployers.

- CVN 78 Gerald R. Ford Class Nuclear Aircraft Carrier: The report notes poor or unknown reliability of systems critical for flight operations. The Navy has implemented improvements that have steadily increased operational availability through the Post Delivery Test and Trials period. Operational availability increases include the Electromagnetic Aircraft Launch System from 82% to 90%, the Advanced Arresting Gear from 76% to 87%, and the Dual Band Radar from 95% to 96%. As of December 2021, all 11 Advanced Weapons Elevators were turned over to the Navy. The report also states that CVN 78 Full Ship Shock Trial (FSST) results identified several design shortfalls not previously discovered by modeling and simulation or component-level testing. The results of FSST are under review and will be published in 2022. To date, no design shortfalls have been identified.

- F-35 Joint Strike Fighter: The report discusses the status of Block 4 mission systems software. The program continues to update the Continuous Capability Development and Delivery (C2D2) process to improve software development and software quality. In 2021, C2D2 delivered multiple weapons capabilities including ASRAAM B6, AIM-9X-3, CATM-154C-1 and the external gun pod carriage. The program fielded 7 significant software releases comprising 15 of the 39 Block 4 capabilities for the TR-2 hardware suite, including Auto Ground Collision Avoidance System, advanced Electronic Warfare expendables, GBU-54/38 Laser Joint Direct Attack Munition, and United Kingdom's SPEAR Capability 1.

I appreciate DOT&E's coordination with the individual program offices. Over the years, the Navy has voiced concern about the classification of the DOT&E Annual Report. DOT&E's development of two reports with different and appropriate levels of releasability based on program security classification guides should reduce the risk of disclosure of critical unclassified

information to our adversaries from official sources. Thank you for this opportunity to comment on the Fiscal Year 2021 DOT&E Annual Report.

Meredith Berger
Assistant Secretary of the Navy
(Energy, Installations and Environment)
Performing the Duties of the
Under Secretary of the Navy

Copy to:
ASN (RD&A)
PCD/PMD ASN (RD&A)
DASN (RDT&E)

SECRETARY OF THE AIR FORCE
WASHINGTON

MEMORANDUM FOR THE DIRECTOR, OPERATIONAL TEST AND EVALUATION

SUBJECT: Department of the Air Force Response to Fiscal Year (FY) 2021 Director, Operational Test and Evaluation (DOT&E) Annual Report

I appreciate the opportunity to review the FY21 report. Holistically, this report reflects an accurate status of oversight programs in the Department of the Air Force (DAF) and identifies the challenges and opportunities of resourcing the Department of Defense test enterprise. The DAF has also provided clarifications and amplifying information for your consideration in the final report.

It is important to note the status of test and evaluation (T&E) resources not mentioned in the report including the ongoing DAF and Under Secretary of Defense (Research and Engineering) Test Resource Management Center (TRMC) investments in T&E infrastructure that support the hypersonic and nuclear modernization efforts. While not addressing all shortfalls cited in the report, these funds are providing continuous improvement to the T&E infrastructure within current program and budget priorities. For example, AF/TE in coordination with TRMC has begun addressing long range corridor shortfalls and hypersonic wind tunnel issues cited in the report. In addition, the DAF is addressing the range instrumentation needs for hypersonic testing via the OSD-funded SkyRange program. These efforts, in various program phases, are on track to address shortfalls by FY26.

The DAF looks forward to continuing the partnership with DOT&E required to meet the test needs of Airmen and Guardians now and in the future.

KENDALL.FRANK.III.1009574375

Frank Kendall

cc:
AF/CV
AF/TE

Index of Programs

7.62mm Advanced Armor Piercing (ADVAP), M1158 69
120mm Advanced Multi-Purpose (AMP), XM1147 67
Abrams M1A2 System Enhancement Package version 3 (SEPv3) Tank with Trophy Active Protection System (APS) 71
Advanced Anti-Radiation Guided Missile - Extended Range (AARGM-ER) 129
Aegis Modernization Program 131
Aerosol and Vapor Chemical Agent Detector (AVCAD) 37
AGM-183A Air-Launched Rapid Response Weapon 191
AIM-9X Air-to-Air Missile Upgrade Block II 134
AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM) 194
Air Operations Center–Weapon System (AOC-WS) 196
AN/TPQ-53 Counterfire Target Acquisition Radar 73
Armored Multi-Purpose Vehicle (AMPV) 75
Army Integrated Air & Missile Defense (AIAMD) 77
Assured–Positioning, Navigation, and Timing (A–PNT) 79
B-52H Commercial Engine Replacement Program (CERP) 198
B-52 Radar Modernization Program (RMP) 200
Bradley Family of Vehicles (BFoV) Engineering Change Proposal (ECP) 82
CH-53K King Stallion 136
CMV-22B Joint Services Advanced Vertical Lift Aircraft – Osprey – Carrier Onboard Delivery 138
Command Post Computing Environment (CPCE) 84
Conventional Prompt Strike 140
CVN 78 ***Gerald R. Ford***-Class Nuclear Aircraft Carrier 142
Dark Eagle 87
DDG 1000 – ***Zumwalt***-Class Destroyer 146
Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives 39
DOD Healthcare Management System Modernization (DHMSM®) 43
Electronic Warfare Planning and Management Tool (EWPMT) 90
Evolved Sea Sparrow Missile Block 2 148
Extended Range Cannon Artillery (ERCA) 91
F-15 Eagle Integrated Infrared Search and Track 205
F-15 Eagle Passive Active Warning and Survivability System (EPAWSS) 202
F-16 Radar Modernization Program 207
F-22A – Raptor Advanced Tactical Fighter Aircraft 209
F-35 Joint Strike Fighter (JSF) 45
F/A-18E/F Super Hornet 152
F/A-18 Infrared Search and Track Block II 150
Family of Advanced Beyond Line-of-Sight Terminals (FAB-T) 211
FFG 62 ***Constellation*** Class – Guided Missile Frigate 155
Global Positioning System (GPS) Enterprise 212
Handheld Manpack and Small-Form Fit (HMS) Programs – Leader Radio and Manpack 93
HH-60W Jolly Green II 216
Infantry Squad Vehicle (ISV) 95

Integrated Tactical Network (ITN) . . . 98
Integrated Visual Augmentation System (IVAS) . . . 100
Joint Air-to-Ground Missile (JAGM) . . . 102
Joint Assault Bridge (JAB) . . . 104
Joint Biological Tactical Detection System . . . 54
Joint Cyber Warfighting Architecture (JCWA) . . . 218
Joint Light Tactical Vehicle (JLTV) Utility (UTL) and Fire Direction Center (FDC) . . . 106
Joint Regional Security Stack (JRSS) . . . 57
KC-46A Pegasus . . . 220
Key Management Infrastructure (KMI) . . . 60
LHA 6 Flight 1 (LHA 8) Amphibious Assault Ship . . . 157
Littoral Combat Ship (LCS) . . . 159
Long Range Fires . . . 109
M917A3 Heavy Dump Truck (HDT) . . . 111
Maneuver-Short Range Air Defense (M-SHORAD) Increment 1 . . . 113
Massive Ordnance Penetrator Modification . . . 223
MH-139A Grey Wolf . . . 225
Missile Defense System . . . 233
Mk 48 Torpedo Modifications . . . 162
Mk 54 Lightweight Torpedo Upgrades Including the High Altitude Anti-Submarine Warfare Weapon Capability (HAAWC) . . . 164
Mobile Protected Firepower . . . 115
MQ-4C Triton . . . 167
MQ-8 Fire Scout Unmanned Aircraft System (UAS) . . . 169
Multi-Function Electronic Warfare – Air Large . . . 117
Next Generation Jammer Mid-Band(NGJ-MB) . . . 171
Offensive Anti-Surface Warfare (OASuW) Increment 1 . . . 174
Over-The-Horizon Weapons System (OTH-WS) . . . 176
Presidential and National Voice Conferencing (PNVC) Integrator . . . 227
Public Key Infrastructure (PKI) Increment 2 . . . 62
RQ-7Bv2 Block III SHADOW – Tactical Unmanned Aircraft System . . . 119
Ship Self-Defense System (SSDS) Mk 2 Integrated Combat Systems . . . 178
Small Diameter Bomb Increment II . . . 228
Soldier Protection System (SPS) . . . 122
Stryker Family of Vehicles (FoV) . . . 125
Surface Electronic Warfare Improvement Program (SEWIP) Block 2 . . . 181
Tactical Tomahawk Modernization . . . 183
Unmanned Influence Sweep System (UISS) Including Unmanned Surface Vessel (USV) and Unmanned Surface Sweep System (US3) . . . 185
VH-92A® Presidential Helicopter Replacement Program . . . 187
Wide Area Surveillance . . . 230

1 Director's Foreword
5 Introduction
11 Table of Contents
17 Mission
19 Executive Summary
29 Test and Evaluation Resources
35 DOD Programs
65 Army Programs
127 Navy Programs
189 Air Force Programs
233 Missile Defense
241 Cyber Assessment Program (CAP)
251 Center for Countermeasures (CCM)
255 International Test and Evaluation Program (ITEP)
261 Joint Aircraft Survivability Program (JASP)
267 Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME)
275 Joint Test & Evaluation Program (JT&E)
281 Test and Evaluation Threat Resource Activity (TETRA)
287 Oversight List
293 DOT&E Activities
299 SASC Statement for the Record
307 HASC Statement for the Record
313 Service Secretary Comments
321 Index of Programs