FY 2024 Annual Report

Director, Operational Test & Evaluation

January 2025

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.

Dr. Raymond D. O'Toole, Jr.
Director (Acting)

Director's Introduction

U.S. military Service members deserve to be equipped with combat-credible systems that meet the demands of today's evolving threats and tomorrow's unpredictable challenges. In a rapidly changing global security environment, where adversaries continue to develop sophisticated capabilities across all domains, our commitment to providing timely, rigorous, and independent evaluations has never been more critical. The U.S. military operates in an era of accelerating technological advancements, increasingly complex operational environments, and evolving global challenges. The DoD must rapidly and rigorously test and evaluate its systems to determine if they are not only operationally effective and suitable, but also survivable and lethal across contested domains.

To achieve these goals, DOT&E advanced our Strategy and Implementation Plan (I-Plan) this year. This plan lays out a clear path to make a strategic shift in test and evaluation (T&E) processes and builds on years of effort. These efforts started under Honorable Robert Behler, when he looked at the science and technology (S&T) of T&E and released the S&T Plan in January 2021. That work was codified under Honorable Nickolas Guertin in June 2022 with five strategic pillars and championed by Honorable Douglas Schmidt during his first six months tenure, after he was sworn in as Director, Operational Test and Evaluation on April 8, 2024. The I-Plan capitalizes on the latest advances in S&T to modernize our professional skillsets, enable our agility and efficiency, and inspire trust and confidence in system performance under wartime conditions. The plan's five pillars represent DOT&E's commitment to testing in ways that reflect operational realities, adapting to new technologies, and ensuring that our warfighters are equipped with the best possible capabilities.

CODIFYING STRATEGY IN POLICY AND GUIDANCE

This rapid pace of change from a technological, operational, and global geopolitical scale, demands that we must embrace a strategic shift in how we conduct T&E. Toward that end, in December 2024 Honorable Douglas Schmidt signed out a new policy for operational test and evaluation (OT&E) and live fire test and evaluation

(LFT&E). This policy – a DoD instruction accompanied by five corresponding DoD manuals – will drive the DoD forward by making strategic shifts in how we execute the T&E mission. I am honored to have played a role in implementing this culmination of a multi-year effort to update policy and guidance. These documents encourage early engagement from OT&E and LFT&E stakeholders and engagement in OT&E and LFT&E activities across the acquisition life cycle. The policy calls for:

- Using the latest advances in science and technology to both plan tests and evaluate outcomes,
- Requiring the integration of all relevant information into OT&E and LFT&E planning and assessment activities,
- Mandating the consideration of risk as part of the test planning process,
- Requiring that OT&E and LFT&E planning start in parallel with the initiation of the program,
- Considering the time and resources required to correct deficiencies identified in test, and,
- Ensuring T&E against the full domain of kinetic and non-kinetic threats to address the rapidly evolving threat landscape.

This policy and the corresponding manuals encourage us to lean forward in a measured way. We need to research, pilot, and inform how our future T&E practices leverage digital transformation, digital engineering models, and data collected from across the acquisition life cycle. The intricacies of software and artificial intelligence (AI) models make these practices imperative because the complexity they impose cannot be adequately tested in dedicated operational tests alone.

The I-Plan's goals, key challenges, and how the policy advances the current state of T&E is spelled out in each of the five pillars presented below.

Pillar 1 – Test the Way We Fight

Realistic operational conditions are the cornerstone of defensible T&E. Test conditions that systems are exposed to in operational tests routinely reveal new vulnerabilities and failure modes that should be remediated to avoid failure in combat. To reflect the evolving battlefield, there is a critical need for modeling and simulation (M&S) to undergo verification, validation, and accreditation (VV&A) with live data.

Pillar 1 focuses on developing T&E frameworks that reflect joint and coalition operations, particularly in highly contested and congested environments, such as cyber and electromagnetic spectrum (EMS) realms. DOT&E's new policy and guidance emphasizes the importance of using all credible sources of information to inform OT&E and LFT&E plans and assessments.

To improve our ability to test in operationally realistic environments, we are leveraging training and exercises for data. Retrieving data from theater assessments to support the continual VV&A of complex M&S is crucial to this effort's success. Early engagement by operational testers will ensure that program requirements incorporate testability considerations, so systems are instrumented to provide this critical data. Another challenge is testing in commercial cloud environments to ensure our cyber capabilities are robust enough to withstand attacks while adapting to new operational and economic realities.

In early 2024, I signed out the long anticipated F-35 Initial Operational Test and Evaluation (IOT&E) report as we concluded a multi-year test program. I shared the results with DoD leaders and Congressional defense committee members, informing the full-rate production decision for this $2 trillion program. The development of the Joint Simulation Environment (JSE) enabled adequate testing of the F-35. JSE enabled realistic scenarios with high-density threats that could not be completed in open air. Its development was critical to an adequate OT&E for the F-35 program and was championed by DOT&E. It now provides a great asset to the T&E enterprise for future F-35 and other aircraft testing.

This year I signed a memorandum of understanding (MOU) with Japan, allowing T&E projects between the two countries. This achievement and our ongoing efforts with the F-35 program illustrate how we are “testing the way we fight.” We will continue to champion testing of systems as they will be deployed in conflict through partnerships, advocacy, and other investments.

Pillar 2 – Accelerate the Delivery of Weapons That Work

In an era of rapid development, our ability to identify issues early in the life cycle of systems is crucial. Our new policy encourages shifting mission realism left and conducting OT&E and LFT&E activities throughout an acquisition program’s life cycle. By pushing more test activities into earlier phases of system development, we reduce the likelihood of discovering problems late in the process, when fixes are more expensive and time-consuming.

Digital models are a key element of shifting left, but they must be coupled with live data collection to validate and update models to reflect operational realities. We are progressively shifting towards automated test tools for operational data collection and the investment in more agile processes aimed at reducing the T&E timeline while maintaining high standards of performance.

DOT&E worked with the maritime autonomous system community, and other communities utilizing emerging technologies, to identify test infrastructure requirements and develop test methods this year that will accelerate evaluation and contribute to operator confidence when applying these technologies in modern warfare.

Pillar 3 - Improve the Survivability of the DoD in a Contested Environment

Systems today must operate seamlessly in increasingly contested domains, including cyber, the EMS, and space. Building and testing systems that are resilient to these threats while also integrating them into larger networks and federated systems is hard. A key element of our new policy is testing for full-spectrum survivability and lethality, which is an integral part of the modern battlefield.

In future conflicts, the DoD and our partners and allies will face significant threats in cyber and congestion in the EMS. The advantage in these conflicts will accrue to whichever side can fix and improve their software most rapidly and reliably. The ability to rapidly reprogram, recode, and minimize total system downtime and integration downtime will be key, and must be tested intentionally and explicitly to ensure the survivability of DoD systems *and* kill webs. As we work through the implementation of the new policy, we will undoubtably uncover additional needs for digital models and live, virtual, constructive range infrastructures.

This year, DOT&E completed operational testing of the Mounted/Dismounted Assured Positioning, Navigation, and Timing Systems (MAPS/DAPS), which are among the Army’s first programs designed to provide assured position navigation and timing to tactical units in a contested and congested electronic warfare environment. DOT&E also began oversight of programs that provide both military and intelligence capabilities, to help ensure these programs are operationally effective, suitable, and survivable in the hands of military personnel under representative combat conditions.

Pillar 4 – Pioneer T&E of Weapon Systems Built to Change Over Time

We no longer have the luxury of developing static, one-time-use systems. Many of our new capabilities, particularly those involving AI and software, will evolve over time. Testing for these systems requires a shift in mindset – we must embrace testing across the acquisition life cycle, even into operations and sustainment. We have to accelerate using adaptable test processes and methods that reflect prior knowledge. As a result, DOT&E is pioneering new testing methods for systems that will be updated and modified continuously throughout their life cycle.

Even when every process is followed correctly, the complexity of systems can lead to significant delays. However, by aligning our testing strategies with the evolving nature of these technologies, we can reduce the risk and ensure that these capabilities reach the warfighter when they are needed.

To support the new OT&E and LFT&E policy, Honorable Douglas Schmidt signed out the first ever DoD manual on testing AI-enabled and autonomous systems, which provides an initial starting point for the DoD to develop best practices for testing AI.

Pillar 5 – Foster an Agile and Enduring T&E Workforce

Our workforce is the backbone of the T&E enterprise. However, we are seeing increasing difficulties in recruiting and retaining the talent we need. As DoD systems become more complex, our workforce must be equipped to handle these advancements, from AI-based assessments to cybersecurity.

Many of these positions – especially in software development for operational testing – require highly sought after expertise in the private sector. To compete with companies like Google or Amazon for the best talent, we must find innovative ways to incentivize public service.

DOT&E is proud to partner across the DoD in developing innovative programs to educate and recruit the next generation of the T&E workforce. For example, we partnered with the Office of the Secretary of Defense (OSD) on the Pathfinder Program this year to develop next-generation cyber-T&E talent. We also partnered with the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD[A&S])'s Defense Civilian Training Corps (DCTC), which focuses on developing the next generation of acquisition and T&E experts. DOT&E also continually provides growth opportunities for our current workforce, including implementing Learning Journeys to empower our workforce to develop new areas of expertise.

Another milestone this year that aligns with many of our I-Plan's pillars was the choice by the current Operational Test Agencies' (OTAs') commanders to re-validate their commitment to their six Core Test Principles: Early Operational Test Involvement; Tailor to the Situation; Continuous and Cumulative Feedback; Streamline Processes and Products; Integrated and Combined Collection/Test; and Adaptive. The OTA commanders recently signed a new memo supporting these test principles. DOT&E also continues to support these principles, which were originally captured in 2019.

DOT&E CONTRIBUTIONS TO THE T&E ENTERPRISE

The value of operational and live fire testing goes beyond informing a single decision point. We live in an era where data drives operational decisions through AI and automation. We must carefully consider how our mission needs to evolve to support the DoD at large and of course ultimately the Service members that execute its mission.

Several opportunities exist. By partnering with the acquisition community and developing requirements for testability, DOT&E can improve T&E automation and take advantage of other venues for T&E, like training, large-scale exercises, and even operations. The need for T&E is not shrinking and if anything is growing to handle the complex threat space. Unfortunately, we cannot realistically continue to grow our T&E workforce to scale given various programmatic and pragmatic limitations.

As Honorable Douglas Schmidt said, "as a researcher, I know the potential that AI can have for our T&E processes and practice, including Generative AI (GenAI), which can create certain types of images, text, videos, and other media in response to prompts." DOT&E is closely tracking today's technology transitions and leveraging them to continue improving and scaling our practice of rigorous T&E. We are also exploring how combining GenAI with live data capture can help provide more robust test data sets. Coupled with templates, large language models (LLMs) can also accelerate our analysis and communications.

SUCCEEDING THROUGH TEAMWORK

Ensuring essential operational properties of DoD systems is a team sport since DOT&E by itself can't simply "test our way to success." Moreover, the new policy and initiatives cannot be accomplished by DOT&E alone. We therefore need a holistic life cycle view on how we acquire the best capabilities for the DoD. This vantage point requires us to collapse conventional stovepipes and partner across the DoD to succeed.

WAY AHEAD

As mentioned above, T&E is a team sport. Here are some ways DoD can work together to help to deliver weapons that work, faster:

- We must enhance the cyber resilience of products and information technology infrastructure by maintaining awareness of cyber threats, vulnerabilities, and intelligence; enforcing industry best practices for cyber defense; securing our software development environments; contracting for best security features in the cloud; and understanding and addressing supply chain vulnerabilities and dependencies.
- Initial T&E activities usually start with contractor testing and then transition to developmental testing, and ultimately, to operational testing. However, the more all this testing can be conducted in a representative operational environment, under realistic operational conditions, with as much actual threat information as possible, the more accurate and useful the results will be.
- We must continue to innovate by enabling more effective digital-physical fusion using live, virtual, constructive training environments; digital engineering and digital twins; and uncertainty quantification. These capabilities transform and enhance the value proposition of T&E by shifting the focus from what is required to what delivers the most decisive military advantage.
- Finally, we must hasten the adoption of measures that enable AI and machine learning in weapon performance evaluation, such as expanding data warehouse capabilities; automating data collection and large-scale analytics, processes, and administrative activities; and developing methods and tools that can leverage generative augmented intelligence at scale for T&E.

In an era where time, expertise, and resources are limited, our I-Plan's five pillars and their desired outcomes, coupled with our new policy, offer a solid roadmap for how we will address these challenges. We have already laid the groundwork for the T&E community to innovate and lean forward leveraging new technologies. I am confident this community can work together to develop new and innovative practices that couple new technologies with the rigorous methods and tools we have always leveraged, to ensure DoD systems are adequately tested before fielding. Together, we will ensure that the systems we deliver to our warfighters are tested thoroughly, efficiently, and in ways that reflect the future battlefield.

On January 10, 2025, I became the Director, Operational Test and Evaluation (Acting) for the third time. It is a great honor to serve as the senior advisor to the Secretary of Defense on OT&E and LFT&E of DoD weapon systems. DOT&E is immensely grateful to Congress for their continued support, and for encouraging us to innovate. Our global allies and partners in T&E transformation, and DoD liaison officers deserve our gratitude as well. Thank you to the DOT&E staff and our warfighters for their dedication to working as a formidable team. As a result of all of your efforts through hard work and timeliness dedicated to service, I am confident DOT&E is well-positioned to work successfully with the new administration and the new Secretary of Defense to continue to defend our nation.

Raymond D. O'Toole

Dr. Raymond D. O'Toole, Jr.
Director (Acting)

This page intentionally left blank.

CONTENTS

CONTENTS

The Director, Operational Test and Evaluation (DOT&E) is the 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:

- 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, 4171, and 4231) and then in 1986 (title 10, section 4172). 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 (JT&E) 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. **The 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. **The International T&E Program (ITEP)** – 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.

This page intentionally left blank.

EXECUTIVE SUMMARY

This page intentionally left blank.

MAJOR PRODUCTS

In FY24, DOT&E designated 25 new DoD systems for OT&E and LFT&E oversight and removed 26 systems from the T&E Oversight List. As of September 2024, DOT&E had 265 DoD systems on the T&E Oversight List for OT&E and/or LFT&E, pursuing different acquisition pathways and in different phases of their acquisition life cycles. In FY24, DOT&E:

- Reviewed and approved 24 TESs/TEMPs and disapproved 1 TEMP.
- Approved 65 individual test plans.
- Published 47 reports, including 29 reports to the Services, Congress, and/or the SECDEF providing system evaluations, a classified annual assessment of the Missile Defense System, and 17 special or legislative reports.

DOT&E completed nine legislative actions, summarized in Table 1, for which DOT&E was assigned as the Office of Primary Responsibility (OPR). DOT&E completed seven legislative actions, summarized in Table 2, for which DOT&E was assigned Office of Coordinating Responsibility (OCR).

Table 1. Summary of DOT&E Congressional Activities as OPR

Source	Title	Status
FY23 NDAA		
Sec. 217	Competitively awarded demonstrations and tests of electromagnetic warfare technology	Complete
Sec. 242	Study and report on sufficiency of operational test and evaluation resources supporting certain major defense acquisition programs	Complete
Sec. 1656	Persistent cybersecurity operations for ballistic missile defense systems and networks	Complete
FY23 Other Legislative Actions		
HASC Report	Assessment of contractor-provided test and evaluation capabilities	Complete
HASC Report	Battery testing infrastructure	Complete
HASC Report	Development and testing of body-worn equipment	Complete
HASC Report	Equipment shortfalls within the test and evaluation community	Complete
FY24 Other Legislative Actions		
SAC Bill	Assessment of the DoD’s and Services’ Funding of Test Infrastructure, Assets, and Personnel to Support Agreed-Upon Test and Evaluation of Programs on the DOT&E Oversight List	Complete
SAC Bill	Certification of Appropriateness and Risk Assessment of Services’ Planned Test Strategies for Approved Middle Tier of Acquisition (804) and Accelerated Acquisition Programs	Complete
Acronyms: HASC – House Armed Services Committee; NDAA – National Defense Authorization Act; SAC – Senate Appropriations Committee		

Table 2. Summary of DOT&E Congressional Activities as OCR

Source	Title	Status
FY22 NDAA		
Sec. 833	Pilot Program on Acquisition Practices for Emerging Technologies	Complete
Sec. 1529	Demonstration program for automated security validation tools	Complete
FY22 Other Legislative Actions		
HASC Report	Report on Testing Infrastructure to Support Strategic and Missile Defense Programs	Complete

Table 2. Summary of DOT&E Congressional Activities as OCR, Continued

Source	Title	Status
FY23 NDAA		
Sec. 240	Report of potential for increased utilization of the electronic proving grounds testing range	Complete
Sec. 1514	Operational testing for commercial cybersecurity capabilities	Complete
Sec. 1553	Plan for commercial cloud test and evaluation	Complete
FY24 Other Legislative Actions		
SASC Report	Fiscal Year 2024 Modernization Plan of Hill Air Force Base Little Mountain Test Facility	Complete
Acronyms: HASC – House Armed Services Committee; NDAA – National Defense Authorization Act; SASC – SSenate Armed Services Committee		

In FY24, DOT&E completed the adjudication of all stakeholder comments on the forthcoming DoD Instruction for OT&E and LFT&E and the following DoD Manuals:

- TEMP/TES
- Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A) for OT&E and LFT&E
- OT&E and LFT&E of Software
- OT&E and LFT&E of Artificial Intelligence (AI)-Enabled and Autonomous Systems
- Full-Spectrum Survivability and Lethality T&E

These policies, which DOT&E expects to publish by early FY25, are intended to enhance DOT&E's execution of its OT&E and LFT&E roles and responsibilities through the acquisition lifecycle. They emphasize the importance of using the right type and amount of data, including from validated modeling and simulation, training events, and joint exercises, to evaluate operational effectiveness, suitability, survivability, and lethality. They also consider survivability and lethality holistically across all potential threat and target types – kinetic and non-kinetic.

OT&E AND LFT&E OVERSIGHT OF DOD SYSTEMS

» ENSURED ADEQUATE OT&E AND LFT&E PLANNING AND EXECUTION

TES and Test Plan Recommendation Trends

In FY24, DOT&E evaluated the adequacy of TEMPs, TESs, and test plans to ensure they will provide: (1) data to support credible evaluation of operational effectiveness and suitability, (2) coverage of the operational environment and threats with users executing realistic mission operations, (3) adequate verification and validation (V&V) of M&S, (4) complete assessments of system survivability and lethality against relevant kinetic and non-kinetic threats, (5) production-representative test articles, and (6) sufficient funding and resources required to support test execution.

In FY24, DOT&E approved all but one TEMP. The TEMP disapproval was the result of insufficient resources available to execute the strategy as documented. Common DOT&E conditions for document approval include: (1) testing of the supply chain and inclusion of all potential attack vectors in contested cyberspace, (2) coverage of the operational environment and threats (current and future), (3) M&S V&V plans, (4) use of latest software versions, (5) data collection processes or equipment, (6) use of operationally realistic users and maintainers exercising the most recent tactics, techniques, and procedures, (7) planning for any correction of fixes regression testing, (8) survey administration, and (9) resource sufficiency.

Test Adequacy Recommendation Trends

In FY24, DOT&E assessed the adequacy of OT&E and/or LFT&E in 28 of 29 systems evaluations.[1] DOT&E assessed 64 percent (18 of 28) of testing as adequate, 14 percent (4 of 28) as partially adequate, and 21 percent (6 of 28) as not adequate, as shown in Figure 1. By comparison, over the last 8 years (FY16 – 23), DOT&E assessed 66 percent (167 of 252) of the executed OT&E and LFT&E as adequate, 24 percent (61 of 252) as partially adequate, and 10 percent (24 of 252) as not adequate. The determinations of inadequacy or partial adequacy of OT&E and LFT&E in FY24 were caused by: (1) insufficient scope or lack of operational testing prior to early fielding, (2) early test termination or execution shortfalls, (3) insufficient data to conduct rigorous analysis, and/or (4) lack of testing against all relevant threats, including cyber and electromagnetic spectrum. DOT&E also highlighted limitations discovered in testing or in post-test analysis, including but not limited to:

- Lack of a complete assessment of relevant non-kinetic attack vectors or paths.
- Safety restrictions.
- Software and firmware updates.
- Reliability of an available threat target, simulator, or surrogate.
- Presentation of an operationally realistic environment that replicates the most challenging scenarios and based on current threat information.
- Insufficient amount and quality of data to conduct an adequate evaluation.
- Lack of mission effects data due to being part of a training exercise or day-to-day operations with deprioritized OT&E objectives.

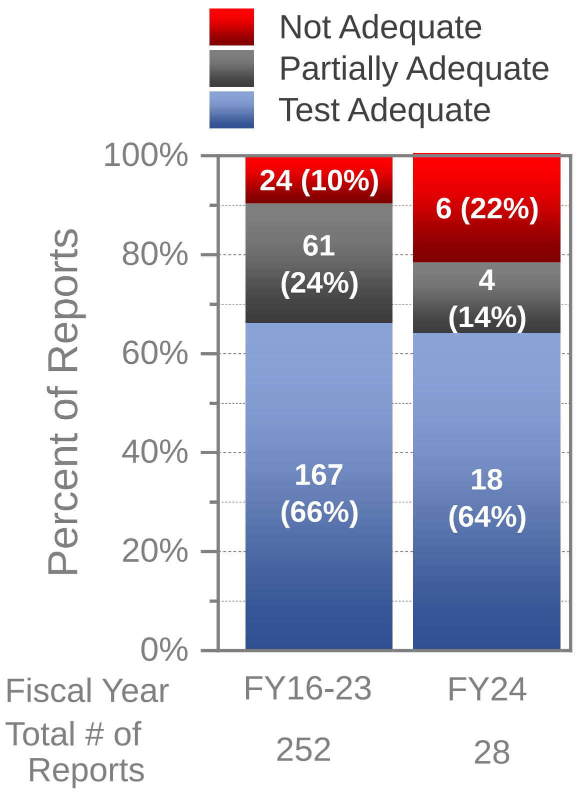


Figure 1. Test Adequacy in FY24 and Prior Years

DOT&E reports also provide recommendations for improving test adequacy. These recommendations include:

- Completing testing with production-representative assets to support early fielding or deployment decisions.
- Conducting operational testing across the relevant missions sets, operating conditions, and threats. Execution of robust testing continues to reveal important shortfalls that can be addressed prior to fielding.
- Testing all relevant cyber-attack paths, including supply chain on all subcomponents, and requiring test teams to execute a complete cyber restore of the system.

1 DOT&E did not make an adequacy determination in the Three-Dimensional Long-Range Radar Operational Assessment Interim Observation Memo.

- Evaluating system suitability and cyber survivability early in the design to increase test efficiency, discover problems early, and improve outcomes in OT&E and LFT&E.
- Developing robust and independent V&V for all M&S for use in OT&E and LFT&E.
- Increased use of telemetry for data collection and understanding interoperability mission effects.

Programs Pursuing the Middle Tier of Acquisition Pathway

In FY24, for the 97 programs approved by the Service Acquisition Executives to pursue the Middle Tier of Acquisition pathway, DOT&E received and reviewed 45 test strategies and certified 37 of those as appropriate, and 8 test strategies as not appropriate. DOT&E did not review the test strategies for the remaining 52 programs because they were either still in development or not made available for review. Test strategies were not certified as appropriate primarily due to inadequate resources for OT&E and/or LFT&E to evaluate the required performance in operationally representative environment, including in contested cyberspace and electromagnetic spectrum environments.

Adequacy of Funding Resources for Programs with Approved TEMPs or TESs

In FY24, DOT&E assessed the adequacy of OT&E and LFT&E resources required to execute the agreed upon OT&E and LFT&E, scheduled in the current year and future years defense planning. This assessment could only be made for those programs on DOT&E oversight that have approved TEMPs or TESs.

- Fifty-three percent (71 of 134) of the eligible programs were assessed to have adequate funding to support the remainder of the planned test execution. Sixteen percent (21 programs) were identified as having funding shortfalls, while 19 percent (26 programs) required updated TEMPs or TESs due to program changes that may require new or altered testing or resource requirements. Eleven percent (15 programs) have fully executed all required testing and require no current or Future Years Defense Program funding. One additional program, Public Key Infrastructure Increment 2, was not assessed despite being eligible for this assessment because funding data was not provided.
- The identified OT&E and LFT&E resource funding shortfalls were primarily related to the following: (1) flight test instrumentation, most commonly, for Open Air Battle Shaping capability, (2) funding for LFT&E events, and (3) accredited threat representation in contested environments, including space.

» PROVIDED INDEPENDENT EVALUATION OF OPERATIONAL PERFORMANCE

In FY24, DOT&E published 29 independent system evaluation reports on the operational performance of the system. System reports where DOT&E was unable to assess operational effectiveness, operational suitability, and/or survivability were based on early fielding and early operational testing, where not enough data are available to make full assessments. In those cases, DOT&E's reports comment on progress towards operational effectiveness, operational suitability, and survivability. The performance trends, discussed below, are depicted in Figure 2.

Operational Effectiveness Trends

In FY24, DOT&E was able to assess operational effectiveness for 13 of 29 systems reports. Of those 13 evaluated programs, DOT&E reported 54 percent (7 of 13) as operationally effective. By comparison, over the last 8 years (FY16 – 23), DOT&E reported 53 percent (82 of 154) as operationally effective. DOT&E assessed two FY24 programs as not operationally effective and four programs as being partially effective because the system could either not complete one or more of its primary missions, the system performed worse than the legacy capability, or had poor operational effectiveness in some operationally relevant conditions against intended threats and targets, including against realistic cyber and electromagnetic spectrum environments.

Operational Suitability Trends

In FY24, DOT&E was able to assess operational suitability for 12 of 29 systems reports. Of those 12 evaluated programs, DOT&E reported 58 percent (7 of 12) as operationally suitable. By comparison, over the last 8 years, DOT&E reported 48 percent (70 of 147) as operationally suitable. DOT&E assessed four programs as not operationally suitable and one program as being partially operationally suitable. These five programs experienced shortfalls in hardware and software reliability and availability. Other common suitability limitations included insufficient training, maintainability, and network connectivity issues.

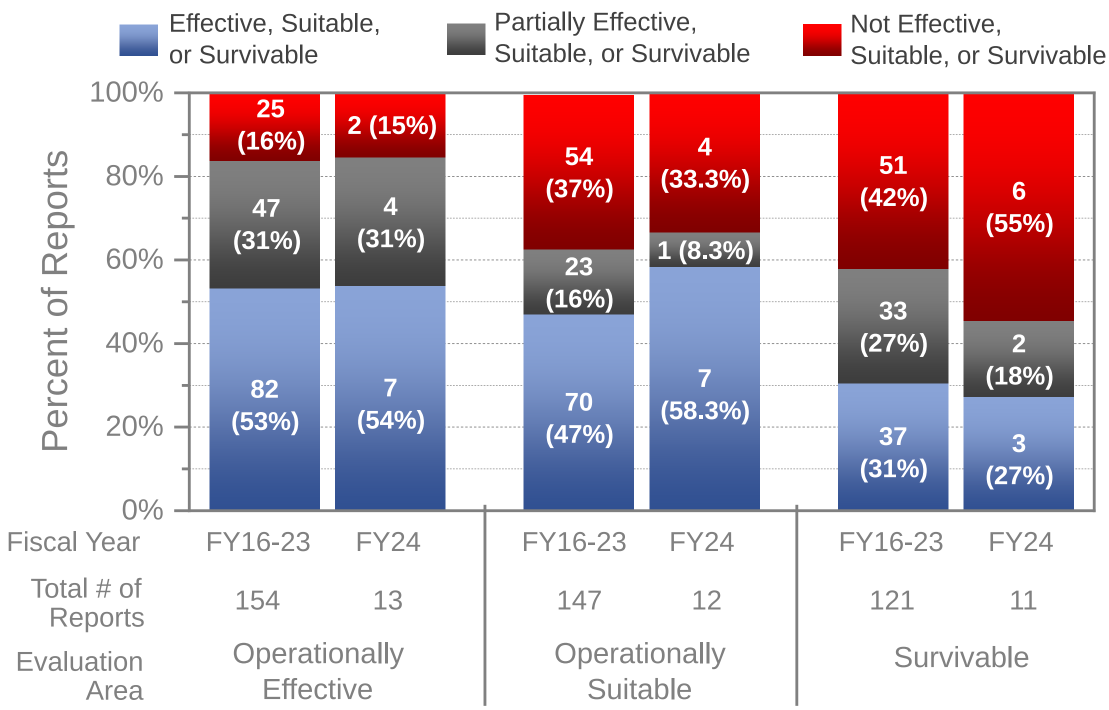


Figure 2. Operational Performance Trends in FY24 and Prior Years

Survivability Trends

In FY24, DOT&E assessed survivability for 11 of 29 systems reports. Of those 11 evaluated programs, DOT&E reported 27 percent (3 of 11) were survivable and 18 percent (2 of 11) were partially survivable. By comparison, over the last 8 years, DOT&E assessed 31 percent (37 of 121) as survivable and 27 percent (33 of 121) as partially survivable, primarily due to vulnerabilities in contested cyberspace. Cyber threats remain the most common threat type tested against in comparison to testing against kinetic; electromagnetic spectrum; or chemical, biological, radiological, and nuclear (CBRN) threats in OT&E and LFT&E.

Recommendations Trends

DOT&E reports include practical recommendations to fix the identified deficiencies and improve the operational performance of the DoD systems in expected operational scenarios and conditions to minimize risk to warfighters and maximize probability of mission success. Examples of common problems discovered in OT&E and LFT&E include immature software, poor reliability, poor network availability and connectivity, not survivable against cyber-attacks, poor system performance in all threat and operational environments, deficient human systems integration, and insufficient training and technical manuals. DOT&E commonly makes recommendations to fix system deficiencies in these problem areas prior to fielding.

» DOT&E ACTIVITIES SUMMARY

In FY24, DOT&E continued to manage the Cyber Assessment Program (CAP) alongside the following field activities: (1) Center for Countermeasures (CCM), (2) Joint Aircraft Survivability Program (JASP), (3) Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) that includes the Joint Live Fire (JLF) program, (4) Joint Test and Evaluation (JT&E), and (5) Test and Evaluation Threat Resources Activity (TETRA). These efforts supported the advancement of DOT&E's Strategy Implementation Plan (I-Plan), published in April 2023, which focused on integrating emerging technologies and adapting our workforce to future challenges. The year marked a shift toward more innovative and forward-thinking testing approaches. Below is a summary of how these field activities have enhanced the DoD's T&E infrastructure, tools, processes, and workforce in FY24. Further details are available in the DOT&E Strategy I-Plan Update, T&E Resources, and DOT&E-Managed Activities sections of this Annual Report.

T&E Infrastructure

DOT&E field activities have improved the DoD's T&E infrastructure by introducing advanced technologies and modernizing facilities. For example, JTCG/ME has implemented cloud-hosted environments that enable real-time analysis of weapon effectiveness data. In partnership with the Test Resource Management Center, they have also provided new infrastructure to support realistic and rapid cyber testing. JLF expanded DoD-wide data repositories to support review, approval, and access of lethality and vulnerability data and documentation. JASP coordinated development of a threat launch simulator for testing two-color infrared missiles warning systems, which will be a vital asset for maturing countermeasure systems. TETRA has delivered high-fidelity electronic warfare (EW) threat models to enhance EW and space system testing. The Integration Lab, launched by JT&E, introduced a digital transformation framework, promoting AI systems and digital twin workflows development.

T&E Tools

This year saw significant enhancements in T&E tools. Key advances included the use of AI and machine learning by groups like JTCG/ME, which created predictive models for fragment penetration and lethality assessments. JTCG/ME also expanded existing lethality and vulnerability data repositories and used modern software methods to enhance weaponeering tool capabilities and interfaces. TETRA is investigating use of an intelligence digital ecosystem to analyze threat intelligence data, supporting more efficient test design and threat modeling across multiple domains, including cyber and space. TETRA is also initiating pilot activities to develop AI-driven EW threat models that simulate complex adversary systems for testing. JASP introduced and validated new tools to enhance aircraft survivability assessments, including capability to simulate multi-domain engagements, EW, cyber threats, surface-to-air missiles, and high-energy lasers. CCM continued to support numerous test events in FY24 by providing threat simulators and other tools to characterize platform survivability.

T&E Processes

FY24 improvements in test processes have been substantial, incorporating modern statistical methods, AI, automation, and real-time analytics. TETRA provided roadmaps to improve test designs for space asset survivability. JTCG/ME developed a workflow management tool to streamline targeting data. JASP partnered with the Navy to improve the efficiency and accuracy of cyber analysis using a digital twin for the P-8A. JT&E introduce introduced an agile test process to expedite T&E of joint warfighter concepts and tactics, techniques, and procedures.

T&E Workforce

DOT&E invested heavily in workforce development, expanding training programs and internships to prepare staff for emerging technological challenges. JTCG/ME's training events have enhanced operational proficiency in new weaponeering technologies. JASP continued to enhance training on aircraft combat damage assessments, focusing on real-time forensics in anti-access/area denial environments. TETRA continues to manage configuration control boards to bring together experts from communities and disciplines to foster a workforce capable of addressing modern multi-domain threats. DOT&E revised its competency model and is working on a course catalog that will map specific trainings to the competencies to provide DOT&E Action Officers (AOs) the resources and guidance they need to increase their skills.

» CONTINUED SUPPORT TO GLOBAL T&E PARTNERSHIPS

The International Test and Evaluation Program (ITEP) has been making significant strides in strengthening international partnerships. In FY24, ITEP signed 16 new agreements, bringing the total number of active agreements to 33. These agreements cover a wide range of testing activities, including EW, tactical armored personnel vehicle testing, data fusion, reciprocal use of facilities, and more. The partners involved are from Australia, Canada, Germany, Italy, Japan, the Netherlands, Norway, and the United Kingdom. These projects aim to improve capabilities and instrumentation among U.S. allies in areas including EW, autonomy, and survivability.

Outside of ITEP, DOT&E increased collaboration with allies and partners in areas such as experimentation, co-development, research, testing, and evaluation. Key strategic partnerships were identified, focusing on the development of AI-enabled systems, synthetic ranges, and the integration of the DOT&E Strategy with the United Kingdom's "T&E Transformation Programme." Short term initiatives aim to enhance verification, validation, and accreditation of AI-enabled systems. A memorandum of understanding was finalized with the United Kingdom, establishing a United Kingdom liaison position within DOT&E to further advance collaboration on these strategic initiatives.

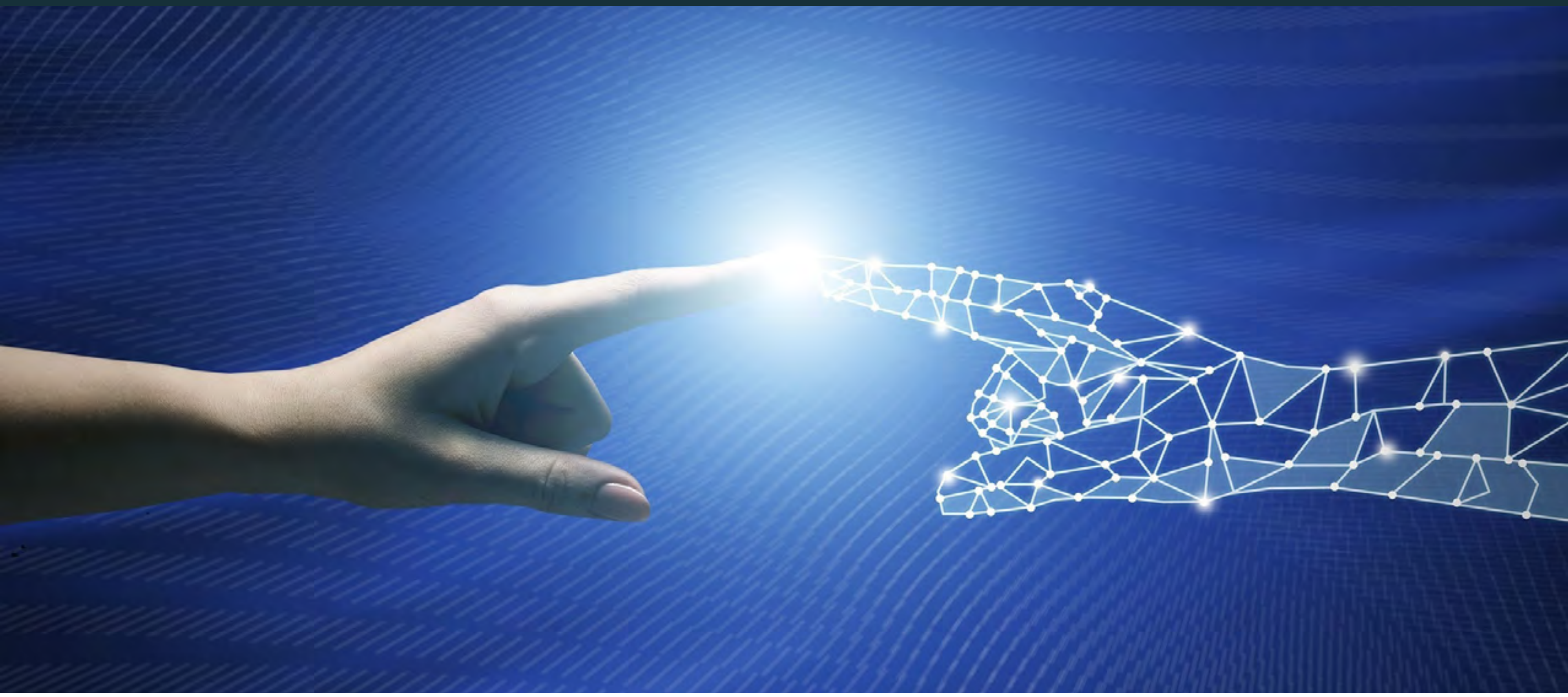
» CONTINUED SUPPORT TO T&E WORKFORCE

DOT&E offered its annual AO Course from September 30 to October 4, 2024. This annual training covers AO duties, their role within the test community, and the basics of DOT&E's legal obligations. This year, the course was offered in a hybrid format and comprised briefings on over 30 topics, to include policy overviews, technical topics, exercises, and panels. Approximately 100 people registered for the course, including staff from DOT&E, DOT&E's FFRDC-support, and other agencies, such as Service operational test agencies and foreign partners. Post-course survey results showed that attendees were satisfied with the course, finding many presentations engaging and informative. Attendees also found the course effective and well-organized. They self-reported an increased knowledge about all DOT&E topics, with a particular increase noted for electromagnetic spectrum operations; chemical, biological, radiological, and nuclear; and AI. Future courses plan to include additional reference materials and examples.

DOT&E STRATEGY IMPLEMENTATION PLAN

This page intentionally left blank.

DOT&E Strategy Implementation Plan (I-Plan)



In April 2023, DOT&E – in coordination with USD(R&E), USD(A&S), and the Military Service Secretaries – published a DOT&E Strategy Implementation Plan (I-Plan) to collaboratively and cooperatively transform the DoD T&E infrastructure, tools, processes, and workforce in response to emerging changes in acquisition, technology, and warfighting. DOT&E's Strategy I-Plan is built on five strategic pillars and twelve lines of efforts summarized below.

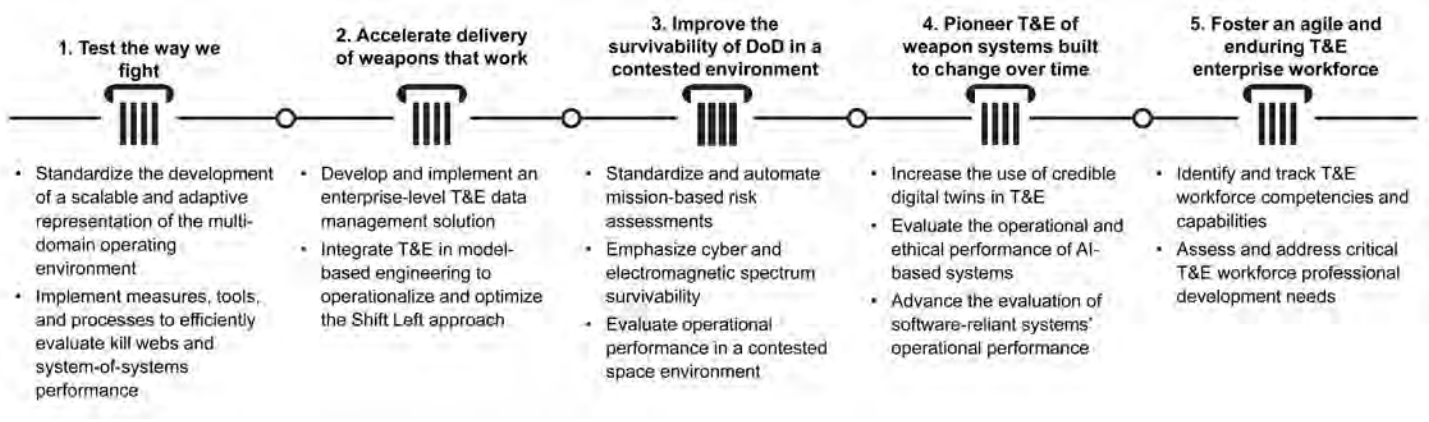


Table 1. DOT&E Strategy I-Plan Desired End States

Pillars	Desired End States
1. Test the way we fight	• Accurate representation of the joint, multi-domain operating environment in test (and training) • Established processes, resources, and capabilities to evaluate joint warfighting capabilities and mission threads
2. Accelerate the delivery of weapons that work	• Near real-time test data analysis and assessments • Discoverable, accessible, and secure T&E data repositories • Established tools and processes to "shift left" and optimize integrated T&E • Digital documentation and tracking of T&E strategies, data, and plans
3. Improve DoD survivability in contested environments	• Minimized mission-critical vulnerabilities and maximized defense in a contested environment • Efficient mission-based risk assessments and full-spectrum survivability T&E
4. Pioneer T&E of weapon systems built to change over time	• Standardized and increased use of credible digital tools in T&E • Adequate assessment of operational and ethical performance of artificial intelligence (AI)-enabled systems • Established processes and capabilities to enable dynamic testing and monitoring of programs throughout operations and sustainment
5. Foster an agile and enduring T&E enterprise workforce	• Highly skilled T&E workforce prepared to meet the toughest challenges • Effective continuous learning program and a robust recruitment/retention plan

As documented in the DOT&E Strategy I-Plan, DOT&E recognizes the critical role of T&E within the wider DoD enterprise including acquisition, requirements, warfighting, and intelligence communities. DOT&E also recognizes the critical role of industry, academia, federally funded research and development centers, university-affiliated research centers, and international partners to help DoD accelerate innovation and support the delivery of the world's most capable warfighting capability at the speed of need. To align this T&E enterprise against common objectives, the DOT&E Strategy I-Plan identifies the desired end state for each of the five pillars, as summarized in Table 1. DOT&E looks forward to continuing collaboration with the T&E enterprise to refine and accomplish the T&E initiatives listed for each of the five strategic pillars.

Pillar 1 – Test the Way We Fight

Pillar 1 is designed to architect T&E around validated joint force mission threads and kill webs (including multiple systems under test) to demonstrate their agility and responsiveness in multi-domain operations and facilitate accurate assessments of operational effectiveness, suitability, survivability, and lethality.

The T&E community can support the measurement of the operational performance of such mission threads and kill webs by establishing:

- An accurate representation of the joint, multi-domain operating environment in test (and training).
- Processes and capabilities to evaluate joint warfighting concepts, capabilities, and mission threads (e.g., kill webs, system-of-systems performance) effectively and efficiently.

DOT&E contributed to the Pillar 1 end state in FY24 as follows:

- Initiated a T&E Capabilities and Requirements Assessment Process that expands on the "range of the future" analysis discussed in the FY23 Annual Report and standardizes how DOT&E identifies, prioritizes, and coordinates mitigation of the OT&E and LFT&E range capability needs across the T&E infrastructure enterprise.
- Advanced the development of a T&E Capabilities and Requirements Dashboard prototype designed to display current capabilities, and to identify, prioritize, and digitally track the status of current

and emerging OT&E and LFT&E range capability, capacity, and availability gaps.

- Collaborated with T&E enterprise stakeholders across the OSD to establish responsibilities to ensure that OT&E and LFT&E are representative of key real-world mission threads.
- Developed a joint test concept roadmap that identifies milestones and goals to implement changes to the T&E of joint operations.
- Delivered electromagnetic spectrum (EMS) passive detection hardware-in-the-loop (HWIL) and software-in-the-loop (SWIL) capabilities to the Naval Air Warfare Center Weapons Division and completed unclassified system integration. The classified system integration is pending authorization to operate.
- Upgraded EMS facilities with a Reconfigurable Signal-Injection Missile Simulation (RSIMS) HWIL simulator for an advanced electro-optical (EO) and infrared (IR) sensors-guided threat and delivered the RSIMS HWIL design for a second advanced EO/IR-guided threat to Naval Surface Warfare Center Crane Division.
- Provided funding to the Naval Surface Warfare Center Dahlgren Division to upgrade their Aerial High-Powered Radio Frequency/Microwave Instrumentation measurement system.
- Acquired the High-Powered Microwave (HPM) Beam Evaluation Tool (HBET) to utilize at Kirtland AFB for HPM testing.

Pillar 2 – Accelerate the Delivery of Weapons that Work

Pillar 2 is designed to accelerate acquisition and T&E by adopting digital technologies and workflows to speed up the delivery of capabilities to the warfighter. The T&E community can implement faster, simple, data-driven T&E methods by:

- Developing, implementing, and enabling an enterprise-level T&E data management and automated analysis solution (e.g., T&E data standards, data stores, knowledge management tools, automated data fusion and analytic tools to expedite data collection, data analysis, and reporting).
- Using advanced statistical methods to support the development and sustainment of a well-structured approach that rigorously codifies how system behavior can be inferred from a collection of evidence (i.e., live data collected on the system as it matures across the acquisition life cycle, and modeling and simulation [M&S] results).
- Leveraging digital engineering and implementing efficient digital representations of T&E strategies and plans that trace back to the technical and operational requirements.

DOT&E contributed to the Pillar 2 end state in FY24 as follows:

- Developed an Integrated Decision Support Key (IDSK) architecture and tools that utilize data to support the acquisition decision-making process for operational testing (OT) and live fire testing (LFT). This includes a tool to capture metadata and a tool to port data from DOT&E-approved TEMPs into the IDSK tool.
- Partnered with several Service T&E representatives, operational test agencies (OTAs), and field activities to support federated data concept developments, such as cloud services and data mesh architectures that will be leveraged by programs to increase the speed of system analysis and evaluation.
- Designed and developed a platform to automate test data analysis that enhances speed, analysis reproducibility, and error reduction; while supporting complex, multi-tiered analysis targeting high-level effects of multi-domain mission threads and kill webs.
- Developed a software application that adapts test designs based on real-time data collected during testing, enabling robust T&E by focusing on system performance, increasing the understanding of system effectiveness and suitability.
- Stood up a DOT&E cloud environment to support development of capabilities that can generate insights into OT/LFT. The environment enables the application of artificial intelligence (AI) and machine learning (ML), data analytics, and data management to meet emergent testing

needs. Within this cloud environment, DOT&E is investigating the secure and reliable applications of large language models and generative AI technologies to accelerate operational effectiveness, suitability, and survivability evaluations.

Pillar 3 – Improve DoD Survivability in Contested Environments

Pillar 3 is designed to enable dynamic assessments and improvements of a system's ability to effectively operate and survive in a hostile full-spectrum threat environment while maintaining mission effectiveness. The T&E community can assist in minimizing mission-critical vulnerabilities and maximizing defenses against full-spectrum threats by:

- Standardizing and automating mission-based risk assessments to optimize the evaluation of kinetic and non-kinetic threats, and their combined effects. These risk assessments include efficient: (1) characterization of system designs, (2) identification and prioritization of vulnerabilities, (3) identification of potential attack conditions, and (4) evaluation of threats effects on the mission.
- Providing automated and integrated processes, tools, and representative threats scenarios with emphasis on cyber and EMS survivability.
- Enabling adequate evaluation of operational performance in a contested space environment by delivering: (1) space environment modeling, system modeling, and analytic tools; (2) space T&E process, policy, and guidance; and (3) space test infrastructure to support subsystems ground-testing or testing space systems and combined effects at scale.

DOT&E contributed to the Pillar 3 end state in FY24 as follows:

- Expanded the development of an M&S framework concept for evaluating vulnerability to both kinetic and non-kinetic threats and launched a limited pilot. This framework combines engineering methodologies and M&S tools to assess a warfighting system's performance and survivability in a contested environment. Ongoing development includes expanded M&S integration, Application Programming Interface (API) coding, and user interface development on both classified and unclassified networks.
- Enhanced the Cyber Operations Lethality and Effectiveness (COLE) Joint Munitions Effectiveness Manual capability for cyber vulnerability and resiliency assessments. COLE now supports models such as Cameo Enterprise Architecture files for interoperability with current model-based systems engineering initiatives and is compatible with the USD(R&E)-directed ontology for attacks in cyber risk assessment frameworks, allowing integration into other M&S frameworks. Additional details on the COLE tool can be found in the Joint Technical Coordinating Group for Munitions Effectiveness article of this Annual Report.
- Established a mission-based risk assessment methodology to evaluate methods for identifying and defending the scope of OT&E and LFT&E required to adequately test a system in both kinetic and non-kinetic contested environments. DOT&E initiated partnerships to develop guidance on the methodology and conduct proof-of-concept pilots.
- Developed a cloud-based digital ecosystem with AI-enhanced tools for identifying and tracking tailored threat intelligence to incorporate into operational testing and inform future T&E investments and threat shortfalls. DOT&E completed a beta capability for unclassified data discovery using ML and retrieval-augmented generation. This capability provides document summarization, context-rich question-and-answer capability, and semantic searching. Future plans include utilizing a robust data collection source, ensuring scalability and adaptability requirements from various data sources, and implementing multi-layer security for handling classified documents.
- Delivered 40 new threat models (hardware and software), 5 new National Air and Space Intelligence Center CHIMERA models and major updates, and 4 new Missile and Space Intelligence Center threat software asset management HWIL

models to various T&E locations (laboratories, facilities, and ranges).

- Conducted a space requirements study to address uplink survivability and anti-jamming concerns, with gap analysis and solutions analysis teams working with Space Force and intelligence communities.

Pillar 4 – Pioneer T&E of Weapon Systems Built to Change Over Time

Pillar 4 is designed to respond to new warfighting capabilities that will be upgraded and changed throughout the life cycle. This includes aircraft mission systems, AI and ML, test automation, and digital engineering. These systems will require new tools and processes to evaluate their performance as they adapt to changing conditions. The T&E community may evolve its processes by:

- Increasing the use of credible digital twins in T&E by: (1) developing a methodology to describe the effective use of T&E digital twins and the associated verification, validation, and accreditation process; and (2) developing and standardizing an architecture for calibrating models based on real, operational data.
- Advancing the research and capabilities including the definition of criteria, methodologies, and metrics for assessing operational and ethical performance of AI-based systems and various aspects of AI and ML technologies.
- Advancing the evaluation of software-reliant systems' operational performance including, but not limited to: (1) software pipelines and factories; (2) software bill of materials monitoring and management to reduce supply chain risk; (3) capability to collect software effectiveness and suitability data from automated testing; and (4) tools and processes to effectively evaluate interoperability and other performance metrics as DoD systems continuously change over time.

DOT&E contributed to the Pillar 4 end state in FY24 as follows:

- Hosted a digital twin workshop and assessed the technological and organizational maturity of model-based systems engineering and digital twins through detailed frameworks and cost-benefit analyses.
- Developed natural language processing-based system to extract vulnerabilities from a software bill of materials and link to known vulnerabilities and exploits to improve Red Team analysis of systems.
- Established the Centralized Capabilities Repository of Software for T&E teams to discover, access, and compare software testing tools. This software provides support in shifting OT&E data collection to left and right to provide continuous insight into software systems' ongoing effectiveness, suitability, and survivability.
- Integrated research into practice using a T&E harness, a collaborative software platform serving as a hub for AI T&E. This research developed use case examples that run through the T&E process, capturing their unique nuances. This approach allows for testing various processes and requirements, aiming to accelerate the transition of cutting-edge research into practical tools for educating and training the T&E community.
- Finalized DoD policy for publication, including policies on T&E for software-intensive systems, software-embedded systems, AI-enabled systems, and autonomous systems to enable continuous and responsible performance evaluation of these capabilities as they change during operational use.
- Hosted the OT&E of Autonomous and AI Systems Trust Workshop to capture DoD OT&E experiences, challenges, and potential solutions while focusing the discussion on warfighter trust and responsible AI OT&E metrics generation and collection.

Pillar 5 – Foster an Agile and Enduring T&E Enterprise Workforce

Pillar 5 is designed to respond to the evolving nature of T&E necessitating a thorough review and refinement of the T&E workforce competencies and the development of continuous learning opportunities for T&E professionals to attract, hire, and retain top talent. The T&E enterprise will better track and manage the T&E workforce's overall readiness in real-time and deliver improved talent management initiatives by sharing DoD’s best practices and establishing and maintaining:

- The appropriate infrastructure to inform the DoD efforts to identify and track the status of required T&E skillsets.
- An effective continuous learning program and robust recruitment and retention plan to prepare the T&E workforce for the emerging challenges.

DOT&E contributed to the Pillar 5 end state in FY24 as follows:

- Launched “learning journeys” that combine classroom, peer, and on-the-job training to enhance action officer (AO) proficiency in key areas. Following a workforce needs analysis, DOT&E updated its competency model to outline the essential knowledge, skills, and abilities required for future success. This competency-based approach enables strategic planning for critical skills and supports targeted training and development.
- Revised, executed, and improved the annual DOT&E AO course, integrating the updated competency model into a refreshed curriculum. The course covered over 40 modules with topics including DOT&E’s mission and role in the acquisition process, TEMP and TES oversight, test planning and execution, T&E of software and AI, and technical writing and reporting. Attendees engaged in use cases, scenario-based exercises, T&E community-wide networking opportunities, and panel discussions, ensuring a steady talent pipeline for future T&E expertise. For the first time this year we had attendees from the United Kingdom and Australia attend the course in an effort to strengthen the partnerships between the three countries.
- Expanded the Pathfinder Internship Program to address the demand for certified cyber and software T&E talent. The 2024 summer internship – a collaboration between DOT&E and the Army’s Program Executive Office for Simulation, Training, and Instrumentation – involved 45 students from over 22 universities. This six-week program combined rigorous technical training with engaging activities, resulting in an increased talent pipeline.
- Initiated a partnership with the Defense Human Resources Activity’s Advanced Distributed Learning team, to leverage the Enterprise Digital Learning Modernization program and establish a dedicated digital learning management system for DOT&E. This system will offer easy access to curated learning resources aligned with DOT&E’s competency needs. By integrating training into DOT&E’s workflow, this approach ensures content is available on-demand, minimizing disruptions and enhancing efficiency.

TEST AND EVALUATION RESOURCES

This page intentionally left blank.

Test and Evaluation Resources

DoD T&E infrastructure must facilitate reliable and thorough performance evaluations of weapon systems in operationally representative environments. However, current deficiencies in T&E resources adversely impact the ability of DOT&E to fulfill its statutory mission. In turn, these deficiencies hinder the Department's ability to perform adequate T&E.

To keep pace with the threat capabilities in the modern multi-domain operational environment, the DoD needs to make significant and steady investments in T&E range modernization, including for threat surrogates and instrumentation. However, range restrictions, security, safety requirements, and cost limit the amount of live testing that is practically achievable. Investments are needed to maintain and update verification, validation, and accreditation (VV&A) of modeling and simulation (M&S) environments to augment live testing.

The T&E workforce is essential to plan and execute the adequate T&E required for performance assessments of DoD systems. DoD should invest in hiring, training, and maintaining sufficient workforce across the Service operational test agencies and other T&E organizations, especially in specialized or emerging technical fields like space, cyberspace operations, software engineering, data analysis, and artificial intelligence (AI). A well-trained and resourced T&E workforce is better equipped to accomplish its mission and adapt to emerging threats and technologies.

RANGE MODERNIZATION

The DoD lacks simulated (e.g., Joint Simulation Environment [JSE]) and open-air multi-domain infrastructure (e.g., numbers and types of target surrogates) necessary to assess weapon systems' performance in realistic combat environments. These combat environments involve collaborative and synchronized command-and-control networks that connect sensors to shooters across domains and networks. Since both U.S. systems under test and adversary systems employ these networked environments, the networks must operate at multiple classification levels. These multi-level classification capabilities introduce additional cost and complexity to the execution of test events. The DoD needs long-range test infrastructure that can be rapidly activated and configured to support complex mission scenarios involving air, land, sea, spectrum, cyber, and space systems.

» OPEN-AIR RANGES

Existing laboratories and range systems do not sufficiently represent current or future threat laydowns and operational scenarios. Test ranges should emulate system capabilities, tactics, and operating space that define the existing and future threats to characterize performance of systems under test. The current open-air range space should be expanded to better support system of system assessments of air, land, and sea combat systems with capability for emerging long-range fires, hypersonic missiles, electromagnetic spectrum (EMS) warfare, and directed energy weapons (DEW). Necessary improvements include connecting U.S. test and training ranges via secure networks; acquisition of high fidelity, rapidly reprogrammable, open-air threat emulation systems; and upgrades to current high-fidelity systems, like the Radar Signal Emulator systems procured by DOT&E in 2014, to provide greater flexibility and fidelity.

The Air Force demonstrated use of Open-Air Battle Shaping (OABS) during recent operational testing. In addition, the Navy has been demonstrating OABS over the past few years during T&E events that span both the test and training communities as well as multi-Service events. OABS includes instrumentation and systems used on open-air ranges, aircraft, and threat systems. OABS provides real-time integration of live aircraft and ground threat systems with modeled weapon performance to provide real-time kill removal to simulate the results of air-to-air, air-to-surface, or surface-to-air engagements in mission-level, force-versus-force, scenarios. Data collected by OABS are critical for VV&A of M&S and essential for the fidelity of JSE.

The Services should improve OABS by adding more entities such as red and blue aircraft, ground threats, and weapons. Additional improvements to monitor data link/network connectivity among players and across multiple test ranges to use modern weapons engagement methods are required. Improved virtual threat insertion, such as missile launch effects and self-protection electromagnetic warfare (EW) techniques add operational realism in a contested environment. Finally, a kill/survive determination methodology to support upcoming operational testing of additional aircraft systems.

In addition, there are shortfalls in the reliable collection of time, space, and position information (TSPI) from participating platforms at open-air ranges. The quality of TSPI collected in tests and in large-force exercises varies from range to range and, in some cases, from platform to platform in any given test event. This shortfall impedes post-test analysis by making it difficult to reconstruct ground truth in aircraft testing.

The open-air test ranges available for operational testing of EMS-dependent systems also lack adequate instrumentation for capturing and reconstructing the many RF signals present in a test. Mobile RF collection instrumentation is required that can be sited with ground-based radar, communications, and jamming systems employed in an open-air test to capture truth data for the signals emitted by these systems. Inadequate instrumentation often precludes both determination of and validation of causes of performance shortfalls in EMS systems under test and validating digital models of EMS systems.

In addition, none of the U.S. test ranges presently have sufficient numbers and variety of RF emitters and surrogate systems capable of replicating peer threat capabilities for radar jammers, GPS jammers, and data link jammers. Surrogates for each of these threat capabilities are essential for T&E of the end-to-end effectiveness of platforms and their weapons. This shortfall limits the ability of the DoD to represent a modern threat environment with realistic signal density and congestion and is common across all EW system assessments.

» LONG RANGE MISSILE TESTING

The DoD requires long-range, overland missile flight test corridors with land-based impact areas to support test flights of missiles with extended ranges. Currently, longer-range oversea flight tests use both broad ocean area and land masses as impact areas. However, neither produce the required lethality data against threat-representative targets at operationally required ranges. The Test Resource Management Center is exploring overland corridors to mitigate this shortfall. The corridors need to increase capacity to support the testing of new hypersonic weapons and use of hypersonic-specific range instrumentation for terminal area and lethality assessments, including mobile data collection assets. OT&E and LFT&E need tools to analyze terminal area scoring data collected during flight tests. These tools support effectiveness decisions on engagement outcomes and are inputs to mission-level simulations that assess lethality of hypersonic missiles and interceptors.

In addition, the Missile Defense Agency (MDA) requires a replacement for the Pacific Tracker and Pacific Collector missile range instrumentation ships that are nearing end-of-life and are essential to provide ground truth telemetry and flight termination functions for flight tests of all MDA programs and other missiles. The MDA will also require shipboard radar upgrades for these assets and is exploring courses of action, but a funding gap remains.

THREAT AND TARGET EMULATION

The T&E community is struggling to characterize system performance against representative threat scenarios and threat surrogates of representative physical size, quantities, and sophistication. The DoD requires substantial resources to keep pace with the rapid development of adversary threats and ensure that Intelligence Community-validated threats are available to the T&E community. Development of more complex target laydowns would enable more realistically stressing conditions for testing the operational capabilities of systems under test and the performance of operational units employing these systems.

» AIR

Piloted Aircraft for Mission-Level OT. In combat versus peer-level adversaries, DoD aircraft can be expected to encounter large numbers of advanced threat fighter aircraft with capabilities comparable to their own. The DoD's aggressor units lack a sufficient number of aircraft, with sufficient electromagnetic systems capabilities, to be able to represent threat fighter aircraft in open-air, mission-level, operational test trials. These threat surrogate aircraft must be equipped with active, electronically scanned array radars that are fully integrated with advanced, digital self-protection radar jammers. Moreover, these aircraft require integrated, air-to-air electro-optical (EO) and infrared (IR) sensors and communications data links, with capabilities comparable to those of advanced threat fighter aircraft, and data recording instrumentation to satisfy T&E analysis requirements.

Airborne Targets for Live Weapons Testing. The availability of threat surrogate full-scale targets for live, air-launched weapons testing is insufficient to assess lethality and validate models for end-to-end effectiveness for missiles. Planned testing may include limited or no full-scale targets due to test asset availability limitations. Surrogate targets are required for fourth- and fifth-generation threat fighter aircraft, large bomber and mobility aircraft, helicopters, and others. These targets should have physical sizes, radar cross sections, and IR signatures comparable to the threat aircraft they need to represent. They should include electronic attack (EA) and radar emitters that replicate the full RF spectrum, power, and angular coverage of these threats.

Air Defense Fixed-Wing Aircraft. The Army lacks organic fighter aircraft to support testing of air defense sensors and systems and relies on agreements with the Navy or Air Force to provide that support. Fixed-wing aircraft are needed to evaluate target tracking, identification, and survivability to electronic attack for air defense sensors and systems. Previously, Air Force fixed-wing aircraft stationed adjacent to White Sands Missile Range provided support along with associated airborne jamming and identification, Friend or Foe. These assets have been relocated and are no longer available. The Army is currently pursuing agreements with Air Force and/or Navy for this support as well as leveraging large test events for Integrated Fires Test Campaigns (including for Guam Defense System) to gain fixed-wing support from the other Services.

Hypersonic threat surrogates. OT&E of hypersonic missile defense will require increasingly sophisticated hypersonic threat surrogates and targets that can represent cross-range and terminal maneuvers. The MDA is developing Aegis Sea-Based Terminal and GPI capabilities to address these types of threats. The Navy's supersonic aerial targets, the GQM-163, cannot fly evasive maneuver flight trajectories representative of supersonic anti-ship cruise missile threats nor can they fly the aggressive diving profiles of some anti-ship cruise missiles. The Navy, similar to the MDA, also requires a hypersonic threat surrogate that is usable in terminal defense scenarios.

The Navy is investigating solutions to address this capability gap. The maximum range of the GQM-163 is not large enough to demonstrate some Navy kill-chain and missile capabilities. These shortfalls limit DOT&E assessments of air and missile defense systems which are intended to defend against such threats, their associated defensive combat systems, and their host platforms that need to survive against such threats. Flight testing against realistic threat surrogates provides data to evaluate hypersonic missile interceptors and to support V&V of high-fidelity and hardware-in-the-loop M&S.

» SEA

Diesel Submarine. Diesel-electric submarines represent important threats that are smaller than U.S. submarines, have different maneuvering and acoustic characteristics, and are capable of resting on the sea floor. To properly evaluate torpedoes and antisubmarine warfare capabilities, the Navy needs a mobile target that can accurately represent a diesel-electric submarine.

Torpedo Countermeasure Representation. The Navy currently uses U.S. countermeasures for torpedo testing that operate differently from foreign threat countermeasures. To accurately determine and maximize torpedo performance against other nation's submarines, the Navy needs static and mobile submarine-launched countermeasure surrogates that can emulate threat capabilities.

Weapons Set-to-Hit Target. The Navy conventionally conducts torpedo testing in a set-not-to-hit mode, with the unarmed weapon passing safely above or below the target submarine and lacks a capability to evaluate final approach and impact on the target hull, known as set-to-hit testing. The Navy is currently investigating the use of older submarines, which are about to be decommissioned, as representative set-to-hit targets that are mobile and reactive. The ability to evaluate this final stage of torpedo attack is required to accurately determine lethality and effectiveness of the torpedo against threat submarines employing full evasion capability. The Navy needs to build a full-size autonomous submarine surrogate that can provide representative response in both maneuver and countermeasure employment.

Self-Defense Test Ship (SDTS). Navy ships and combat systems must be able to defend themselves against anti-ship cruise missile attack if they are to survive in armed conflict. Test range safety restrictions do not permit aerial targets to fly close enough to or directly at Navy ships to allow for operationally realistic self-defense testing so the Navy has traditionally used the unmanned SDTS for close-in self-defense evaluation. The SDTS is a decommissioned Spruance-class destroyer that can be equipped with the combat systems of various ship classes and operated via remote control. Aerial targets can be flown close enough to the SDTS to evaluate performance within proximity to the test platform that cannot be accurately determined from other testing. The current Navy SDTS is planned to support self-defense testing for multiple classes of ship programs. The Navy is actively working to overcome shipyard delays and additional funding costs to assure SDTS availability and prevent delay of future test programs. The Navy expects these issues to be resolved by early 2025. The Navy has yet to determine SDTS capability for follow-on platform and system evaluation including future improvements to the Aegis Combat System. To support adequate testing, the Navy should identify and develop an SDTS capability, which could include further extension of the existing SDTS, that supports upcoming testing, as well as future ship-class and combat system programs.

» LAND

Ground-based Air Defense Replication. The ground-based air defenses of peer-level adversaries are multifaceted and multilayered, involving kinetic defenses, EA defenses, and DE point defense weapons. Major shortfalls exist in each of these domains. Surface-to-air missile (SAM) sites are one of the key classes of ground targets for U.S. aircraft and air-launched weapons, as well as key threats to these aircraft and weapons. Despite initiatives to enhance the open-air range infrastructure for threat radar EA and DEW emulation, shortfalls remain because adversaries continue to rapidly advance and expand their capabilities. The DoD requires additional investment in high-fidelity emulation of threat EA and DEW systems.

In addition, the DoD requires additional investments in radar test assets capable of high-fidelity emulation of signal detection and tracking capabilities of advanced threat radars. These radar assets should be associated with specific SAM systems and the wider integrated air defense systems that support SAM employment. For each of the aforementioned threat systems, test ranges should have sufficient numbers of moveable vehicle shells to physically represent the threat system vehicle types accurately, with reflectivity properties, coatings, and camouflage netting typical of those employed.

MODELING & SIMULATION

As adversary threats and system capabilities become more complex, the DoD has struggled to develop and maintain validated M&S. The rate of adversary threat development is currently faster than the pace of high-fidelity M&S threat model development. As a complement to live testing of physical systems, there is increased effort in the DoD to pursue digital M&S solutions that represent current capabilities of systems under test and of the threats they need to be tested against in joint environments. Validated M&S solutions are necessary to support the end-to-end assessment of systems, particularly in cases where the system cannot be demonstrated for operational, cost, or security reasons.

Integrated Air Defense. The evaluation of integrated air defense systems will require a joint M&S environment to provide the end-to-end performance of numerous sensors, shooters, and command and control networks developed across the Army, Navy, Air Force, and MDA. This capability will require integration of M&S tools developed across the Services.

Missile Defense Systems. The MDA needs to develop a system-level, high-fidelity digital modeling venue to allow quantitative assessments of the effectiveness of integrated hypersonic and ballistic missile defense systems. The MDA began development of the End-to-End Digital Integrated System-level Simulation in 2018 but recently terminated funding for that effort. Even with the right test corridors and instrumentation, there will be flight safety and cost limitations that make high-fidelity M&S essential.

Joint Simulation Environment. Limitations in open-air range infrastructure caused the Navy and Air Force to explore incorporating additional weapon systems into the JSE to enable testing and training that cannot currently be conducted on the DoD's major test and training ranges due to technical (i.e., threat complexity or density) and security reasons. The JSE requires additional blue and red platforms, emitters, and weapon types to simulate a "night one" fight against a peer-competitor or near-peer-competitor adversary. Shortfalls exist in JSE with regard to current and future representation of surface-to-air, air-to-air, and naval threat capabilities. The recently established joint Navy and Air Force JSE Governance is working to overcome these shortfalls, but technical, programmatic, and cost obstacles remain.

Autonomous Systems. Maritime autonomous systems have a large range of sensors. Perception of their environment is dependent upon below or at surface operation. Attaining confidence in the autonomy based on this perception requires significant assessment of capability within a decision-rich environment that is time intensive and challenging with live testing alone due to safety constraints and the pace of operations. Development and assessment of these systems will be accelerated with credible synthetic range capability that supports hardware-in-the-loop and software-in-the-loop evaluation within operationally representative conditions. Investment is required to fully characterize the perception of the employed sensors across the spectrum of operational environments.

Anti-Ship Missile and Launch Platforms. The Navy needs M&S of anti-ship missile and launch platform threats to support operational testing for ship combat systems, EW suites, and ship missile systems. The Navy lacks validated threat models to determine systems performance across the range of threats. Recent shipboard EW programs had only two intelligence-community validated threat models available for operational test. The Navy also has no

M&S representations of the foreign radar systems which provide the pre-launch targeting information to anti-ship missiles. Without models, DOT&E cannot assess how well systems perform against such threat radars.

Cyber. Assessing the DoD cyber survivability and resilience would benefit from accredited simulation environments to evaluate mission effects caused by cyber-attacks that have been demonstrated through other testing. Without exercising the mission in the presence of a given cyber effect, it is not possible to assess end-to-end system performance.

EMS OPERATIONS

The electromagnetic operating environment (EMOE) is increasingly congested and contested by military and civilian systems and constrained by national and international regulations. In addition, modern software defined EMS-dependent systems can rapidly change their operating characteristics. Future adversary EMS-dependent systems will include complex, autonomous behavior (incorporating AI to varying degrees) that will adapt to changing environments as the systems learn. The Threat Systems Management Office developed the Ground Electronic Warfare T&E Roadmap that provides a time-phased investment plan to fill Army and Marine Corps EW T&E gaps. This plan, however, does not address EW T&E gaps required to test in a multi-domain environment.

The inability to represent modern radars affects T&E of EW systems and their associated combat systems and platforms. Emulating the closed-loop tracking capabilities of modern threat radars, including software-defined radars, remains a shortfall. This shortfall critically affects the ability to conduct adequate operational testing of our Electronic Attack (EA) capabilities. Additionally, it affects the ability the test EA capabilities to support their host platforms' mission. Most of the radar emulation capabilities on the test ranges and in laboratory facilities emulate only the open-loop signal emissions of threats, and not the sophisticated back-end processing, including electromagnetic protection logic, that these radars employ.

Other key EMS-related shortfalls are focused on our emulation of threat electromagnetic attack systems. For example, the current set of anti-ship missile surrogate (aerial target) payloads do not sufficiently represent foreign electromagnetic attack systems for use in testing a program's electromagnetic protection. While the Navy has improved their ability to represent such threats, advancements in these capabilities have not yet been fully integrated into aerial targets. This issue affects all variants of shipboard air and missile defense systems, and host platforms. Another key shortfall is in the ability to conduct frequent and simultaneous GPS jamming and spoofing across multiple test ranges, at times due to FAA regulations.

In addition, adversaries are fielding passive radars utilizing the emissions from commercial transmitters, which need to be emulated in test. Including emulations of all types of neutral emissions in OT&E is critical to assessing the DoD ability to operate in complex military and commercial electromagnetic environments.

Potential adversaries have a diverse set of capabilities to detect U.S. units across a broad set of operational environments. The DoD must be able to fully characterize the susceptibility of U.S. troops and friendly units to the detectability of acoustic, visual, IR and electromagnetic emissions by our adversaries. These characterizations require a combination of M&S-, laboratory-, field-, and operational testing.

DIRECTED ENERGY WEAPONS

The DoD lacks facilities to safely test High Energy Laser (HEL) weapon systems in realistic combat conditions. DoD initiatives are required to outfit test and training ranges with HEL-specific safety equipment to conduct open-air, self- and area-defense test scenarios with weapons expected to produce HEL beams. Radar, IR and EO sensors will also be needed throughout the engagement zone to collect data on target position, velocity, reflected irradiance, and battle damage for assessing performance.

The Army's White Sands Missile Range is developing requirements to upgrade its HEL Systems Test Facility. Current operations are limited to testing one system at a time and do not support test in multi-domain operations. The upgrades would provide DE and counter-DE, as well as comprehensive integrated air and missile defense T&E capabilities. Future open-air tests of Navy shipboard self-defense HEL systems will need accredited threat surrogates for anti-ship cruise missiles and swarming unmanned airborne and surface vehicles. Finally, the DoD lacks test ranges with surrogate systems capable of replicating peer threat capabilities for tactical lasers, high-power microwave, or ultra-wideband DEW point defenses to assess end-to-end effectiveness and vulnerability of airborne platforms.

CYBER

Emerging Cyber Command capabilities for cyberspace operations, including those that are part of the Joint Cyber Warfighting Architecture, will require novel, range-based resources to assess the ability of the cyber operational force to monitor activity, issue orders, and engage across the spectrum of friendly, neutral, and adversary cyberspace. These resources include ranges with neutral and malicious traffic, scenario generation capabilities, and digital copies of cyber operational force mission systems to support OT&E while the primary systems support real-world operations.

DoD Instruction O-3600.03, “Test and Evaluation of Cyberspace Effects and Enabling Capabilities,” aligns testing requirements for cyberspace effects and enabling capabilities (CEEC) with traditional acquisition requirements for non-cyber capabilities to ensure that CEEC are effective, suitable, and survivable in their intended operational environments and against intended targets. Current CEEC testing requires additional investment in opposing force emulation to create operationally realistic attack surfaces.

Cyber OT&E relies on appropriately trained adversarial testers, DoD Cyber Assessment Teams (DCAT), and DoD Certified Red Teams (DCRTs) to act as aggressors. Demand for adversarial cyber testing is increasing. The DoD should ensure these teams are fully staffed and trained on emerging cyber threat tactics, techniques, and procedures. DCRTs/DCATs also require collaboration environments to share information and jointly develop tactics, techniques, and procedures. Digital and physical collaboration spaces should exist at all necessary classification levels.

Cyber test teams lack sufficient expertise in several technology areas where cyber threat actor capability is out-pacing our ability to defend, including:

- Cloud systems supporting software development, hosting user-facing applications, or housing national defense data
- Networks using non-traditional protocols, including automotive and aircraft controls; weapons systems (e.g., firing, targeting); radio communication; satellite communication; hull, mechanical, and electrical; supervisory control and data acquisition; and industrial control systems
- Systems that exchange vital mission data via RF interfaces
- AI and machine learning-based approaches to cyberspace attack and defense

These limitations constrain the DoD’s ability to understand system performance and survivability against a peer or near-peer threat actor.

NUCLEAR MODERNIZATION

The DoD requires full funding to support upgrades to critical T&E infrastructure that supports nuclear modernization programs. Test chambers at proper classification are needed to support development and testing of the various nuclear effects as associated with DoD Instruction 3150.09, “Chemical, Biological, Radiological, and Nuclear Survivability.”

AI AND AUTONOMY

Testing AI and autonomy (AI&A)-enabled systems requires expanded processes, networks and instrumentation to cover the larger operational space required to assess model generalizability. More workforce expertise in software integration and data analytics are needed to collect, integrate, store, reduce, and analyze enough data to quantify performance and risk. Testing survivability against adversarial attacks and addressing unintended bias and unexpected performance for AI&A functions will be necessary to adequately evaluate AI&A systems.

Data infrastructure is a major enabler for T&E of AI&A-enabled systems for automated and real-time data collection, reduction, and analysis. Big data analytics and large knowledge management systems are required to improve the quality, speed, and depth of post-mission data processing. In addition to data collection infrastructure, system and platform agnostic data collection tools will be required. The Joint Mission Environment Test Capability program is building out the network infrastructure to support operations across integrated test ranges, and wide area off-range exercises and experimentation events. SkyRange is advancing instrumentation needs across larger operational spaces using modified Global Hawks as instrumentation platforms. Cloud Hybrid Edge-to-Enterprise Evaluation and Test Analysis Suite (CHEETAS) is closing gaps in collecting, integrating, storing, and analyzing the data. The B-52 upgrade programs and hypersonic weapons testing recently demonstrated the use of CHEETAS for managing and transporting data faster.

The Chief Digital & Artificial Intelligence Office seeks to address a lack of AI&A tools, but increased emphasis needs to be placed on educating test agencies, programs, and field organizations on what tools exist and how to use them. Numerous efforts are underway across the Services, including the Air Force's VISTA X-62A testbed that facilitates evaluation of AI&A aircraft capabilities; the Army's Combat Vehicle Robotics technology integration program to address capability gaps on robotic and autonomous platforms; and the Navy's Naval Autonomous Test System that creates a simulation framework for testing autonomous systems.

SPACE

To increase resilience of U.S. space operations, communication and missile defense programs will place many more satellites into orbit performing various missions, increasing the importance of adequate T&E for these systems. Tests conducted on-orbit need high-fidelity space-based threat surrogates and range instrumentation to collect data from testing and transmissions to ground-based command-and-control systems. The space environment will also need to be emulated in space simulation chambers to replace or supplement on-orbit testing, especially for survivability evaluations from lasers, high power microwaves, and kinetic attacks. When on-orbit tests are impractical, evaluations can use full motion mission simulators and simultaneous reproductions of the natural and man-made environments.

Space test and training ranges – including the National Space Test and Training Complex (NSTTC) – are being developed to connect space-based resources with open-air and laboratory-based hardware-in-the-loop simulation environments. NSTTC, under the authority of Space Training and Readiness Command (STARCOM), is envisioned to provide resources for T&E in EW, cyber, DE, kinetic, and nuclear environments.

The DoD needs qualified personnel to operate test assets, analyze data, and conduct tests on new space systems and technologies. STARCOM and Space Delta 12 lack experienced T&E personnel and funding needed for adequate OT&E of programs under DOT&E oversight. These shortages impede comprehensive assessments of operational effectiveness, suitability, and survivability.

DOD PROGRAMS

This page intentionally left blank.

Aerosol Vapor Chemical Agent Detector (AVCAD)

In June 2023, DOT&E approved the Aerosol Vapor Chemical Agent Detector (AVCAD) Milestone C (MS C) TEMP, which required additional developmental and operational testing on low-rate initial production systems to address deficiencies discussed in DOT&E's April 2023 operational assessment report. Laboratory testing with chemical warfare agents (CWAs) is scheduled to finish by 1QFY25. The multi-Service operational test and evaluation (MOT&E) began in FY24, and DOT&E intends to publish an MOT&E report in 2QFY25, to support the Army's full-rate production (FRP) decision later that quarter.

SYSTEM DESCRIPTION

The AVCAD is an aerosol and vapor CWA and non-traditional agent detector. The AVCAD will provide warfighters with the new capability to detect CWA aerosols as well as additional persistent V-Series and A-Series CWAs. The Joint Services, without the Air Force, plan to employ AVCAD as a man portable detector; a fixed-site monitoring device; and on manned vehicles, ships, and aircraft to detect and alert personnel to the presence of chemical warfare agents and support force-protection decisions. The AVCAD is designed for operation using shore power, battery, or the power provided by the integrated platform itself.

The Army is the only Service intending to use the AVCAD in a perimeter defense mission. The AVCAD is designed as a networked detector with the ability to be controlled and send alerts over a network using the Army's Integrated Sensor Architecture. Receiving units will need to provide necessary hardware not fielded with the system in order to add AVCAD to any network.

MISSION

Joint warfighters equipped with the AVCAD will employ the system to detect CWAs and non-traditional agents in aerosol and vapor physical states; alert personnel in the event of a chemical attack; and support post-attack reconnaissance, surveillance, and decontamination missions across the full range of military operations. The Army has a perimeter defense mission where detectors are placed in an array and alarms are remotely monitored over a radio network. The radios are not fielded as part of the system.

PROGRAM

AVCAD is a joint Acquisition Category III program and was authorized in May 2023 to enter the production and deployment phase. DOT&E approved the MS C TEMP to support the low-rate initial production decision in June 2023.

In April 2023, DOT&E published an operational assessment, which identified a number of challenges. The program office worked with the vendor to address the recommendations. The vendor updated software algorithms with intentions to improve detection performance and false alarm rates. The program office added a cleaning tool and updated preventative maintenance checks and services (PMCS) procedures to address reliability and system-to-system variability concerns. The program office updated the technical manual with the PMCS procedures. The program office also updated hardware components to improve performance in electromagnetic environments.

The production and deployment phase of testing began in January 2024, with a FRP decision targeted for March 2025. The program conducted an MOT&E in August 2024 in accordance with the DOT&E-approved test plan. DOT&E observed the testing and will publish a classified MOT&E report in 2QFY25 prior to the FRP decision.

» MAJOR CONTRACTOR

- Smiths Detection, Inc. – Edgewood, Maryland

TEST ADEQUACY

In accordance with the DOT&E-approved TEMP, the AVCAD program office is conducting a series of laboratory chamber tests to demonstrate performance against vapor and aerosol disseminations of chemical warfare agents. Due to deficiencies identified during the engineering and manufacturing development phase, the MS C TEMP directed additional developmental and operational testing on the low-rate initial production items. The program office conducted a number of false alarm and reliability tests at a variety of locations to confirm fixes emplaced after engineering and manufacturing development was completed in FY23.

In FY24, the program began the MOT&E, in accordance with the DOT&E-approved test plans:

- In April 2024, the program conducted cyber survivability testing with a cooperative vulnerability and penetration assessment, which was followed by an adversarial assessment in August 2024.

- In August, the program conducted the land portion of the MOT&E with the Army and Marine Corps.
- In October 2024, the Navy conducted a maritime operational test.

DOT&E observed each of the MOT&E events, which cumulatively were adequate to assess operational effectiveness, suitability, and cyber and electromagnetic survivability. DOT&E will publish a classified MOT&E report when data analyses are complete in 2QFY25.

PERFORMANCE

» EFFECTIVENESS

DOT&E will provide an evaluation of the operational effectiveness, following the scheduled completion of laboratory testing in December 2024, in the classified MOT&E report in 2QFY25.

» SUITABILITY

DOT&E will provide an evaluation of the operational suitability, following the completion of all testing outlined in the DOT&E-approved TEMP, to include evaluating the efficacy of the updated training and technical manuals, in the classified MOT&E report in 2QFY25.

» SURVIVABILITY

DOT&E will assess cyber and electromagnetic survivability in the classified MOT&E report in 2QFY25. The report will also assess if the updates to AVCAD mitigated the identified cyber deficiencies discussed in the classified annex to the DOT&E AVCAD operational assessment report, dated April 2023.

RECOMMENDATIONS

The Joint Product Manager for Chemical, Biological, Radiological, and Nuclear Sensors should:

1. Review the recommendations in the DOT&E MOT&E report released in 2QFY25.

The Army should:

1. Purchase equipment needed for the perimeter defense mission.

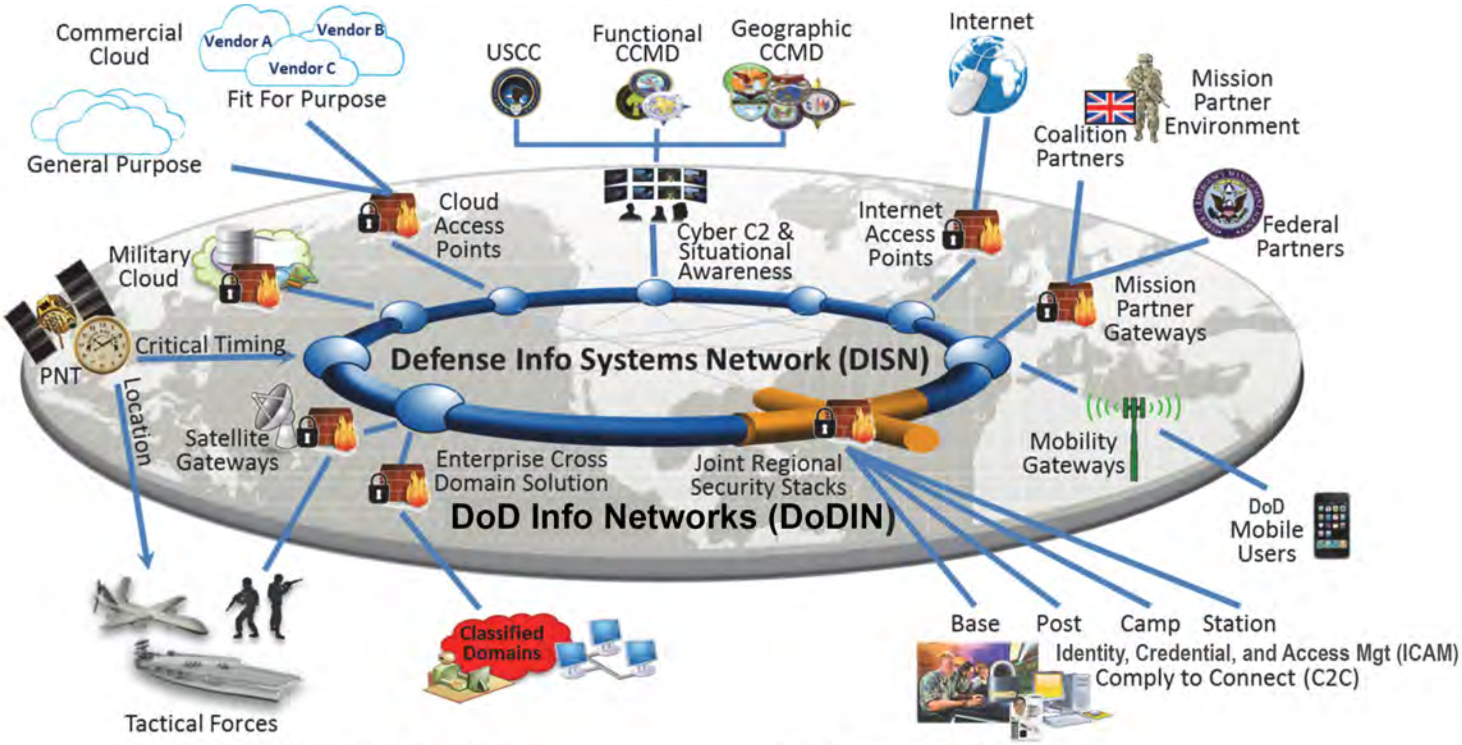
Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives

The DoD Information Enterprise Portfolio Management, Modernization and Capabilities (PM2C) Council continues to govern aspects of the Department's information enterprise to include the Joint Warfighter Cloud Capability (JWCC) oversight and cloud rationalization initiative. In June 2024, the DoD Chief Information Officer (CIO) published the new *Fulcrum: The Department of Defense (DoD) Information Technology (IT) Advancement Strategy.* The Fulcrum Strategy advances the Digital Modernization Strategy (DMS) for the DoD. The DoD CIO, Defense Information Systems Agency (DISA), and Services have been implementing programs, projects, and initiatives intended to achieve DoD DMS objectives. Many DMS initiatives lack an overarching systems integration process, test strategy, and program executive organization to manage cost, drive schedules, and monitor performance. Deploying untested DMS programs, projects, and initiatives poses an operational risk to the DoD enterprise, particularly in a cyber-contested environment. Future deployment decisions must be informed by adequate OT&E.

SYSTEM DESCRIPTION

The DoD DMS summarizes the Department's approach to IT modernization, focused on the Joint Information Environment Framework intended to improve networking capabilities for fixed and mobile users. The DoD DMS aims to institute new enterprise IT services, modernize technology through coordinated refresh efforts, implement a new joint cybersecurity capability, and improve access to data. Current DoD DMS efforts are intended to:

- 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) via Microsoft Office 365 (O365) on NIPRNet, SIPRNet, and tactical (Denied, Disconnected, Intermittent, or Limited (DDIL)) networks; Capability Set 2 - Business Voice and Video; and Capability Set 3 - Assured Command and Control Voice
- Deploy Identity, Credential, and Access Management (ICAM) capabilities that support DoD systems using a federated approach for DoD-approved Identity Providers
- Transform the DoD cybersecurity architecture to implement Zero Trust throughout the DoD Enterprise, including initiatives to provide endpoint security for devices (both desktop and mobile devices)
- Sustain cybersecurity capabilities to protect the DoD Information Network and support defensive cyber operations and network operations for bases, posts, camps, and stations (known as Joint Regional Security Stack (JRSS))
- Strengthen collaboration, international partnerships, and allied interoperability through a Mission Partner Environment (MPE)



CCMD – Combatant Command
C2C – Comply to Connect
DoD – Department of Defense
ICAM – Identity, Credential, and Access Management
USCC – United States Cyber Command
C2 – Command and Control
DISN – Defense Information Systems Network
DoDIN – DoD Information Networks
PNT – Positioning, Navigation and Timing

PROGRAMS, PROJECTS, AND INITIATIVES

In June 2024, the DoD CIO published *Fulcrum: The DoD IT Advancement Strategy*. The Fulcrum Strategy advances the DMS for the DoD. Fulcrum represents the Department's shift towards leveraging technology as a strategic enabler capable of enhancing operational effectiveness and delivering superior value to the warfighter. The DoD CIO intends to establish a governance forum to manage the priorities outlined in the Fulcrum Strategy, track delivery, and focus on resources.

The DoD Information Enterprise PM2C Council continues to govern aspects of the Department's information enterprise to include JWCC oversight and cloud rationalization initiatives. Cloud rationalization is the DoD CIO effort to consolidate the Department's disparate cloud contracts under a single DoD umbrella contract.

DISA is the principal integrator for DoD Information Network enterprise capabilities, enabling initiatives, and testing. Many DMS efforts lack an overarching systems integration process, test strategy, and program structure with trained program managers to manage costs, drive schedules, and monitor performance factors. The DoD CIO, DISA, and Services intend to achieve DMS objectives by implementing programs, projects, and initiatives, which currently include:

- **Enterprise Collaboration and Productivity Services (ECAPS):** In FY24, the DEOS Program Management Office (PMO) continued efforts to provide commercial cloud-hosted SIPRNet office productivity and collaboration capabilities (known as DoD365-Sec) with cyber testing support provided by the Joint Interoperability Test Command (JITC). In FY24, the DoD CIO and DISA continued fielding DoD365 Integrated Phone System (DIPS) on NIPRNet to support ECAPS Capability Set 2 (Business Voice) to the Services and Agencies with projected full deployment in FY25. The DoD needs to address OCONUS and Next Generation 911 dialing in DIPS; however, these enhancements have yet to be funded. DISA is providing ECAPS Capability Set 2 (Business Video) on NIPRNet via DoD365 Teams. In the future, the DEOS Program Office intends to work with the Services to implement tactical DDIL network solutions. In FY21, the DoD CIO and DISA determined the solution for Capability Set 3 (Assured Command and Control Voice) to be the DISA-managed Enterprise Classified Voice over Internet Protocol (ECVoIP) service on SIPRNet. The DoD CIO identified Global Video Services-Classified (GVS-C) and DoD365-Sec as the hybrid solution for Capability Set 3 (Assured Video) on SIPRNet. In FY24, DISA began a GVS-C technical refresh that will continue into FY25.
- **Identity, Credential, and Access Management (ICAM):** The DoD CIO is the lead for ICAM governance for the DoD. The six DoD CIO-approved ICAM solutions are Army, Navy, Air Force, Defense Logistics Agency (DLA), Defense Health Agency (DHA), and DoD Enterprise ICAM. DISA is the service provider for DoD Enterprise ICAM. In FY24, DoD CIO and DISA shifted to a Federated approach for Identity Providers (IdP). DISA intends to build a Federation Hub and integrate the Army, Navy, and Air Force ICAM by the end of FY25, and DLA and DHA ICAM in FY26. The DoD Enterprise ICAM is made up of three capability pillars: IdP, Automated Account Provisioning (AAP), and Master User Record (MUR). In FY24, DISA continued integrating financial and other applications with the ICAM capabilities on NIPRNet that will continue through FY26. ICAM solutions need to support Service and Agency requirements and the Zero Trust activities by FY27. The FY24 National Defense Authorization Act (NDAA) required the DoD to establish an Enterprise ICAM acquisition program of record. However, the DoD CIO and DISA are seeking a waiver from this task. A major part of the ICAM acquisition effort is the Public Key Infrastructure, detailed in a separate section of this Annual Report.
- **Zero Trust:** The DoD is adopting a Zero Trust data-

centric security model intended to provide effective security even if networks or devices are breached by an adversary. Thunderdome is an effort to help the DoD implement Zero Trust principles. DISA awarded a Thunderdome production agreement in 4QFY23 and implemented Thunderdome on NIPRNet at DISA and 4th Estate agencies in FY24. DISA transitioned Thunderdome to a Middle Tier of Acquisition program in FY24 and intends to implement Thunderdome on SIPRNet in FY25.

- **Joint Regional Security Stack (JRSS):** In FY21, the DoD CIO began efforts to phase out JRSS and transition to a Zero Trust security and network architecture. The DoD intends to decommission JRSS by the end of FY27.
- **Mission Partner Environment (MPE):** In support of DoD Directive 5101.22E, the Air Force is developing enterprise MPE services tailored to meet DoD mission partner information sharing needs, while supporting rationalization of existing combatant command MPE capabilities, such as Combined Enterprise Regional Information Exchange Systems (CENTRIXS). The Air Force is developing the Secret and Below Releasable Environment (SABRE) as the first modernized MPE capability platform. JITC is working with the Air Force to develop an MPE SABRE TES. In 1QFY25, the Air Force employed SABRE to demonstrate a federated Enterprise IdP capability for Project Olympus, which is a Joint Staff initiative focused on integrating capability development activities in Bold Quest 24. In FY25, DISA intends to provide real identities via Global Federated User Domain (GFUD) to support Project Olympus. In 4QFY25, JITC intends to conduct an operational assessment of SABRE to support an initial operational capability declaration.
- **Enterprise Cloud Efforts:** The DoD continues to leverage commercial cloud innovations to deliver infrastructure and services for the DoD enterprise. In December 2022, the DoD awarded the JWCC multi-vendor contract designed to meet DoD enterprise cloud requirements. Congress directed the DoD in the FY23 NDAA, Section 1553, to conduct cyber testing of DoD commercial clouds containing classified data.

TEST ADEQUACY

DOT&E is monitoring the DMS programs, projects, and initiatives that could provide significant benefits to the DoD, but also could pose a significant operational risk to the DoD in a cyber-contested environment if not adequately protected. Below are specifics for each:

- **ECAPS:** The DEOS PMO and JITC did not conduct an early operational assessment on DoD365-Sec in FY24 as originally planned and reported in DOT&E's FY23 Annual Report because the PMO decided not to test prior to fielding. However, JITC conducted a cyber assessment of DoD365-Sec and GFUD for SIPRNet IdP in 3QFY24, per a DOT&E-approved cyber test plan. DOT&E observed the cyber assessment. DISA has yet to fund JITC to conduct OT&E of ECAPS Capability Sets 2 and 3.
- **ICAM:** DISA did not fund JITC to conduct operational ICAM capability testing in FY24. In FY24, DISA submitted a service request and intends to fund JITC to resume testing support for the DoD Enterprise ICAM in FY25. The DoD CIO sponsored an ICAM issue paper in FY24 that included some funding for JITC to conduct future DoD Enterprise ICAM and Federation Hub operational testing.
- **Zero Trust:** The NIPRNet Thunderdome capability is designed to address the seven DoD Zero Trust pillars. In late FY23 and early FY24, JITC conducted an early cyber assessment of the NIPRNet Thunderdome capabilities. DISA intends to fund JITC to conduct operational NIPRNet and SIPRNet Thunderdome capability testing in FY25.
- **JRSS:** JITC did not conduct OT&E of JRSS in FY24 but will continue to monitor JRSS until it is decommissioned by the end of FY27.
- **MPE:** The MPE SABRE PMO and JITC did not conduct OT&E

of MPE capabilities in FY24. The PMO and JITC intend to conduct a cyber assessment of MPE SABRE in late FY25.

- **Enterprise Cloud Efforts:** In 3QFY24, JITC conducted a threat-representative cyber assessment of the DoD365-Sec cloud infrastructure, per a DOT&E-approved cyber test plan. This was the first operational cyber assessment of a DoD secure commercial cloud per the FY23 NDAA, Section 1553, which required such testing of DoD commercial clouds containing classified data. DOT&E observed the cyber assessment.

PERFORMANCE

In FY24, except for the DoD365-Sec cyber assessment, there was no operationally realistic testing performed on DMS programs, projects, or initiatives, precluding an evaluation of their operational effectiveness, suitability, or cyber survivability. DOT&E intends to publish a classified DoD365-Sec cyber test report in 1QFY25.

RECOMMENDATIONS

As recommended in the FY23 Annual Report, the DoD CIO, Services, Director of DISA, and various DMS governance forums should:

1. Manage DMS initiatives with trained program managers and supporting offices.
2. Develop a TEMP or TES for each funded DMS enterprise IT initiative.
3. Fund JITC to fully support DMS enterprise IT initiatives, testing, and test-related forums.
4. Perform threat representative cyber survivability testing of all DMS enterprise IT programs, projects, and initiatives in accordance with current DoD and DOT&E cyber survivability T&E guidance and policy, and use operational test data, analyses, and reporting to inform DMS governance decisions.
5. Conduct comprehensive cyber survivability testing of secure cloud environments per the FY23 NDAA, Section 1553.

DoD Healthcare Management System Modernization (DHMSM®)

DoD Healthcare Management System Modernization (DHMSM) consists primarily of MHS GENESIS, which is the DoD's electronic health record system that is now fully fielded to all major medical treatment facilities. In FY23, the Joint Interoperability Test Command (JITC) executed a DOT&E-approved operational test on the billing component of the MHS GENESIS system, known as Revenue Cycle Expansion (RevX), that was added after the initial deployment of the system. DOT&E will publish a report on this test event in FY25.

DHMSM® and MHS GENESIS® are registered trademarks of the DHMSM Program Management Office (PMO).

SYSTEM DESCRIPTION

MHS GENESIS is a modernized electronic health records system for the DoD, the Department of Veterans Affairs, the U.S. Coast Guard, and the National Oceanic and Atmospheric Administration. It creates a single healthcare record for each patient that can be utilized by all four organizations.

MHS GENESIS comprises three major elements: (1) the Millennium suite of applications, which provides medical capabilities; (2) Dentrix Enterprise, which provides dental capabilities; and (3) the Orion Rhapsody Integration Engine, which enables the majority of the external information exchanges.

The RevX component of MHS GENESIS covers all revenue features, to include patient scheduling, registration, preauthorization, medical coding, claims submission, billing, and payment processing.

MISSION

DoD and other Federal Government medical staff use MHS GENESIS to manage delivery of healthcare within garrison facilities. DoD medical staff also use MHS GENESIS to perform administrative support, front desk operations, logistics, billing, and business intelligence.

PROGRAM

MHS GENESIS is a Business System Category I program that completed fielding to all major medical treatment facilities in March 2024. With deployment completed, MHS GENESIS is approaching the capability support phase of its acquisition pathway.

DOT&E approved the TEMP in October 2017. The program completed IOT&E in July 2018, with multiple rounds of FOT&E and cyber testing between 2019 and 2023. The DHMSM PMO has committed to executing at least one additional FOT&E event to capture any outstanding requirements and capabilities that have not been assessed. The PMO continues to fund the execution of Persistent Cyber Operations (PCO) to help maintain and improve cyber survivability.

The DHMSM PMO began deploying the Revenue Cycle Expansion (RevX) component of MHS GENESIS as part of its regular fielding activities for new waves of MHS GENESIS in September 2022. The PMO completed fielding to sites where MHS GENESIS had previously been fielded without RevX in April 2023. RevX covers all revenue features, to include patient scheduling, registration, preauthorization, medical coding, claims submission, billing, and payment processing. It introduces new capabilities and workflows to support patient accounting and billing.

» MAJOR CONTRACTORS

- Leidos Partnership for Defense Health – Reston, Virginia
- Oracle Health – Austin, Texas (Millennium suite)
- Henry Schein ONE – American Fork, Utah (Dentrix Enterprise)

TEST ADEQUACY

JITC executed a DOT&E-approved operational test of the RevX component of MHS GENESIS in May 2023. DOT&E observed the test and will report the findings in 2QFY25. This is a delay from the FY23 Annual Report. DOT&E expects to report separately on PCO activities covering FY24 in FY25.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

DOT&E will report on the operational effectiveness and suitability of the RevX capability in 2QFY25.

» SURVIVABILITY

The RevX OT&E did not evaluate cyber survivability because RevX is a subcomponent of MHS GENESIS, and its survivability cannot be evaluated separately.

RECOMMENDATIONS

The DHMSM PMO should:

1. Conduct an FOT&E of MHS GENESIS to re-evaluate the operational effectiveness and suitability of MHS GENESIS, including RevX, with patient-facing components and at OCONUS sites.
2. Continue to fund and execute PCO on MHS GENESIS and its components.

The Director, Defense Health Agency (DHA) should:

1. Continue to fund and execute PCO on DHA infrastructure and platforms that support and integrate with MHS GENESIS.

F-35 Joint Strike Fighter (JSF)

In February 2024, DOT&E published a classified F-35 combined IOT&E and LFT&E report, supporting the Milestone C Defense Acquisition Board review in March. The report provides an independent assessment of the overall mission capability of the F-35 in the Block 3F configuration, in terms of its operational effectiveness, suitability, and survivability. The report included a separate annex that provided an assessment of F-35 Block 4 operational testing which occurred following IOT&E.

The program proceeded to full-rate production, based on an acquisition decision memorandum (ADM) signed by USD(A&S) in March 2024. The transition to full-rate production occurred in the middle of nearly a year-long pause in acceptance of production aircraft, as the program worked to achieve stability in the new hardware and software to the point where it met the acceptance standards of the Services, facilitating the aircraft's delivery. Although Lockheed Martin planned to deliver the Lot 15 aircraft – the first lot with the new Technology Refresh 3 (TR-3) mission systems architecture – starting in July 2023, they had to put the aircraft in long-term parking because the mission systems software did not satisfactorily function on the TR-3 hardware. As a result, the Services, in coordination with the program office, refused to take delivery of TR-3-equipped aircraft until July 2024.

The F-35 development effort too was facing challenges in delivering reliable, fully functional software to the operational test (OT) teams. In February 2024, the United Operational Test Team (UOTT) called for a "stop test" of the software they were testing (30R08) – intended as the last version of software fielded on the TR-2 aircraft – due to stability problems, shortfalls in capability, and deficiencies they discovered. Quality escapes from the manufacturing and production processes (i.e., problems that should have been identified and corrected during the check-out and acceptance process for new aircraft) are still being identified in the field.

The F-35 Joint Program Office (JPO) has not adequately planned for OT of the upgraded TR-3 hardware configuration to be completed prior to delivering multiple TR-3 aircraft to field units. DOT&E assesses that dedicated operational testing of these aircraft will not occur until mid to late FY26, approximately two years after the configuration began delivery to the field.

SYSTEM DESCRIPTION

The F-35 Joint Strike Fighter (JSF) is a tri-Service, multinational, single seat, single-engine strike fighter aircraft. It is replacing legacy strike fighter aircraft in the U.S. Air Force, Marine Corps, and Navy and is being produced in three variants:

- F-35A Conventional Take-Off and Landing for the Air Force
- F-35B Short Take-Off/Vertical Landing for the Marine Corps
- F-35C Aircraft Carrier Variant for the Navy and the Marine Corps

The F-35 modernization plan, as defined in the Block 4 Modernization Capability Development Document (CDD), specifies required capabilities and associated capability gaps that drive incremental improvements under an agile acquisition framework.

MISSION

The missions of the F-35 aircraft include attacking fixed and mobile land targets, surface combatants at sea, and air threats, including advanced aircraft and cruise missiles, in joint operations during day and night, in all weather conditions, and in heavily defended areas.

PROGRAM

The F-35 JSF is an Acquisition Category ID program. DOT&E approved the fourth revision of the System Development and Demonstration TEMP in March 2013, which directed and governed the conduct of IOT&E. IOT&E was completed in September 2023, and DOT&E published a combined IOT&E and LFT&E report in February 2024 for Block 3F with a separate annex on Block 4 testing to date. The report supported a subsequent Defense Acquisition Board, which resulted in the USD(A&S) approving full-rate production in a March 2024 ADM.

The full-rate production decision ADM directed the program to designate two major subprograms within the overall acquisition program – one for the engine modernization effort and one for F-35 Block 4 development. The Block 4 development subprogram will replace the former Continuous Capability Development and Delivery program for adding new capabilities – both hardware and software – to the F-35 aircraft. The TR-3 avionics upgrade is a key enabler for new Block 4 mission systems capabilities and includes upgraded integrated core processors, aircraft memory system, and panoramic cockpit displays. The TR-3 upgrade replaces the corresponding TR-2 components that are currently fielded. No combat-capable TR-3 aircraft have been delivered to the U.S. Services to date.

The program planned for the TR-3 upgrade to cut into the production line in time to deliver with the Lot 15 aircraft in 2023. As designed, the TR-3 architecture would host the capabilities from the 30R07 TR-2 software build with the new designation of 40R01. The capabilities added and delivered in the 30R08 TR-2 software would be added to the next software build, 40R02. However, problems with both the hardware and software during developmental testing (DT) forced the program to delay delivery of the Lot 15 production aircraft until performance improved. These aircraft were put into long-term parking after production, to enable the production line to continue.

To stabilize the performance on the new TR-3 hardware, the program developed a truncated version of software by disabling combat capabilities that had already been fielded on the TR-2 aircraft. In July 2024, a year after the planned delivery, the JPO, Services, and Lockheed Martin reached an agreement to allow the Services to start accepting TR-3 aircraft with the truncated software lacking these TR-2 capabilities. The U.S. Air Force accepted the first two TR-3 Lot 15 aircraft later that month, with an interim test software build of the truncated version, designated 40R01.351, that would allow pilots in the field to use the aircraft for training. According to the JPO, as of the end of FY24, the program had delivered 41 TR-3 aircraft. The limitations in terms of combat capability of these aircraft are not known, nor is the timeline on which the previously fielded capabilities (on the TR-2 aircraft) will be tested and provided to the newly delivered TR-3 aircraft.

The decision to proceed into full-rate production occurred after nearly thirteen years and fifteen lots of aircraft production at the prime contractor facility. Over that time span, the program office monitored key production and manufacturing metrics, including the scrap, rework, and repair hours per aircraft for each lot (due to problems identified during manufacturing and assembly) and quality escapes (i.e., problems that should have been identified and corrected during the check-out and acceptance process for new aircraft). According to JPO reports, efforts to improve production quality resulted in a 47 percent reduction in the time associated with scrap, rework, and repair and a 63 percent reduction in the observed number of quality escapes from the production line, between 2016 and 2023. While these efforts continue, quality escapes from the production line are still being discovered in the field. In one example, a U.S. Marine Corps fighter squadron in California discovered a series of quality escapes with a number of F-35C aircraft delivered to the unit in FY24.

A separate F-35 Overarching Block 4 TEMP and associated annexes govern the conduct of Block 4 FOT&E. Block 4 includes DT and OT with aircraft in the TR-2 configuration. For these aircraft, the program has designated flight software using a 30-series designation (i.e., 30RXX for development and flight testing software iterations, and 30PXX for final production and fielding). Block 4 also includes DT and OT with aircraft in the TR-3 configuration. The software for these aircraft is designated with a 40-series nomenclature (i.e., 40RXX or 40PXX). DOT&E approved the F-35 Overarching Block 4 TEMP and Increment 1 Annex in May 2020. The Increment 1 Annex covered the Block 4 DT and OT of software versions 30P03 through 30P06, which were completed in FY21. Increment 2 Annexes, which cover Block 4 software versions 30P07, 30P08, and 40P01, and their associated hardware enablers, including the transition from TR-2- to TR-3-equipped aircraft in the production line, were approved in October and December 2022. The Increment 3 Annexes, which cover Block 4 software versions 40P02, 40P03, and 41P01, and their associated hardware enablers were approved by DOT&E in November 2024.

At the time of this report, the program is undergoing a major review of sequencing and prioritizing the series of additional new capabilities through the establishment of the Block 4 subprogram. DOT&E expects the results of this effort will likely affect schedules and resources for the OT activities covered by the F-35 Overarching Block 4 TEMP and its annexes. The program office must adjust timelines that support OT of the capabilities as they become defined within the Block 4 subprogram. These timelines must prioritize aircraft capability, modifications, and instrumentation — to include Open-Air Battle Shaping (OABS) — so eight fully capable aircraft are available for dedicated operational test trials during the OT periods.

» MAJOR CONTRACTORS:

- Lockheed Martin Aeronautics Company – Fort Worth, Texas
- Pratt & Whitney, a subsidiary of RTX – East Hartford, Connecticut

TEST ADEQUACY

» BLOCK 4 OPEN-AIR TESTING

During FY24, the U.S. Operational Test Team transitioned from being a U.S.-only team to the United Operational Test Team (UOTT), absorbing test teams from the United Kingdom and Australia to the F-35 OT enterprise.

Block 4, TR-2, 30-Series Open-Air Testing

In February 2023, DOT&E approved only four weapon events in the UOTT's 30R08 test plan, due to the lack of readiness of key requirements, such as the final version of software, flight test instrumentation, aircraft modifications, and OABS, the latter being required to complete dedicated operational test (DOT) scenarios. By October 2023, readiness requirements improved, allowing DOT&E to approve some additional test events in the plan. These included four Close Air Support and four Defensive Counter Air DOTs, along with seven additional weapons events (three bomb and four missile events). The remaining test events will be approved by DOT&E when readiness requirements are met.

The UOTT 30R08 OT plan, signed in January 2023, governs the open-air OT for all units assigned to the UOTT. The plan includes a spectrum of open-air test events that can be conducted with the incremental versions of the software. Capability test events (CTEs) are events that may be conducted with early, less mature versions of the software and are designed to characterize the performance of new capabilities or verify corrections to deficiencies identified during previous testing. CTEs are flown as an extension of the development effort, particularly for this later build of 30-series software for the TR-2-configured aircraft, since most of the current DT fleet have been upgraded to the TR-3 configuration.

Mission area trials (MATs) may also be flown with early versions of software and are normally conducted as a part of large force joint exercises to collect data from scenarios more operationally representative than the tightly controlled, smaller scenarios flown in the CTEs. MATs provide the added benefit of evaluating interoperability with other air warfare platforms. DOT missions are events that require full mission-level evaluations, assessing F-35 operational effectiveness in terms of lethality and survivability in mission scenarios, like those flown during IOT&E. They are generally flown with the final version of software in the series, which is the version that will be delivered to field units.

DOTs include variations in operational conditions, such as the number of red and blue airborne forces or the number and type of ground threat systems. Finally, dedicated weapon events, both captive carry (weapon test article flown, but not released) and live-fire events, are included in the test plan. The UOTT can complete CTE and MAT events from the test plan without DOT&E approval, but the weapons events and DOTs must be approved by DOT&E, to ensure test readiness and adequacy.

Prior to February 2024, the UOTT completed four DOT&E-approved Close Air Support DOT events, which DOT&E did not observe. The UOTT conducted AIM-120 and AIM-9X weapons events, which DOT&E observed. In February 2024, the UOTT issued a "stop test" of the 30R08 software, citing two critical Category I deficiencies and overall poor software stability performance, which prevented additional test events from being approved. The UOTT also conducted regression testing of previously approved AIM-120 events after the stop test was issued. The UOTT was not able to complete any additional weapons events or DOT events due to poor software stability.

Block 4, TR-3, 40-Series Open-Air Testing

The UOTT began making plans for OT of the first TR-3 production configuration, with software version 40R02, but the program's DT effort with the TR-3 aircraft and associated software remained significantly behind schedule throughout FY24. Aircraft modifications, flight test instrumentation, OABS capabilities, and stable software will all be required before dedicated operational testing can begin on the TR-3 aircraft with the capabilities already fielded on the TR-2 aircraft. Given the program constraints on contracting and associated timelines, DOT&E estimates that DOTs of TR-3 aircraft will likely not begin in earnest until mid to late FY26, two years after the aircraft began being delivered to field units. If readiness criteria involving modifications, instrumentation, OABS and software that is adequately mature and stable are met sooner, operational testing may be able to start earlier.

» BLOCK 4 –JOINT SIMULATION ENVIRONMENT (JSE)

Following the completion of F-35 IOT&E test trials in the JSE at Patuxent River Naval Air Station, Maryland, program management of the JSE moved to an organization outside of the JPO. A joint U.S. Air Force and Navy JSE enterprise now manages the JSE environment, services, and threat models. The F-35 JPO continues to manage the F-35 model updates that run inside the environment – referred to as the F-35-in-a-box (FIAB). The next iteration of OT of the F-35 in the JSE will be based on the capabilities fielded with 30R08 software, in TR-2 aircraft.

To support these OT events, the JPO began early 30S08 software integration (the 30S08 is 30R08-equivalent software for the FIAB) in the JSE at Patuxent River in August 2024, with the goal of having a working (i.e., usable for training) 30S08 FIAB late in FY25. Development and integration of 30S08 is planned to continue through FY25, and the verification, validation, and accreditation process leading to formal accreditation is planned for completion in FY26. The UOTT plans to conduct 30R08 mission-level test trials once the JSE has been accredited for OT, likely no earlier than mid to late FY26.

» SUITABILITY TESTING

DOT&E approved the latest iteration of the UOTT's Annual F-35 Modernization Block 4 Suitability Test Plan in October 2023. Since the plan did not comply with TEMP requirements, DOT&E directed the UOTT to continue dynamic radar cross-section measurements of two OT aircraft per variant, in accordance with the TEMP. To date, no additional dynamic measurement testing has been done on any variant, in violation of TEMP requirements and DOT&E direction.

In late July and early August 2024, the UOTT conducted the remaining events to complete testing of Autonomic Logistics Information System (ALIS) disconnected contingency operations, under a test plan approved by DOT&E in August 2023. DOT&E observed the events. This was a limited test wherein ALIS components were disconnected for a period of time under different contingency operating scenarios. The purpose of the testing was to assess overall effects on flight operations when connections within the ALIS architecture become unavailable, whether through intended actions or other incident that results in denial of service. The UOTT conducted the first scenarios in August 2023, where the Standard Operating Unit (SOU) was disconnected from flight line operations. The scenarios tested in July through early August 2024 included operations where the SOU was disconnected from the Central Point of Entry (CPE). The CPE is the hub that provides connectivity to the higher-level Autonomic Logistics Operating Unit, which interfaces with Lockheed Martin's global sustainment system.

ALIS and Operational Data Integrated Network (ODIN)

The transition from ALIS to ODIN continues to undergo changes in process and in capability. The JPO originally expected to fully containerize ALIS software in a single update referred to as "lift and shift," without adding capability, to transfer it to the new ODIN hardware. Instead, the program is now planning to gradually containerize ALIS software features over many smaller updates on a six-month release cadence, while concurrently adding new capabilities long demanded by operators.

While developing this first six-month software release for ODIN, designated Mx-P.01, the program is concurrently fielding a new version of ALIS and deploying updated ODIN hardware. The current (and planned-to-be final) version of ALIS, called 22.Q4, started fielding in June 2024. It is a major release that includes modernized operating systems and infrastructure applications such as database management software.

It is designed to address critical obsolescence and cybersecurity issues. Given the unusual size of the upgrade, the program projects ALIS 22.Q4 roll-out will not complete to all fielded units until between July and November 2025.

The JPO plans to freeze the content for Mx-P.01 in October 2024, followed by contractor and government-led DT, to support a release in 4QFY25. Each subsequent six-month release is expected to have an 18-month development timeframe, leading to multiple, serial versions in development simultaneously. The second expected six-month release, Mx-P.02, started development in 4QFY24 for fielding in 2QFY26. Mx-P.02 is planned to have improved disconnected operations performance, and cybersecurity hardening of the hypervisors used to host virtualized operating systems. The third release, Mx-P.03, is planned for fielding in 4QFY26. The program expects it to feature a significant expansion of containerized features, as well as additional cybersecurity changes.

ODIN hardware continues to proliferate in the field, and new ODIN hardware is in development. The first tranche of ODIN hardware is the unit-level ODIN Base Kit-Unclassified (OBK-U). The OBK-U is the replacement for the legacy unclassified ALIS unit-level hardware for the squadron kit, the SOU version 2. The OBK-U is smaller, faster, and can better facilitate operating system virtualization. The program anticipates complete replacement of all ALIS SOU version 2 instances with an OBK-U by the end of FY25. The program is also developing the classified, squadron-level adjunct for low-observable (LO) maintenance, the OBK-LO, as well as an upgraded version of the unclassified country-level CPE known as the ODIN Country Kit (OCK-U).

» CYBER SURVIVABILITY TESTING

In FY24, the UOTT cyber team completed a cyber survivability assessment of supply chain refurbishment practices, a high interest area for the DoD and the F-35 program. The UOTT cyber team also completed a risk reduction event to support testing of a Cross-Domain Solution in early FY25. They also observed the ALIS-disconnected contingency operations, discussed above, to assess cybersecurity implications. The UOTT started a cooperative vulnerability and penetration assessment and an adversarial assessment of the U.S. Reprogramming Laboratory (USRL), which provides mission data for the F-35. The assessments of the USRL will continue into FY25. The UOTT also attempted an assessment of the Multifunction Advanced Data Link but did not complete it due to test asset materiel condition issues.

All these cyber survivability test activities were conducted in accordance with DOT&E-approved plans and observed by DOT&E. The UOTT cyber team also participated in a Mission Based Cyber Risk Assessment (MBCRA) on an aircraft in a Lot 18, TR-3 configuration, which focused on select air vehicle management and mission systems. The effort was chartered and led by the JPO with developmental test team support to prioritize cyber survivability test opportunities for these Block 4 aircraft.

Additional cyber survivability testing planned for FY24 included Small Diameter Bomb Increment II interfaces, Variable Message Format communications protocol, and initial assessments of radar vulnerabilities – all of which were deferred into FY25 due to test team readiness and asset availability issues. DOT&E has required operational cyber survivability testing of each major update of ALIS software fielded and will do so for ODIN in the future. To date, the program has supported this requirement.

Aircraft made available for cyber survivability testing have been permanently grounded assets that are also used for software development and thus limit testing due to the potentially disruptive nature of cyber tests. More robust and representative aircraft cyber tests are needed, which will involve Service and JPO programmatic investment in requisite hardware- and software-in-the-loop capabilities. To address this need, the JPO plans to make another retired TR-2 mission systems DT aircraft available for dedicated cyber survivability testing in FY25.

PERFORMANCE

» EFFECTIVENESS

This Annual Report does not include effectiveness results contained in the DOT&E classified F-35 combined IOT&E and LFT&E report published in February 2024. That report provided an independent assessment of the overall mission capability of the F-35 in the Block 3F configuration in terms of its operational effectiveness, suitability, and survivability. The report included a separate annex that provided an assessment of F-35 Block 4 operational testing which occurred following IOT&E. Effectiveness details from the annex are not included in this report.

Block 4, TR-2, 30-Series Development

TThe F-35 program has shown no improvement in meeting schedule and performance timelines for developing and testing software designed to address deficiencies and add new capabilities. In fact, the program has shown it cannot simultaneously work out solutions to deficient 30-series software to improve capability of fielded systems that have the TR-2 avionics architecture while developing the 40-series software required to run on the new TR-3 architecture. Challenges added with the TR-3 avionics upgrades, both in development and testing, have caused additional delays to the planned schedules for delivering capabilities in Block 4 for the aircraft in the TR-2 configuration.

Table 1 below compares the development-to-fielding timelines for the latest three versions of 30-series software, as well as the number of software iterations and whether each software version delivered with the full capabilities initially planned for it. Both 30R06 and 30R08 development took longer than planned and more iterations of software to address discoveries and deficiencies. Both 30R07 and 30R08 have or will deliver with less than their planned capabilities. The program has not decided whether it will add another 30-series software version beyond 30R08. The overall result has been no significant 30-series (TR-2) capability improvement through the latest software versions, and the 40-series (TR-3) software getting further behind and amassing new deficiencies.

Table 1. Comparison of Development Parameters of the Latest Software Versions

Comparison Parameters	Production Software Version		
	30P06	30P07	30P08
Developmental software iterations planned	Four: 30R06.01, .02, .03, .04	Three: 30R07.01, .02, .03	Three: 30R08.01, .02, .03
Developmental software iterations delivered to flight test	Seven: 30R06.01, .02, .03, .031, .04, .041, .042	Eight: 30R07.01, .02, .03, .031, .033, .04, .041, .045	Ten (at least): 30R08.01, .02, .03, .04, .041, .051, .061, .062, .063, .900
First DT flight	August 2020	April 2021	December 2021
First OT flight	October 2020	January 2022	March 2022
Planned release to the field	April 2021	May 2022	March 2023
Actual release to the field	September 2021	May 2022	TBD
Span from 1st DT flight to field release	13 months	13 months	TBD
All planned capabilities delivered?	Yes	No	TBD

Block 4, TR-2, 30-Series Open-Air OT

Due to the lack of adequate testing on the 30R08 software, DOT&E is unable to assess its operational effectiveness. The OT teams have flown with immature versions of the 30R08 software to support DT assessments of capabilities and have participated in large force exercises to assess integration and interoperability with other aircraft. However, these tests have not been adequate to evaluate effectiveness of the 30R08 capabilities in mission-level scenarios. The testing that the teams have been able to accomplish continues to lead to discovery of deficiencies. From March through May 2024, the UOTT reported four Category 1 deficiencies against capabilities in the 30R08 software, many of which were against capabilities that were working in previous versions of software, an indication of insufficient integration and regression testing.

Block 4, TR-3, 40-Series Development

Although the program and Services have begun accepting aircraft off the production line, as well as those coming out of long-term parking over the last year, no OT has been completed to date on the TR-3 aircraft in a production-representative configuration.

» SUITABILITY

Reliability, Maintainability, and Availability

This annual report provides an analysis of the historical RM&A performance of the U.S. F-35 fleet in the Block 3 (i.e., the TR-2) configuration. This analysis is an update to that which was included in the annex to the DOT&E classified F-35 combined IOT&E and LFT&E report published in February 2024. The operational suitability of the F-35 fleet continues to fall short of Service expectations and the requirements defined in F-35 Modernization Block 4 CDD and the JSF Operational Requirements Document (ORD). Since the CDD does not change the original reliability and maintainability requirements, the historical trend analyses of reliability and maintainability metrics of the fleet compare historical performance against ORD requirements.

Historical trend data show that, despite reliability improvements initiated by the program, improving and sustaining improvement in aircraft suitability metrics is difficult to achieve. The following assessment covers reliability and maintainability trends for the period from FY15 through FY23, and availability trends for the period from FY15 through FY24. Data for reliability and maintainability include the records of all maintenance activity and undergo an adjudication process by the government and contractor teams, a process which creates a lag in publishing those data.

As of the end of FY24, Lockheed Martin had produced and delivered 695 aircraft to the U.S. Services. Prior to starting the delivery of TR-3 configured aircraft out of long-term parking in July, 649 aircraft had been delivered to the U.S. Services. These numbers, which provide the basis of analyses contained in this section of the report, do not include any aircraft assigned to dedicated DT.

Availability Trends

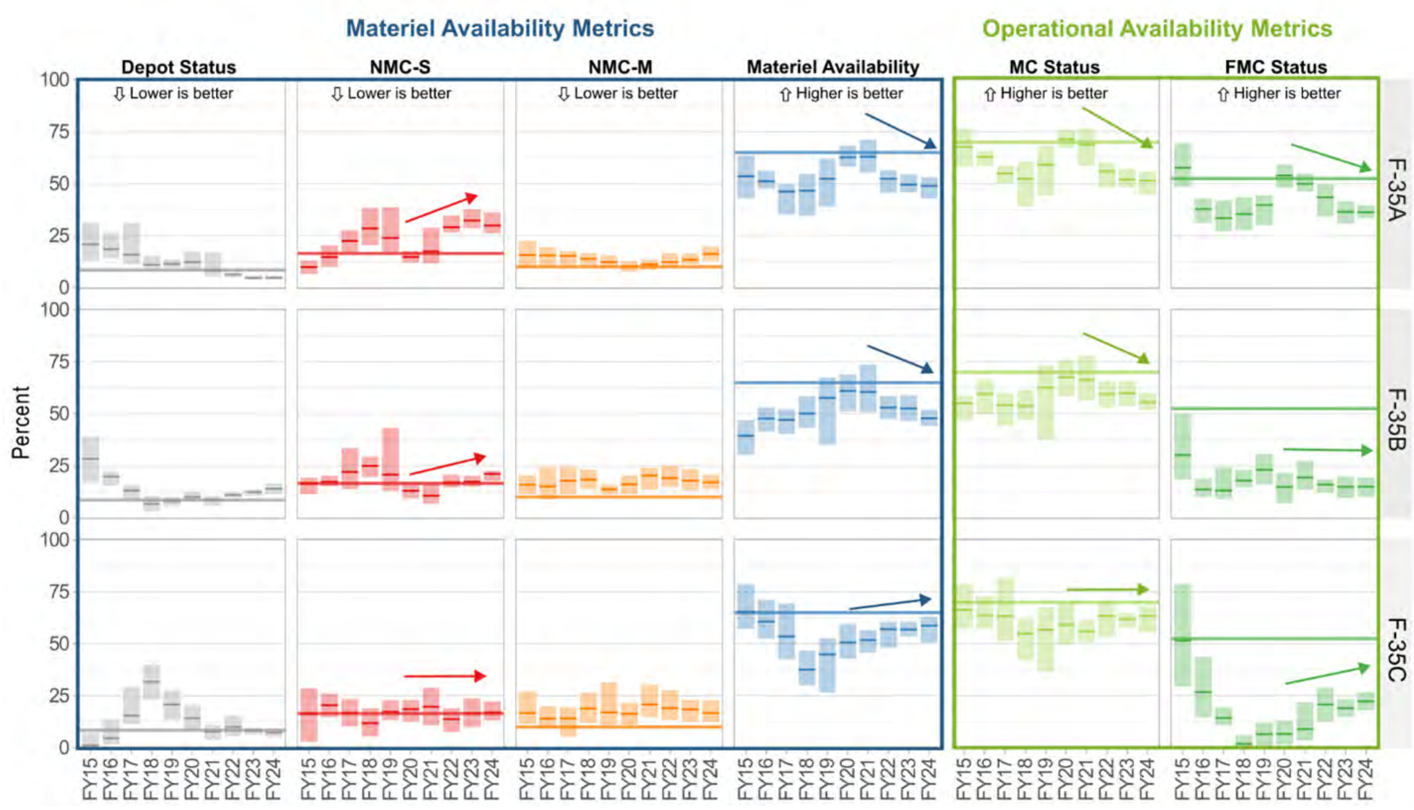
Operational availability is measured in terms of the Mission Capable (MC) rate, of which the Fully Mission Capable (FMC) rate is a subset. As shown in Figure 1 below, these MC and FMC metrics are below, and well below, the Services' target values, respectively. The MC rate indicates the proportion of all fielded aircraft not in depot that are capable of flying at least one mission of the overall F-35 mission set. The FMC rate reports the proportion that can fly all F-35 mission sets, representing a more accurate assessment of overall combat readiness. Materiel availability is the percentage of all aircraft, including those in the depot, that are in an MC status. Materiel availability is generally considered a clearer representation of the overall health of the fleet of aircraft.

Aircraft that are not materially available (i.e., not able to fly) are designated in one of three status categories: Depot (i.e., in the depot for modifications or repairs beyond the capability of unit level squadrons), Not Mission Capable for Supply (NMC-S), or Not Mission Capable for Maintenance (NMC-M). Figure 1 shows the annual average value (dark colored bar) for each metric from FY15 through FY24, as reported by the Services. Minimum and maximum monthly values in a given fiscal year are indicated by longer, lighter colored bars, and the target values are indicated by the horizontal lines. Trend arrows have been added to the plots of NMC-S and operational availability metrics to guide the reader and to highlight the trends discussed below.

Following FY19, there was a notable increase in the operational availability of the F- 35A and F-35B and a corresponding decrease in the proportion of aircraft that were down due to supply (i.e., waiting for parts). During the same time period, the proportion of aircraft that were down for maintenance remained relatively flat. Since FY19, F-35C operational availability has had more year-to-year variability but remained below the target values. There was more variability in the proportion of aircraft that were down due to supply than aircraft that were down for maintenance. The trends suggest that the most impactful near-term option for improving aircraft availability is to increase the pool of available spares – either by purchasing more or by maximizing depot capacity to repair broken parts and return them to the spares pool. Additionally, the JPO is actively working to address degraders that negatively affect aircraft availability.

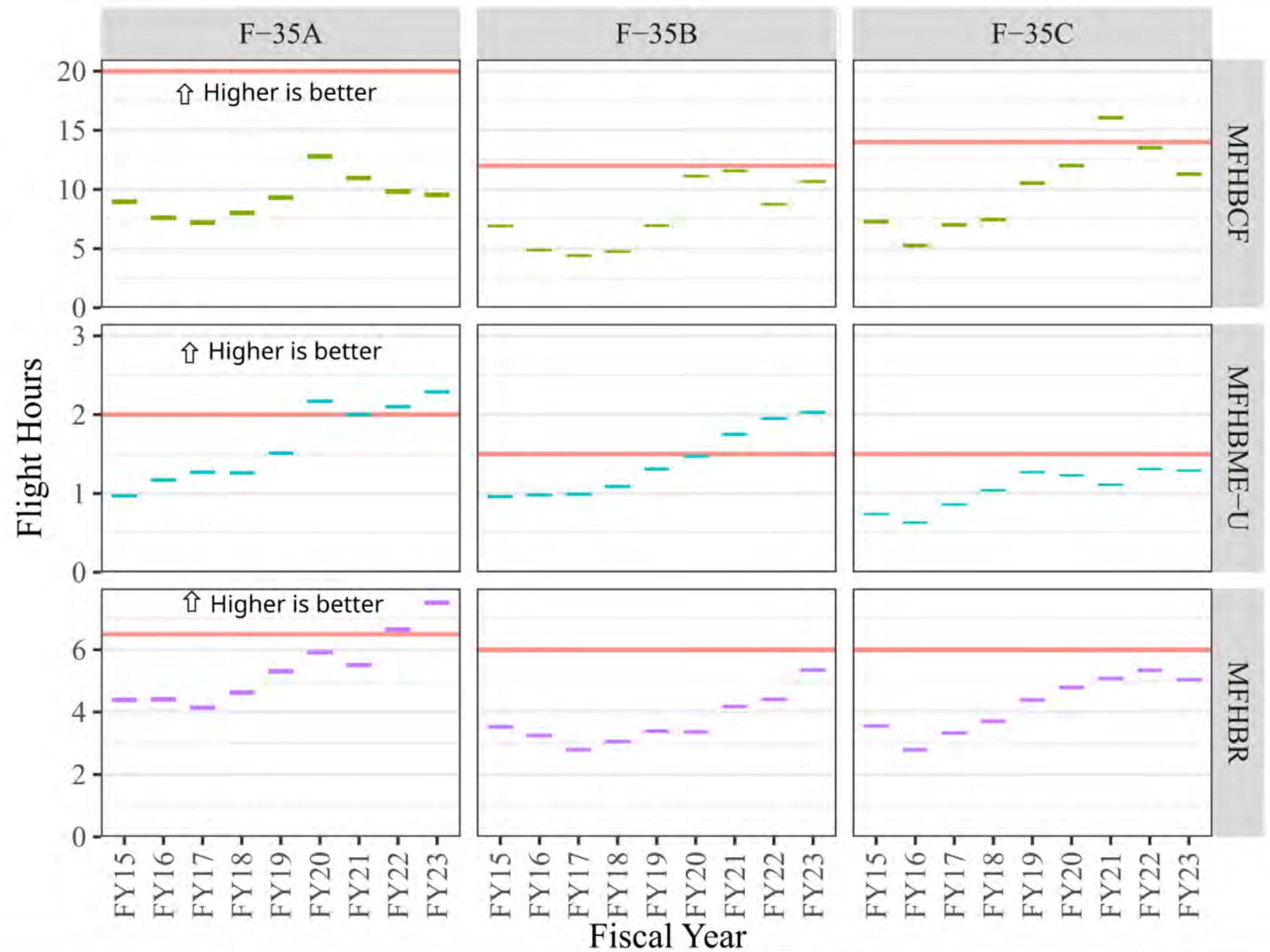
Reliability Trends

The U.S. F-35 fleet remained below the requirements defined in the JSF ORD for some overall



Acronyms: FMC – Fully Mission Capable; MC – Mission Capable; NMC-M – Not Mission Capable for Maintenance; NMC-S – Not Mission Capable due to Supply

Figure 1. F-35 Availability Metrics, U.S. Fleet (FY15 – FY24)



Acronyms: MFHBCF – Mean Flight Hours Between Critical Failures; MFHBME-U – Mean Flight Hours Between Maintenance Events - Unscheduled; MFHBR – Mean Flight Hours Between Removals

Figure 2. F-35 Reliability Metrics, U.S. Fleet (FY15 – FY23)

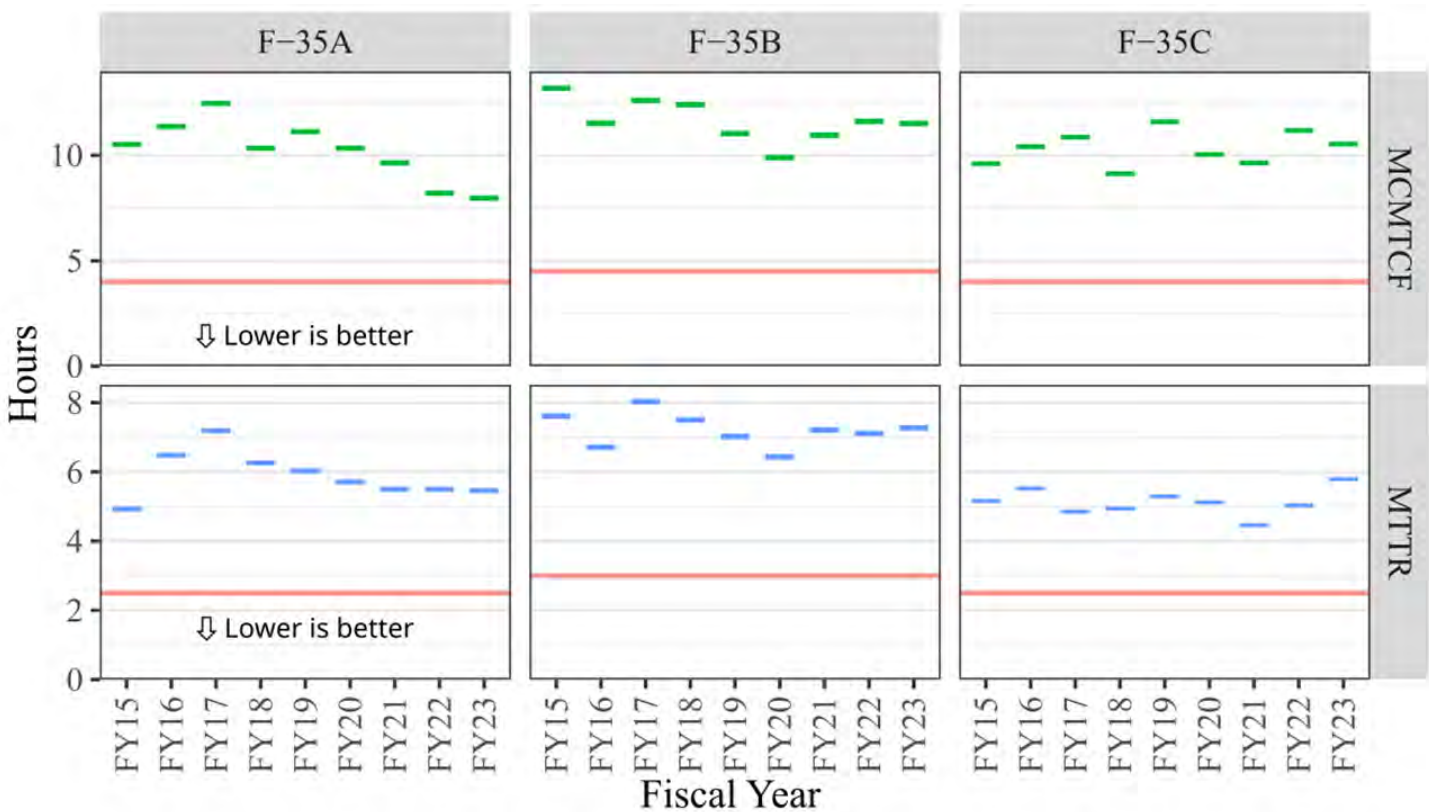
reliability metrics as shown in Figure 2, based on adjudicated data reported by the JPO. Higher numbers reflect better performance and a more reliable system. Since FY15, there was some reliability improvement with increased variability. In FY23, the F-35A met two, the F-35B met one, and the F-35C met none of the three reliability requirements.

In FY23, the F-35A was significantly below, and the F-35B and F-35C were slightly below, the threshold requirement for time between critical failures. Mean flight hours between critical failures (MFHBCF) includes all failures that render the aircraft unsafe to fly, along with any equipment failures that would prevent the completion of any defined F-35 mission. It includes failures discovered in the air and on the ground. The MFHBCF for the F-35A peaked in FY20 and has declined ever since, although FY23 was only slightly worse than FY22, possibly leveling off in the worsening trend. The F-35B had its highest MFHBCF in FY21, declined significantly in FY22, but then regained some ground in FY23 while remaining below requirement. It has approached, but never surpassed its requirement. The F-35C had shown year-over-year improvement since FY16, peaking above its requirement in FY21, but then declining in both FY22 and FY23.

In FY23, the F-35A was above, and the F-35B and the F-35C were below, the threshold requirements for removals. Mean flight hours between removal (MFHBR) indicates the degree of necessary logistical support and is frequently used in determining associated costs. MFHBR includes any removal of an item from the aircraft for replacement, except for consumables like fasteners and tires. While all removals are actions triggered by the need to conduct maintenance, not all removed components actually failed. Some removed components are later determined to have not failed when tested at the repair site – which can be caused by many factors including training issues, incorrect aircraft diagnostics, or maintainer error, amongst others. Other components can be removed due to excessive signs of wear before a failure, such as worn tires. All variants have generally shown steady improvement in MFHBR across most years since around FY16, but in FY23, the F-35C had a slightly worse MFHBR than in FY22.

In FY23, the F-35A and F-35B were above, and the F-35C was below, the threshold requirements for unscheduled maintenance events. Mean flight hours between maintenance events - unscheduled (MFHBME-U) is a reliability metric for evaluating maintenance workload due to unplanned maintenance. Maintenance events are either scheduled (e.g., inspections or planned part replacements) or unscheduled (e.g., failure remedies, troubleshooting, replacing worn parts such as tires). The F-35A and F-35B have exhibited year-over-year improvement in MFHBME-U since FY19, whereas the F-35C improved substantially prior to FY19 but has plateaued since then.

The overall trends in reliability of the U.S. F-35 fleet from FY15 through FY23 are shown in Figure 2. Since only partial reliability data from FY24 were available due to the lag in adjudicating maintenance records, they were



Acronyms: MCMTCF – Mean Corrective Maintenance Time for Critical Failures; MTTR – Mean Time to Repair

Figure 3. F-35 Maintainability Metrics, U.S. Fleet (FY15 – FY23)

not included in this figure. This figure shows yearly average value for each metric for a given fiscal year, and the horizontal line indicates the threshold requirement. MFHBME-U and MFHBR both show more reliability improvement, with some metrics above requirement, but little apparent effect on operational availability rates. For reliability metrics, higher values are better.

Maintainability Trends

The maintainability metrics for the U.S. F-35 fleet from FY15 through FY23 are shown in Figure 3, based on adjudicated data reported by the JPO. Since only partial maintainability data from FY24 were available due to the lag in adjudicating maintenance records, they were not included in this figure. This figure shows yearly average values for each metric for a given fiscal year, and the horizontal line indicates the threshold requirement. For maintainability metrics, lower values are better, indicating shorter average maintenance durations.

For all variants, the average maintenance durations for the U.S. F-35 fleet are longer than the ORD requirements. There has been little improvement in these maintainability metrics since FY15. As of February 2024, no variant met the maintainability requirements.

The mean corrective maintenance time for critical failures (MCMTCF) remains almost double or more than the threshold requirement. No variant showed significant improvement over the period, except for MCMTCF for the F-35A, which remains at nearly twice the required value. This metric measures the active maintenance touch labor time and cure times associated with repairs to LO materials required to correct only the subset of failures that prevent the F-35 from being able to perform a specific mission. It indicates the average time for maintainers to return an aircraft from Not Mission Capable to MC status.

The trend is similar for the mean time to repair (MTTR), the average time for all unscheduled maintenance actions, including cure times associated with repairs to LO materials. This metric includes only active maintenance time and is a general indicator of the ease and timeliness of repair.

Mission Reliability and Software Performance

F-35 aircraft mission systems instabilities can degrade mission performance and may require a pilot-initiated reset of mission systems in-flight, which could have severe consequences during combat, affecting overall mission reliability. ALIS does not currently have the capability to automatically log these events in the Computerized Maintenance Management System (CMMS). While pilots can manually document instability events, this occurs infrequently as the process is cumbersome and Service policy is to rely on an ALIS automated process. The data in CMMS are used to report reliability and maintainability metrics. Software instability issues are not reflected in the metrics and are historically underreported by flight crews. Currently, only proprietary tools used by contractor field-service engineers can identify pilot-initiated reset events. DOT&E recommends, to improve F-35 aircraft mission systems stability, that ODIN include the capability to automatically document pilot-initiated resets of mission systems.

ALIS Disconnected Operations

Data from the testing described in the Test Adequacy section above were under analyses at the time of this report.

» SURVIVABILITY

Results from the cyber survivability assessment of the supply chain refurbishment practices were under review at the time of this report.

Multiple ALIS cyber survivability deficiency reports were created in FY24 based on the FY23 testing, with an additional finding still under evaluation. Several deficiency reports were closed. Many cyber survivability deficiencies remain across the F-35 program. To address the deficiencies, the JPO invested in cyber mitigations associated with recent UOTT testing, and key test findings are being tracked to closure by the Authorizing Official for ALIS and ODIN.

The F-35 JPO is using Development Security Operations (DevSecOps) and Agile software methods to advance frequent software updates to the field in support of the ODIN path forward. The Block 4 30RXX and 40RXX software version development process is also providing more frequent operational flight profile software updates to the combat forces than during the system development and demonstration phase. An increased frequency of new software deployments is stressing the capacity of cyber test teams to thoroughly evaluate each update. Under these new constructs, the importance of cyber survivability testing of the software development environments will also increase – further stressing the cyber test teams' capacity – and will result in the fielding of capabilities not fully tested for cyber survivability until DoD-wide cyber test team capacity expands.

Candidates for cyber survivability testing are continually assessed for inclusion in the cyber test roadmap. Additionally, once cyber effects are adequately and systematically characterized – through a validation process and informed by intelligence centers cyber threat assessments – emulation during mission rehearsals in the JSE, or as appropriate in open-air exercises, will be key to assessing potential mission consequences from cyber exploits. Further insights into air vehicle (AV) priority testing will be forthcoming from the imminent completion of a first-phase Mission-Based Cyber Risk Assessment that commenced in 4QFY22, and from the follow-on second phase that started in 4QFY24.

RECOMMENDATIONS

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

1. Continue preparations for required F-35 FOT&E in the JSE beginning with the 30R08 capability release.
2. Ensure programming, funding, and contracting are in place to modify sufficient OT aircraft to meet operational test requirements, including 4-ship test formations for each variant, with the appropriate capabilities, life limit, and instrumentation, including OABS requirements, in time to accomplish DOT.
3. As recommended in the FY22 and FY23 Annual Reports, continue to pursue maintenance system improvements, training, and tools; especially for common processes distributed among NMC-M drivers, such as LO repairs, adhesive cure times for attaching hardware such as nutplates, and spares posture for those critical items most in demand.
4. As recommended in the FY22 and FY23 Annual Reports, continue to accomplish rigorous testing of data integrity while the transition from ALIS to ODIN continues, as this will be critical to the success of ALIS to ODIN while also supporting operational unit day-to-day activities.
5. As recommended in the FY22 and FY23 Annual Reports, continue to ensure both DT and OT for ALIS and ODIN are adequately resourced to reduce the high risk associated with fielding an immature and inadequately tested replacement.
6. As recommended in the FY22 and FY23 Annual Reports, conduct more in-depth cyber survivability testing of the AV, ALIS/ODIN, training systems, and eventually JSE; provide dedicated hardware- and software-in-the-loop AV cyber-test assets that can be used for the full extent of cyber testing; introduce the ability for JSE to emulate cyber effects during mission rehearsals once cyber effects have been characterized and validated.
7. As recommended in the FY22 and FY23 Annual Reports, continue to correct program-wide deficiencies identified during cyber survivability testing in a timely manner and verify corrections within ALIS prior to rehosting ALIS software on ODIN.
8. As recommended in the FY22 and FY23 Annual Reports, develop and routinely report software sustainment and stability metrics that show how well the program's overall software development capability for the AV and logistics sustainment system is progressing. In particular, incorporate the ability of the aircraft's prognostics health management to detect pilot-initiated resets

of mission critical systems in flight and produce records in the Computerized Maintenance Management System to more accurately track AV system stability.

The UOTT should:

1. Work with the U.S. Services to resume dynamic radar cross-section measurements of two OT aircraft per variant, in accordance with the TEMP.

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

In FY23, the Global Command & Control System – Joint (GCCS-J) Program Management Office (PMO) fielded GCCS-J version v6.1.0.0, delivering a significant infrastructure upgrade to the GCCS-J program. However, v6.1.0.0 did not have all of the capabilities of the fielded version, v6.0.1.30. GCCS-J v6.1.0.4, which has all of the capabilities of v6.0.1.30, was not ready for operational test in FY24. Therefore, the FOT&E of v6.1.0.4 will be reported in 3QFY25 – a one-year slip from what DOT&E reported in the FY23 Annual Report.

SYSTEM DESCRIPTION

GCCS-J is a software-based system with commercial off-the-shelf and government off-the-shelf software and is highly modular, allowing customization of the deployed configuration to fit each deployed sites' requirements. The GCCS-J system uses procedures, standards, and interfaces that provide an integrated, near real-time picture of the battlespace that is necessary to conduct joint and multi-national operations.

MISSION

Joint commanders use GCCS-J to accomplish command and control by:

- Displaying geographic track information integrated with available intelligence and environmental information to provide the user a fused battlespace picture;
- Providing integrated imagery and intelligence capabilities (e.g., battlespace views and other relevant intelligence) into the common operational picture (COP); and
- Providing a missile warning and tracking capability.

PROGRAM

In FY23, the GCCS-J PMO fielded version v6.1.0.0 as a significant upgrade to the existing fielded version of v6.0.1.30. However, v6.1.0.0 did not capture all of the capabilities of the v6.0.1.30, and due to delays in command transitions to v6.1.0.4, FOT&E is planned to be completed in 1QFY25. DOT&E will publish an FOT&E report in 3QFY25. User sites choose when to upgrade GCCS-J for use in military operations. During operational testing, users identified impactful improvements that will be added into future GCCS-J development requirements. As the PMO continues software development, GCCS-J will field user-identified capabilities through the Development Security Operations (DevSecOps) process as part of their Agile software development framework.

» MAJOR CONTRACTORS

- Northrop Grumman Systems Corporation – Newport News, Virginia
- NextGen Federal Systems – Annapolis Junction, Maryland

TEST ADEQUACY

In FY23, the Joint Interoperability Test Command (JITC) conducted one operational test of GCCS-J v6.1.0.0. The test was conducted in accordance with DOT&E guidance and observed by DOT&E and included representative hardware, software, real-world data, and operational end users that exercised system administration, COP, and intelligence user mission tasks. Testing focused on the capabilities and interfaces available at U.S. Central Command (USCENTCOM) and U.S. Southern Command (USSOUTHCOM). Test cases were developed with direct input from users at both combatant commands. In 1QFY25, FOT&E is planned to be conducted with commands at U.S. Army Pacific and U.S. Marine Corps Forces, Pacific, with site-specific test cases as these commands migrate to v6.1.0.4.

The GCCS-J integrated test environment does not currently capture the mission configurations associated with each combatant command and other critical sites. GCCS-J test strategies need to be developed to encompass the agile nature of the product and varying operational site configurations, to inform updates to the TEMP and Agile Operational Test Plan (AOTP). Moreover, the TEMP update should detail operational cyber survivability tests that include cooperative vulnerability and penetration assessments (CVPAs) followed by adversarial assessments (AAs).

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

DOT&E will continue to assess data from the GCCS-J FOT&E of v6.1.0.4, which is scheduled to complete in FY25. DOT&E will report on operational effectiveness and suitability upon completion of FOT&E.

» SURVIVABILITY

JITC has not conducted operational cyber survivability testing of v6.1.0.4 and should conduct a CVPA and an AA to complete the testing necessary to support an evaluation of cyber survivability. DOT&E will report on cyber survivability upon completion of FOT&E.

RECOMMENDATIONS

Defense Information Systems Agency (DISA) should:

1. Develop test strategies to encompass the agile nature and varying operational site configurations to inform the updates to the TEMP and AOTP, which must be submitted to DOT&E for approval, as discussed in the FY22 and FY23 Annual Reports.
2. Conduct a CVPA and an AA to complete testing necessary to support an evaluation of cyber survivability, as discussed in the FY23 Annual Report.

Joint Biological Tactical Detection System (JBTDS)

DOT&E approved the Joint Biological Tactical Detection (JBTDS) Milestone C (MS C) TEMP in September 2023. In FY24, the program office completed a portion of the test matrix from the DOT&E-approved test plan for identifier testing. Identifier testing is scheduled to be complete by 2QFY25. The Army conducted a multi-Service operational test and evaluation (MOT&E) for the biological warfare agent (BWA) identifier in September 2024, to support a critical operational need for that JBTDS component. DOT&E will publish a classified MOT&E report in 3QFY25 to assess the BWA identifier's operational effectiveness, suitability, and survivability. The full system MOT&E is scheduled for 4QFY25. DOT&E will publish another MOT&E report on the JBTDS as a whole system to support the full-rate production decision in 1QFY26.

SYSTEM DESCRIPTION

The JBTDS consists of an integrated man-portable BWA aerosol detector and sample collector, a base station, a meteorological station, a GPS receiver, a sample extraction kit, and a handheld BWA identifier with consumable assays. 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.

MISSION

Army, Marine Corps, and Navy units will deploy JBTDS during major combat, stability, and strategic deterrence operations where an adversary's employment of BWAs could severely disrupt military operations or cause hazardous exposure to warfighters or civilians. Service units equipped with the JBTDS will conduct biological surveillance missions to detect the presence of, collect samples, identify, and warn forces of the BWA threat. The JBTDS is intended to support commanders' force protection actions, support medical planning, and provide information to enable consequence management. The Special Operations Command will employ the JBTDS identifier to identify BWA in samples to support intelligence gathering and forensics analyses.

PROGRAM

JBTDS is a joint Acquisition Category II program which was authorized in August 2023 to enter the production and deployment phase of acquisition. DOT&E approved the MS C TEMP in September 2023. The Marine Corps, National Guard Bureau, and U.S. Special Operations Command desire the BWA identifier component earlier than the targeted May 2026 full-rate production decision for the whole system. The program office desires to field the identifier component in July 2025. The program office plans to complete identifier chamber developmental testing in 2QFY25 according to the DOT&E-approved test plan. The program completed an MOT&E for the identifier component September 2024. The full system MOT&E is scheduled for 4QFY25.

» MAJOR CONTRACTORS

- Chemring Sensors & Electronic Systems – Charlotte, North Carolina
- Biomeme – Philadelphia, Pennsylvania

TEST ADEQUACY

The program is scheduled to complete all developmental and operational testing of all components in 4QFY25. The program conducted a subset of laboratory developmental testing of the identifier beginning in February 2024 to demonstrate its ability to recognize a series of BWAs. The laboratory conducted these tests in accordance with the DOT&E-approved test plans and TEMP. In addition, the program conducted a technical cooperative vulnerability and identification developmental test in March 2024 to initially explore if cyber vulnerabilities exist. DOT&E did not observe these tests.

The Army conducted the MOT&E of the BWA identifier component in September 2024 in accordance with the DOT&E-approved test plan. DOT&E observed the MOT&E, which demonstrated how warfighters use the identifier in operational settings. The laboratory testing and the MOT&E will form the basis for DOT&E's classified MOT&E report, which is expected in 3QFY25, prior to the fielding of the identifier component.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E will assess the operational effectiveness, suitability, and survivability of the JBTDS's BWA identifier component in the classified 2QFY25 MOT&E report. The program has not improved assay performance as recommended in the DOT&E FY23 Annual Report. The program intends to make improvements in the future.

DOT&E will assess the operational effectiveness, suitability, and survivability of the JBTDS whole system in a second classified MOT&E report, expected in 1QFY26.

RECOMMENDATIONS

The Joint Product Manager should continue to address the following recommendations from the FY23 Annual Report:

1. Mitigate identified vulnerabilities to electromagnetic effects.
2. Add cyber-specific topics to the training curriculum to better enable operators to recognize cyber threats and to protect, mitigate, and recover from hostile cyber actions.
3. Continue to address recommendations found in the classified annex of the July 2023 JBTDS operational assessment report.

4. Improve the identifier assays to meet performance requirements.

Joint Cyber Warfighting Architecture (JCWA)

With enhanced budget control and the intent to establish a Program Executive Office (PEO), U.S. Cyber Command's (USCYBERCOM) Joint Cyber Warfighting Architecture (JCWA) Integration Office (JIO) is at a critical juncture, with the goal of establishing a more agile, scalable, and interoperable JCWA. JCWA remains a concept that lacks the requirements, testing, proper governance, workforce, and authorities to successfully enable global cyber operations. The Services continue to aggressively field critical components of the architecture without adequate OT&E, and lessons learned from classified early operations indicate that this process must change. It is critical that USCYBERCOM finalize and submit the JCWA TES to DOT&E for approval. The JCWA TES has been in development for several years and once approved will aide in securing the T&E resources required to successfully verify JCWA system performance; inform critical training; and develop operational tactics, techniques, and procedures across all levels of JCWA global cyber operations.

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.

MISSION

USCYBERCOM intends to use JCWA to support all cyberspace operations, training, tool development, data analytics, and coordinated intelligence functions.

PROGRAM

JCWA is not a program of record itself but currently encompasses the following components:

- Unified Platform integrates cyber capabilities and systems as well as collaboration tools to enable cyber data processing, analysis, exploitation, and dissemination to support full spectrum cyber operations.
- Joint Cyber Command and Control will provide situational awareness, battle management, and cyber forces' management for full-spectrum cyber operations.
- The Persistent Cyber Training Environment will provide individual and collective training as well as mission rehearsal for cyber operations.
- An access component will provide additional capability for cyber operations.
- Other projects and methodologies used to develop and deploy tools and sensors to cyber forces.

At this time, USCYBERCOM continues to rely on the Services for acquisition of the components that comprise JCWA. However, the Command is taking initial steps to bring the acquisition programs under its authority. Each component currently has its own release, testing, and deployment schedule, and there are no validated JCWA-level requirements nor a JCWA Governance Charter.

The National Defense Authorization Acts of FY22 and FY23 provided for both USCYBERCOM enhanced budget control in FY24 and the establishment of a JCWA PEO within USCYBERCOM. The JCWA concept is at a critical juncture, as USCYBERCOM must establish governance processes and establish the workforce to do the following with limited resources: manage acquisition authorities, transition program management activities from the Services to the Command, develop requirements, and deliver capability that has been validated through adequate T&E. In light of these significant changes, DOT&E did not publish the early fielding report in FY24, as stated in the FY23 Annual Report. In 2QFY25, DOT&E intends to issue a classified report on JCWA's ability to conduct global cyber operations.

» MAJOR CONTRACTORS

Each Service uses a multitude of contracts and contractors for the acquisition of Unified Platform, Joint Cyber Command and Control, Persistent Cyber Training Environment, JCWA's access component, tools, and sensors.

TEST ADEQUACY

No JCWA-level operational testing was conducted during FY24. Interoperability efforts are currently ad hoc, with all JCWA components employing different Agile methodologies and on different development and deployment schedules. Operational testing at the component-level has been insufficient. Service-led programs under JCWA continue to develop and execute TESs independent of the JCWA construct. Service Operational Test Agencies have struggled to support the individual component OT&E programs, unable to react to the technical and constantly evolving demands of Agile, software-centric programs. This has resulted in the Services fielding multiple capabilities with insufficient testing, and as in some cases, operators or program managers doing their own series of validation events to inform user acceptance and capability release. DOT&E embraces the Development Security Operations (DevSecOps) approach and will be utilizing data from multiple sources in its operational assessments.

The JIO appointed the Joint Interoperability Test Command as the JCWA lead Operational Test Agency and provided initial funding to begin JCWA-level OT&E planning in FY23, with the intent to conduct initial JCWA-level OT&E events in FY24. Changes in JIO leadership, enhanced budget control, and lack of dedicated government T&E personnel in the JIO resulted in multiple stand-downs across JCWA components and the cancellation of critical T&E planning events intended to inform long-term T&E resource requirements. However, the USCYBERCOM JIO and DOT&E are working to approve the first JCWA TES in 1QFY25, which is a critical step toward establishing the required workforce and capability to support operationally effective, suitable, and survivable cyber missions. JIO and DOT&E also agree that future versions of the JCWA TES must also include an Integrated Decision Support Key that establishes evaluation criteria for the JCWA test program.

As the JCWA concept continues to mature, the scope of OT&E required to support cyber warfighting efforts will need to continuously evolve so that it addresses the entire architecture and the dynamic, operational environment within which it operates. Adequate OT&E of JCWA will require USCYBERCOM to establish a cadence of test and invest in the development of test infrastructure to successfully support JCWA integration and ensure mission effectiveness and survivability as the enterprise evolves. Planning and execution of dedicated JCWA OT&E will begin in FY25. Additionally, the DOT&E Cyber Assessment Program intends to partner with and increase its support to a USCYBERCOM Mission Approval Board over the next fiscal year, which will enable unprecedented cyber survivability assessments of USCYBERCOM's global infrastructure supporting cyber operations.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Insufficient data have been collected to enable a preliminary assessment of the JCWA-level operational effectiveness and suitability, or the performance of its individual components.

» SURVIVABILITY

Insufficient data have been collected to enable an evaluation of JCWA mission resilience in a cyber-contested environment.

RECOMMENDATIONS

As recommended in the FY23 Annual Report, USCYBERCOM should:

1. Prioritize and accelerate efforts to finalize JCWA-level requirements.
2. Require OT&E to inform value assessments.
3. Establish a cadence of test for dedicated OT&E, beginning in FY25, to understand how the capability afforded by JCWA is evolving over time and to ensure it is an operationally effective, suitable, and survivable enabler of cyber operations.

Additionally, USCYBERCOM should:

1. Establish a dedicated, government T&E chief in the JIO/PEO.
2. Establish a Combined Developmental Test/Operational Test Force that streamlines the T&E community.
3. Work with the T&E community to develop an Integrated Decision Support Key to establish evaluation criteria for the JCWA test program.
4. In an effort to secure and mitigate operational risk to cyber missions, partner with the DOT&E Cyber Assessment Program to immediately stand up a USCYBERCOM Mission Approval Board to enable cyber assessments of some of the architecture's most critical assets currently supporting operations.

Joint Operational Medicine Information Systems (JOMIS)

IOT&E events of Joint Operational Medicine Information Systems (JOMIS) managed applications are occurring as the applications become available for deployment. DOT&E will report on these test events as they occur. The Joint Interoperability Test Command (JITC) conducted an IOT&E event for the Medical Common Operating Picture (MedCOP) managed application in November 2023. DOT&E will publish a MedCOP report in 2QFY25. Operational testing of the other managed applications within the JOMIS portfolio began in January 2024, and will continue into FY25.

SYSTEM DESCRIPTION

The JOMIS program management office (PMO) provides a suite of applications – referred to as managed applications – to the warfighter to support the medical missions in theater. The JOMIS managed applications are:

- **MedCOP:** Provides a web-based interactive decision-support platform arming command surgeons and medical commanders with the ability to view, analyze, report, and share Health Service Support/Force Health Protection status in near real-time to inform current decision making and future planning.
- **Operational Medicine Care Delivery Platform (OpMed CDP):** Enables healthcare delivery and documentation of patient care at lower-level medical facilities using a commercial off-the-shelf capability.
- **Battlefield Assisted Trauma Distributed Observation Kit – Joint (BATDOK-J):** Enables healthcare delivery and documentation of patient care at the point of injury and during patient transport using a government off-the-shelf capability.
- **MHS GENESIS Theater (MHSG-T):** Enables healthcare delivery and documentation of patient care to all categories of patients at forward-deployed hospital facilities in a disconnected environment.
- **Operational Medicine Data Service (OMDS):** Serves as the data-centric infrastructure providing critical data transport and management capabilities that are key to all JOMIS operational medicine modernization activities.
- **Theater Blood Mobile (TBLD-M):** Provides the Services and blood operations community with the capability to manage and electronically document blood product donations; blood asset inventory and transfusions; and transmittable disease testing and tracking in both connected and disconnected, intermittent, and low-bandwidth operational environments. TBLD-M also provides real-time blood tracking of Walking Blood Bank candidates at both the local and aggregated level.

MISSION

Warfighters will use the managed applications acquired through the JOMIS PMO to support the five operational medicine healthcare functions: Medical Command and Control (MedC2), Medical Situational Awareness (MedSA), Medical Logistics (MedLOG), Healthcare Delivery (HCD), and Patient Movement (PM). See Table 1 below.

Table 1. Medicine Healthcare Functions Supported by JOMIS Managed Applications

	MedC2	MedSA	MedLOG	HCD	PM
MedCOP	X	X	X	X	X
OpMed CDP				X	
BATDOK-J				X	
MHSG-T			X	X	
OMDS	X	X	X	X	X
TBLD-M			X	X	

PROGRAM

MedCOP, OMDS, and TBLD-M are all software acquisition pathway programs, while OpMed CDP is a Middle Tier of Acquisition pathway program. BATDOK-J was previously developed by the Air Force Research Lab. MHSG-T is jointly developed with the Defense Healthcare Management System Modernization (DHMSM) PMO and is a Business System Category I program. DOT&E approved the JOMIS TES in September 2022. The JOMIS PMO has fielded MedCOP to most combatant commands but has not yet fielded the other five managed applications.

» MAJOR CONTRACTORS

A multitude of contracts and contractors support the JOMIS program.

TEST ADEQUACY

JITC conducted IOT&E of MedCOP at U.S. Africa Command in November 2023. The test was conducted in accordance with a DOT&E-approved test plan and observed by DOT&E. The test team observed operational users at U.S. Africa Command Headquarters and Service component sites use MedCOP in support of their operational mission. The IOT&E event was adequate to evaluate MedCOP's operational effectiveness and suitability. JITC evaluated the cyber survivability of MedCOP by conducting a cooperative vulnerability and penetration assessment in August 2023 and an adversarial assessment in July 2024. DOT&E will publish a MedCOP IOT&E report in 2QFY25.

JITC conducted the first part of a two-part operational assessment (OA) of four of the managed applications supporting the core HCD mission (OpMed CDP, BATDOK-J, MHSG-T, and OMDS) in January 2024. DOT&E observed part one of the OA, which was conducted in accordance with a DOT&E-approved test plan. Medical personnel used the HCD applications to document patient care in simulated scenarios. DOT&E will report on the outcome of the OA following the completion of part two, which is currently scheduled for 1QFY25.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E expects to report on the operational effectiveness, suitability, and survivability of the JOMIS managed applications following each OT&E event, beginning with the MedCOP IOT&E report in 2QFY25.

RECOMMENDATIONS

For operational testing of the HCD applications in FY25, the JOMIS PMO should:

1. Continue close collaboration with JITC and DOT&E to conduct operational testing that evaluates whether each managed application is operationally effective, suitable, and cyber survivable.
2. Ensure that upcoming operational tests have sufficient users to support assessments of operational effectiveness, suitability, and cyber survivability.

Joint Planning and Execution System (JPES)

The Joint Planning and Execution System (JPES) program continues Agile software development to replace the legacy Joint Operation Planning and Execution System (JOPES) program. The Joint Interoperability Test Command (JITC) conducted an early operational assessment (EOA) in October 2023 and two functional verification tests (FVTs) in December 2023 and March 2024, which gave users an opportunity to provide feedback on the effectiveness and usability of completed portions of the software development. The IOT&E previously reported as planned for 4QFY24 has been delayed to FY26 due to program delays.

SYSTEM DESCRIPTION

JPES will provide the Joint Planning and Execution Community with a web-based application on SIPRNet to create, edit, schedule, store, and query time-phased force deployment data (TPFDD) in support of joint contingency, crisis-action, and exercise planning. JPES is using an Agile software development and test approach.

The JPES Program Management Office (PMO) is continuing sustainment of the JOPES v4.5.x until JPES can be deployed to all JOPES users. Once JPES is fully fielded and provides current JOPES capabilities, JOPES is expected to be retired.

MISSION

JPES enables joint commanders to accomplish joint contingency, crisis action, and exercise planning by:

- Linking the National Command Authority to the Joint Task Force, component commanders, and Service-unique systems at lower levels of command.
- Translating policy decisions into operational plans that meet U.S. requirements to employ military forces.
- Supporting force deployment and redeployment.
- Conducting contingency and crisis action planning.

The Joint Planning and Execution Community uses the JPES portfolio to plan and execute military operations and exercises world-wide. This includes the capability to develop, refine, and maintain TPFDD, enable the identification and management of force requirements, and track the sourcing of those force requirements in accordance with the global force management and joint planning processes. The JPES portfolio provides data to and consumes data from the applicable external systems used by the U.S. Armed Forces and supported/supporting combatant commands, as well as their respective subordinate organizations.

PROGRAM

JPES is an Acquisition Category III program. The JPES PMO intends to continue development and conduct user assessments to ensure all necessary functionality meets or exceeds that of JOPES, which JPES is replacing. The JPES PMO is implementing the Development Security Operations (DevSecOps) process as part of its Agile software development framework.

» MAJOR CONTRACTORS

- ERP International, LLC – Laurel, Maryland
- NextGen Federal Systems – Morgantown, West Virginia
- Data Computer Corporation of America, Ellicott City, MD
- CompQsoft – Leesburg, Virginia

TEST ADEQUACY

JITC conducted an EOA in October 2023 and two FVT events in December 2023 and March 2024, in accordance with DOT&E's written guidance. The EOA and FVTs of JPES were conducted on SIPRNet and observed by DOT&E. The JPES integrated test environment on NIPRNet does not currently capture the differences between JPES operational environments (e.g. different commands using JPES). The JPES PMO plans for quarterly operational assessments in FY25; however, the IOT&E previously reported in DOT&E's FY23 Annual Report as planned for 4QFY24 has been delayed to FY26 due to program delays.

JPES test strategies must be developed to encompass the program's Agile nature and varying operational site requirements. The TEMP and the Agile Operational Test Plan (AOTP) are expected to be completed in FY25. The JPES TEMP should detail operational cyber survivability tests that include a cooperative vulnerability and penetration assessment (CVPA) followed by an adversarial assessment (AA).

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

JITC assessed the operational users' feedback from the EOA and FVT test events conducted in FY24. DOT&E will consider that data in the IOT&E report, expected to be released in FY26.

» SURVIVABILITY

No cyber survivability testing of JPES has been conducted. DOT&E's FY26 IOT&E report will address findings from the planned CVPA and AA.

RECOMMENDATIONS

DISA should:

1. Improve the operational representativeness of the JPES integrated test environment to ensure testing more closely reflects the differences of the operational environments, as discussed in the FY23 Annual Report.
2. Submit a JPES TEMP and an AOTP to DOT&E for approval, as discussed in the FY23 Annual Report.
3. Conduct a CVPA and an AA during the IOT&E of JPES, as discussed in the FY23 Annual Report.

Key Management Infrastructure (KMI)

The Key Management Infrastructure (KMI) Program Management Office (PMO) began Capability Increment 3 (CI-3) development in FY21. The National Security Agency (NSA) awarded a major contract modification in FY23 that increased the KMI CI-3 scope to address additional technical requirements packages in 10 Agile releases. The NSA Senior Acquisition Executive re-baselined the KMI CI-3 program in late FY23. The KMI CI-3 PMO intends to update the KMI CI-3 acquisition strategy and the TEMP in FY25 to support a full deployment decision (FDD) in FY27. DOT&E intends to publish a preliminary performance assessment following completion of the KMI CI-3 multi-release operational testing in FY25.

SYSTEM DESCRIPTION

KMI provides 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. The KMI CI-3 delivery will enhance the deployed KMI CI-2 capabilities with a combination of custom software development and commercial off-the-shelf computer components, which include a client host computer with monitor and peripherals, printer, and barcode scanner.

MISSION

Combatant commands, Services, DoD agencies, other Federal agencies, coalition partners, and allies will use KMI to provide secure and interoperable cryptographic key generation, distribution, and management capabilities to support mission-critical systems, the DoD Information Network, and initiatives such as Cryptographic Modernization.

Service members will use KMI cryptographic products and services to enable security (confidentiality, non-repudiation, authentication, and source authentication) for diverse systems, such as Identification Friend or Foe, GPS, and the Advanced Extremely High Frequency Satellite System.

AKP - Advanced Key Processor
CIK - Crypto Ignition Key
CLUAS - Card Loader User Application Software
HAIPE - High Assurance Internet Protocol Encryptor
PCMCIA - Personal Computer Memory Card International Association
Reinit - Reinitialization

PROGRAM

The NSA intended to deliver KMI CI-3 in eight planned Agile releases to enhance existing capabilities. The KMI CI-3 PMO began capability development in FY21 and announced a schedule delay in FY22, due to hardware technical refresh, supply chain delivery delays, system configuration problems, and expanded requirements. The NSA awarded a major contract modification in FY23 that increased the KMI CI-3 scope to address additional technical requirements in 10 total Agile releases. The NSA Senior Acquisition Executive re-baselined the KMI CI-3 program in late FY23, and the KMI CI-3 PMO intends to update the KMI CI-3 acquisition strategy in FY25 to support an FDD in FY27.

» MAJOR CONTRACTORS

- Leidos – Columbia, Maryland (Prime)
- SafeNet Inc., a subsidiary of Thales Group – Belcamp, Maryland

TEST ADEQUACY

In FY20, DOT&E approved the initial KMI CI-3 TEMP that defined an adequate operational test strategy for the KMI program release testing through IOT&E. The KMI CI-3 PMO incurred a major TEMP deviation in FY23, due to the NSA needing to provide a hardware and software technical refresh before delivering KMI CI-3 software releases. The KMI CI-3 PMO and the Joint Interoperability Command (JITC) are updating the KMI CI-3 TEMP to address test strategy, capability scope, and integrated schedule changes with submission to DOT&E now expected in FY25. JITC continues to develop an operational test plan to support KMI CI-3 technical refresh release testing in the production environment, which is now expected to commence in FY25. The KMI CI-3 PMO and JITC intend to operationally test the initial seven KMI capability releases later in FY25. DOT&E intends to publish an assessment of the initial KMI CI-3 capabilities in FY25.

The current Key Management Enterprise (KME) schedule includes concurrent test planning, execution, and reporting between KMI CI-3, Symmetric Catalog Synchronization, Enterprise Service Bus, and legacy Electronic Key Management System efforts. This many parallel activities adds risk to the program, as evidenced by the schedule delays over the past three years. While the KMI Test Infrastructure provides a safe environment for evaluating KMI software builds, it is currently not 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.

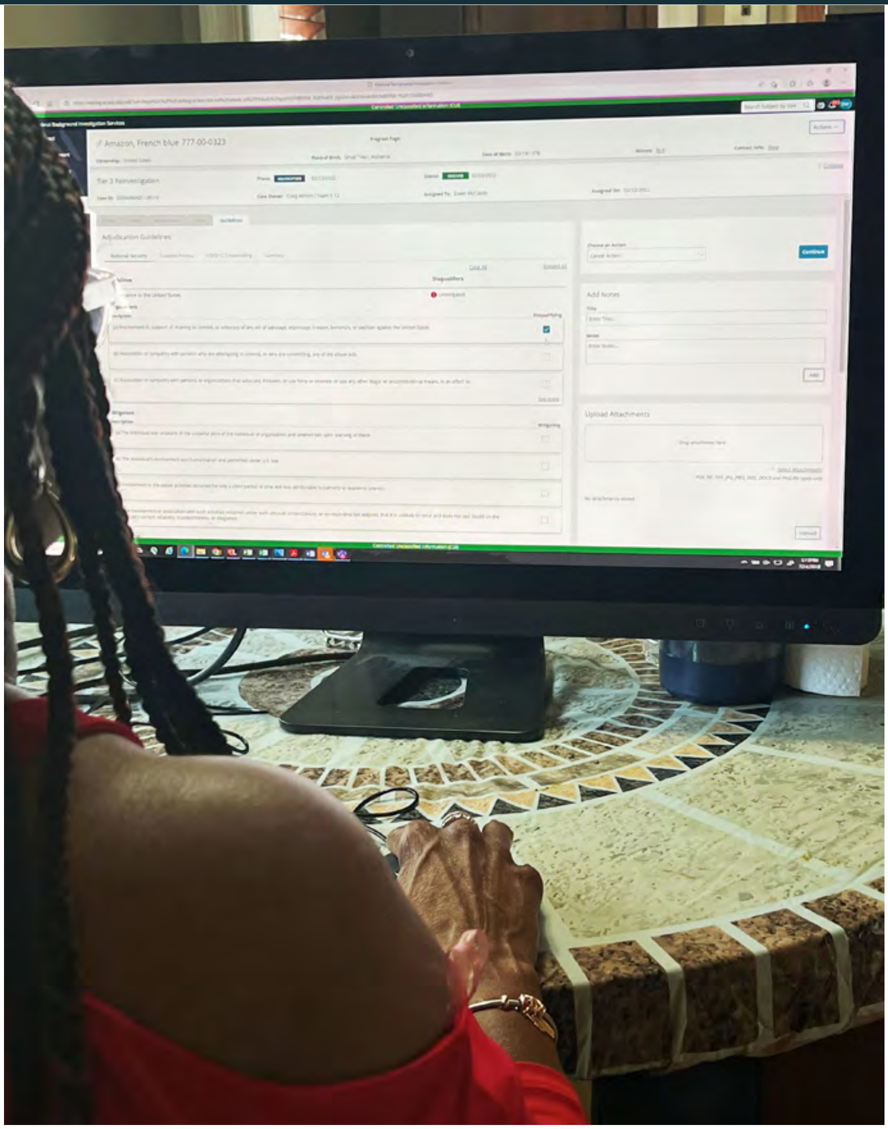
PERFORMANCE

DOT&E will provide a preliminary performance assessment after completion of the KMI CI-3 multi-release testing for the initial Agile releases, scheduled for FY25.

RECOMMENDATIONS

1. The KMI CI-3 PMO should reassess the release cadence and content to reduce test and delivery concurrency to make the integrated schedule more achievable, as recommended in the FY22 and FY23 Annual Reports.
2. The KMI CI-3 PMO and JITC should complete the KMI CI-3 TEMP updates to align the test strategy with the revised acquisition strategy, program baseline, and integrated schedule, as recommended in the FY23 Annual Report.
3. The NSA should mirror the KMI Test Infrastructure configuration to be the same as the operational environment, as recommended in the FY22 and FY23 Annual Reports.

National Background Investigation Services (NBIS)



In FY24, the National Background Investigation Services (NBIS) Program Office conducted a comprehensive re-structure of its acquisition strategy, and changes to the overall Evaluation Strategy are expected to follow in FY25. The program employs Agile software development techniques to field and build out capabilities in support of personnel security vetting missions. DOT&E observed limited operational testing in 1QFY24, but these events were not sufficient to assess program performance.

SYSTEM DESCRIPTION

NBIS is a cloud-based system-of-systems that will integrate both new and legacy systems to support all tasks associated with end-to-end personnel security vetting and continuous reviews. NBIS applications are integrated in a common architecture to support data gathering, storage, and management of data associated with personnel background investigations in a secure and protected environment.

MISSION

The Defense Counterintelligence and Security Agency (DCSA), other Federal agencies, and industry partners will use NBIS to authorize and support background investigations for new applicants as well as incumbent government, military, and contract personnel. NBIS has four operational mission areas: case initiation, adjudication, continuous vetting, and background investigation. It also has three cross-cutting support missions: service operations, metrics and reporting, and subject management. These missions allow agencies to initiate clearance requests, enable candidates to complete background investigation forms, gather public data concerning personnel applying, manage the findings of an investigation, adjudicate personnel clearances, and provide continuous vetting of cleared personnel. The system of systems also simultaneously supports and measures system performance across these functions.

PROGRAM

NBIS transitioned to the software acquisition pathway in FY21 and is being developed using Scaled Agile Framework (SAFe) and Development Security Operations (DevSecOps) methodologies. The DCSA assumed operational control for NBIS from the Defense Information Systems Agency in October 2020 and is deploying NBIS in multiple releases of increasing capability, while building upon some legacy systems. The program has employed SAFe methodologies to rapidly develop and field capabilities in collaboration with the testers and intended customer/user base. Early releases to a limited and restricted user base supported continuous developmental testing and a cumulative validation of system and data security. In March 2022, DOT&E placed NBIS on oversight due to program size, complexity, and importance to DoD operations. DOT&E has approved an NBIS Evaluation Strategy and an online test management process for NBIS. Following a comprehensive program review in FY24, the program office has modified the service and capability delivery schedules and methods to migrate and modernize legacy systems and reduce new software production. This change required a revised Evaluation Strategy. DOT&E approved the revised Evaluation Strategy in 1QFY25.

» MAJOR CONTRACTORS

- Peraton, Inc. – Reston, Virginia (software development)
- HII – Newport News, Virginia (big data platform)
- Copper River Information Technology, LLC – Chantilly, Virginia (systems engineering)
- GovCIO – Eatontown, New Jersey (operations support)

TEST ADEQUACY

NBIS testing has largely focused on developmental software validation and release. Joint Interoperability Test Command (JITC) has completed multiple rounds of cyber survivability tests and began conducting the first operational assessment (OA) in FY24. DOT&E approved the NBIS Evaluation Strategy in December 2022 and approved an online test management process that makes extensive use of online planning software, in lieu of written test documents, for NBIS in July 2023, as a pilot effort with potential relevance to other Agile software developments. JITC conducted a partial OA of the case initiation mission area in 1QFY24, observed by DOT&E, but it was incomplete and not sufficient to assess program performance. JITC also conducted two cyber survivability tests in 3QFY24 and 4QFY24. Additional OA events were included in the updated Evaluation Strategy.

PERFORMANCE

» EFFECTIVENESS

The operational mission areas of NBIS are developing at different rates: case initiation and adjudication capabilities are both relatively mature. Continuous vetting capabilities continue to mature, and background investigations capabilities are in early development. The cross-cutting mission areas are also in varying stages of maturity at this time. The partial OA of case initiation was incomplete and therefore the effectiveness of this mission area cannot yet be fully assessed.

» SUITABILITY

Suitability testing is ongoing, and assessments of issue tracking and resolution, training, and helpdesk support are not yet completed. The partial OA of case initiation was incomplete regarding suitability, and further development of the system monitoring and help desk capabilities is needed prior to the next OA.

» SURVIVABILITY

Several rounds of cyber survivability testing have been conducted on NBIS and relevant connected legacy systems. Based on a 2024 assessment, the system is currently considered not survivable against a moderate threat due to a vulnerability in the DoD supporting infrastructure not under control by the NBIS program. The relevant agencies have stood up a working group to address this finding.

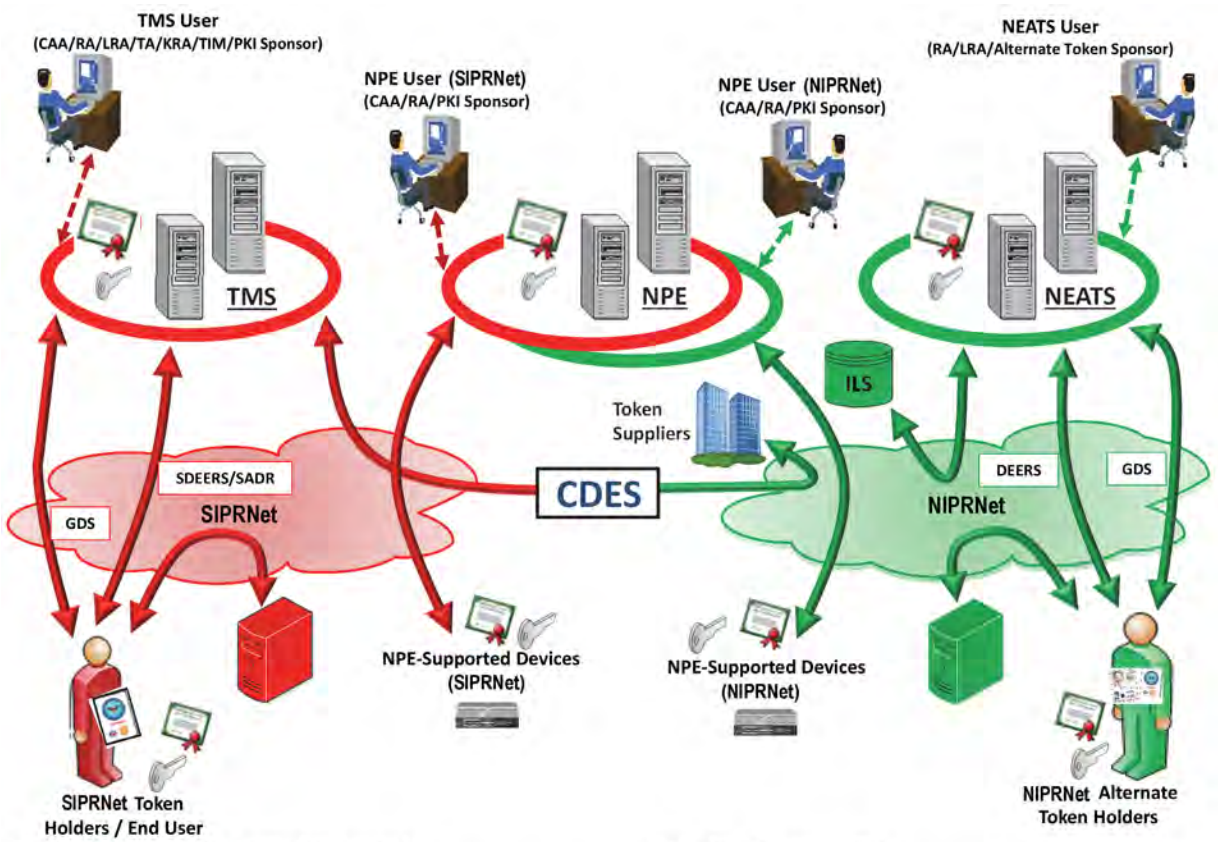
RECOMMENDATIONS

DCSA and the NBIS Program Office should:

1. Continue development of the online test management process and automated test support.
2. Work with the appropriate stakeholders to address infrastructure cyber vulnerabilities to ensure NBIS is cyber-survivable.

Public Key Infrastructure (PKI) Increment 2

The DoD Public Key Infrastructure (PKI) Increment 2 (consisting of Token Management System (TMS), NIPRNet Enterprise Alternate Token System (NEATS), and Non-Person Entity (NPE)) is operationally effective, demonstrating the capability to facilitate secure electronic information exchanges between DoD users and network devices. In FY24, the Joint Interoperability Test Command (JITC) completed the TMS operational suitability and token ordering process reassessment and the NEATS cyber assessment. DOT&E intends to publish a TMS suitability and NEATS cyber survivability assessment in 1QFY25. Given the criticality of PKI to DoD's cyber posture, the National Security Agency (NSA), Defense Information Systems Agency (DISA) and Defense Manpower Data Center (DMDC) should continue to address cyber vulnerabilities and conduct periodic independent cyber testing to ensure PKI is survivable.



CAA - Certification Authority Administrator
CDES - Cross Domain Enterprise Service
DEERS - Defense Enrollment Eligibility Reporting System
GDS - Global Directory Service
ILS - Integrated Logistics System
KRA - Key Recovery Agent
LRA - Local Registration Authority
NEATS - NIPRNet Enterprise Alternate Token System
NIPRNet - Non-classified Internet Protocol Router Network
NPE - Non-Person Entity
RA - Registration Authority
SADR - Secret Authoritative Data Repository
SDEERS - Secret Defense Enrollment Eligibility Reporting System
SIPRNet - Secret Internet Protocol Router Network
TA - Trusted Agent
TIM - Token Inventory Manager
TMS - Token Management System

SYSTEM DESCRIPTION

PKI Increment 2 enables the DoD to ensure only authorized individuals and devices have access to networks and data, thereby supporting the secure flow of information across DoD Information Networks and providing secure local storage of information. PKI Increment 2 provides the hardware, software, and services to generate, publish, revoke, and validate NIPRNet and SIPRNet PKI certificates.

MISSION

DoD users at all levels use DoD PKI to provide authenticated identity management via personal identification number-protected Common Access Cards, SIPRNet tokens, and 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 Service and DoD Agency operators, communities of interest, and other authorized users use DoD PKI to securely access, process, store, transport, and use information, applications, and networks. Network operators use NPE certificates on classified and unclassified workstations, web servers, and devices to create secure network domains, which facilitate intrusion protection and detection.

PROGRAM

The NSA has developed and deployed PKI Increment 2 in four spirals on SIPRNet and NIPRNet. DOT&E approved the PKI Spiral

4 TEMP Addendum in October 2017, the PKI Increment 2 FOT&E plan in October 2020, and the Cybersecurity Annex in November 2020. The NSA delivered the SIPRNet TMS in Spirals 1, 2, and 3 prior to late May 2018. Spiral 4 delivered NEATS and NPE NIPRNet and SIPRNet capabilities in late September 2024. The NSA developed NEATS with the DMDC, and NPE with operational support from the DISA. TMS, NPE, and NEATS use commercial and government off-the-shelf hardware and software hosted at DISA and DMDC operational sites. DOT&E published the PKI Increment 2 FOT&E Report in November 2021, a classified NPE finding memo in February 2022, and a classified PKI Increment 2 Cyber Survivability Interim Annex in January 2023. DOT&E intends to publish a classified PKI Increment 2 Suitability and Cyber Survivability Annex Update in 1QFY25 to support the full deployment decision (FDD).

» MAJOR CONTRACTORS

- General Dynamics Mission Systems – Dedham, Massachusetts (Prime for TMS and NPE)
- Peraton, Inc. – Herndon, Virginia (Prime for NEATS)
- SafeNet Assured Technologies, a subsidiary of Thales Group – Abingdon, Maryland
- Giesecke and Devrient America – Twinsburg, Ohio
- IDEMIA – Reston, Virginia
- 90Meter – Newport Beach, California

TEST ADEQUACY

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 and assess operational effectiveness and suitability of PKI Increment 2 capabilities for long-term sustainment and transition. JITC completed FOT&E re-testing and verifications of fixes for operational suitability issues in FY24, which were observed by DOT&E.

JITC conducted NPE and TMS cyber testing in FY21 and re-tested NPE cyber in late FY21 and FY22. The PKI Program Management Office (PMO) implemented partial NPE cyber mitigations in FY22, which were observed by JITC and DOT&E. JITC completed cyber survivability testing of NEATS in July 2024, in accordance with a DOT&E-approved test plan annex update from October 2023 to support the DoD PKI Increment 2 FDD. DOT&E intends to publish a classified PKI Increment 2 Suitability and Cyber Survivability Annex Update that captures FY24 testing in 1QFY25.

PERFORMANCE

» EFFECTIVENESS

DOT&E assessed PKI Increment 2 NEATS, NPE, and TMS are operationally effective in the DOT&E PKI Increment 2 FOT&E Report published in November 2021. JITC completed verification of fixes for PKI capabilities in FY23 with no additional effectiveness testing required in FY24.

» SUITABILITY

DOT&E assessed PKI Increment 2 NEATS and NPE as operationally suitable in the DOT&E PKI Increment 2 FOT&E Report published in November 2021, and DOT&E intends to publish an updated assessment of TMS operational suitability in 1QFY25. The PKI PMO updated the TMS baseline with improvements in Enterprise Central Management of Tokens (CMT) order tracking to provide for better token accountability in FY23. JITC completed the follow-on assessment in FY24 that showed significant improvement with Enterprise CMT, Service, and Defense Agency token tracking, accountability, and reconciliation processes.

» SURVIVABILITY

DOT&E assessed TMS as survivable and NPE as not survivable against moderate capability cyber threats in the DOT&E PKI Increment 2 FOT&E Report published in November 2021 and the classified PKI Increment 2 Cyber Survivability Interim Annex in January 2023. DOT&E intends to publish a NEATS cyber survivability assessment in 1QFY25. The PKI PMO mitigated all but one of the NPE problems but did not mitigate the remaining problem or conduct further NPE operational cyber testing prior to FDD. The PKI PMO and DMDC mitigated many NEATS findings and other architectural problems found in previous cyber survivability testing. As NSA, DISA, and DMDC migrate PKI capabilities to cloud hosting environments, operational cyber testing will be needed to maintain and improve survivability. The PKI PMO, NSA Acquisition Security Office, and DMDC token supply chain risk management processes need to improve monitoring of token manufacturer processes.

RECOMMENDATIONS

The PKI PMO should:

1. Address remaining cyber vulnerabilities and conduct periodic operational cyber survivability assessments of PKI capabilities after FDD.
2. Improve token supply chain risk management processes to inform Service and Defense Agency token purchasing and operational use decisions.

DEPARTMENT OF THE ARMY PROGRAMS

This page intentionally left blank.

120mm Advanced Multi-Purpose (AMP) Cartridge, High Explosive Multi-Purpose with Tracer, M1147

The Army completed M1147 120mm Advanced Multi-Purpose (AMP) combat ballistic validation testing and First Article Acceptance Testing (FAAT). Testing supported the previously delayed full-rate production decision.

SYSTEM DESCRIPTION

The M1147 AMP cartridge is a line of sight, full-bore multipurpose munition employed by Abrams tanks. The AMP cartridge consolidates the capabilities of four cartridges: the M830 High Explosive Anti-Tank cartridge, M830A1 Multi-Purpose Anti-Tank cartridge, M1028 Canister cartridge, and M908 Obstacle Reduction cartridge, into one cartridge. The AMP cartridge is intended to add new capabilities for breaching walls and defeating dismounted Anti-Tank Guided Missile teams at extended ranges.

MISSION

Commanders employ units equipped with the M1147 120mm AMP cartridge to close with and destroy the enemy by direct fire across the full range of military operations.

PROGRAM

The 120mm AMP cartridge is an Acquisition Category III program. DOT&E approved the M1147 120mm AMP TEMP, to include LFT&E Strategy in December 2020, and the IOT&E plan in August 2021. After the publication of the DOT&E combined IOT&E and LFT&E report in December 2022, the full-rate production decision was delayed due to an investigation to identify the root cause of failure from the FAAT. The Army's root cause analysis was successful, failures were fixed, and follow-on FAAT in May 2024 supported the full-rate production decision.

» MAJOR CONTRACTOR

- Northrop Grumman Defense Systems – Plymouth, Minnesota

TEST ADEQUACY

The Army completed combat ballistic validation testing and follow-on FAAT. Both events were program office-led tests – not operational or live fire tests – and thus their test plans did not require DOT&E approval, nor did DOT&E observe the tests.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

DOT&E published a classified combined IOT&E and LFT&E report in December 2022, providing assessments of M1147 120mm AMP cartridge's operational effectiveness, lethality, suitability, and survivability. DOT&E found performance of the round was operationally effective, lethal, suitable, and survivable. The program office-led tests in FY24 do not affect those assessments.

RECOMMENDATION

All recommendations have been addressed.

AN/APR-39E(V)2 Modernized Radar Warning Receiver (MRWR)

The Army continues to develop the AN/APR-39E(V)2 Modernized Radar Warning Receiver (MRWR) to enhance aircrew situational awareness and aircraft survivability during current and emerging electromagnetic spectrum operations (EMSO). In FY23, developmental testing, monitored by DOT&E, included laboratory and flight test events. In FY24, the Army conducted operational cyber testing on MRWR in accordance with DOT&E-approved test plans. An FOT&E test period is planned for 1QFY25 to inform the Army's fielding and full-rate production (FRP) decisions.

SYSTEM DESCRIPTION

The AN/APR-39E(V)2 MRWR was developed to replace the more than 30-year-old AN/APR-39A(V)1/4 and AN/APR-39C(V)1/4 systems on Army rotary-wing and selected fixed-wing aircraft. New electronics and improved antennas provide a fully digital threat discrimination capability against current and emerging threats that operate over extended frequency ranges with highly agile waveforms. Cockpit display of the threat's location and operating mode, combined with auditory warnings, enhance the aircrew's situational awareness and the aircraft's survivability.

The MRWR includes an open-systems approach and a growth path for integrating an electronic attack capability.

MISSION

Commanders will employ units equipped with the AN/APR-39E(V)2 to improve the mission survivability of Army aircraft by identifying radio-frequency signals from hostile surface-to-air missiles, airborne interceptors, and anti-aircraft artillery. The combination of improved situational awareness, tactics, techniques, and procedures will allow aircrew to deny, degrade, deceive, disrupt, and defeat attacking threats.

PROGRAM

The APR-39E(V)2 is an Acquisition Category II program developed as an engineering change proposal to the Navy's APR-39D(V)2. The Army conducted FOT&E of the D(V)2, in accordance with a DOT&E-approved test plan in 2017, and fielded a limited number as an interim solution to an operational need. MRWR development started in 2019 and the Army's TES, approved by the Program Executive Officer for Intelligence, Electronic Warfare & Sensors, was accepted by DOT&E when the program was placed on DOT&E oversight in December 2022. The Army began low-rate initial production in December 2023. An FOT&E period is planned for November 2024 to inform the Army's fielding and FRP decisions in 1QFY26.

» MAJOR CONTRACTOR

- Northrop Grumman – Rolling Meadows, Illinois

TEST ADEQUACY

The Army conducted three developmental tests in 2023. The first was an installed system evaluation in March 2023 of the APR-39E(V)2 onboard an AH-64E, which occurred in the Joint Preflight Integration of Munitions and Electronic Systems (JPRIMES) anechoic chamber at Eglin AFB, Florida. The aircraft was illuminated with threat signals of interest and background signals to assess the E(V)2's performance and integration with the aircraft's controls and displays. DOT&E participated in JPRIMES testing and observed that the system performance was stable and predictable. The second DT event conducted by the Army was a built-in test demonstration in March 2023. A total of 194 test cases were executed in a laboratory environment, demonstrating that the E(V)2 meets the Army's requirements for fault detection and fault isolation.

For the third DT event in June 2023, JPRIMES testing was followed by open-air-range flight testing of a single AH-64E on the Electronic Combat Range, at the Naval Air Weapons Station in China Lake, California. Flights were conducted against the range's surface threats, along with a "trolling" flight through the Los Angeles area to assess performance in a dense and diverse electromagnetic background environment. After test completion, DOT&E received copies of the Army reports for all three tests and is analyzing them in preparation for the upcoming FOT&E.

The Army conducted a cooperative vulnerability and penetration assessment in December 2023 and an adversarial assessment (AA) in March 2024, in accordance with DOT&E-approved test plans and observed by DOT&E. Both assessments were performed on an AH-64E Apache at the Redstone Test Center in Redstone Arsenal, Alabama. Final system performance and mission accomplishment, while under cyber-attack, will be characterized as part of a second AA during the FOT&E.

PERFORMANCE

» EFFECTIVENESS

Results from developmental laboratory anechoic chamber testing and flight test events of the APR-39E(V)2, along with prior D(V)2 FOT&E effectiveness results, are being analyzed. DOT&E's final assessment of E(V)2 operational effectiveness is pending FOT&E completion, scheduled for November 2024.

» SUITABILITY

Results from developmental laboratory anechoic chamber testing, flight test events of the APR-39E(V)2, along with prior D(V)2 FOT&E suitability results, are being analyzed. DOT&E's final assessment of E(V)2 operational suitability is pending FOT&E completion, scheduled for November 2024.

» SURVIVABILITY

Assessment of E(V)2 cyber survivability is pending completion of the second AA during the FOT&E, scheduled for November 2024.

RECOMMENDATIONS

The Army should:

1. Execute the planned FOT&E to inform their fielding and FRP decisions.
2. Continue to develop and refine the APR-39D/E(V)2 software, libraries, and techniques as threats continue to evolve.

Armored Multi-Purpose Vehicle (AMPV)

Armored Multi-Purpose Vehicle uses, clockwise from top left: General Purpose | Mission Command | Mortar Carrier | Medical Treatment with Shelter | Medical Evacuation

The Army completed full-up system-level (FUSL) live fire testing in May 2022 and an IOT&E in July 2022. DOT&E published a combined IOT&E and LFT&E report, with a classified annex, in January 2023, assessing the AMPV as operationally effective, suitable, and survivable against specified kinetic threats. The Army is implementing corrective actions in response to vulnerabilities and issues identified during operational and live fire testing and plans to validate the design improvements through developmental and live fire testing.

SYSTEM DESCRIPTION

The AMPV is a tracked, ground combat vehicle that supports casualty evacuation and treatment, command post operations, logistical resupply, and heavy mortar fire support to an Armored Brigade Combat Team (ABCT). There are five variants: General Purpose (GP), Mission Command (MCmd), Medical Treatment (MT), Medical Evacuation (ME), and Mortar Carrier (MC). The AMPV replaces the M113A3 Family of Vehicles (FoV), consisting of the M113A3 (GP and ME), M1064A3 (MC), M1068 (MCmd), and M577 (MT) variants, and addresses shortcomings in survivability, force protection (i.e., size, weight, power, and cooling), and the ability to incorporate future technologies, such as the Army Network.

MISSION

ABCTs will employ the AMPV to provide a more survivable and mobile platform than the legacy M113A3 FoV to accomplish required operational support missions across the range of military operations. ABCT units will use AMPVs to support casualty evacuation and treatment, command post operations, logistical resupply, and heavy mortar fire support.

PROGRAM

The AMPV is an Acquisition Category IC program under the major capability acquisition pathway. The full-rate production decision was made in July 2023. The Army is implementing corrective actions in response to vulnerabilities and issues identified during operational and live fire testing and plans to validate the design improvements through developmental and live fire testing.

The Army conducted a demonstration of the AMPV Modular Turreted Mortar System (MTMS) at the Maneuver Warfighter Conference in September 2024, to inform Army leadership on the feasibility of pursuing a future AMPV MTMS program of record.

» MAJOR CONTRACTOR

- BAE Systems – York, Pennsylvania

TEST ADEQUACY

The Army completed FUSL live fire testing in May 2022 and an IOT&E in July 2022. Testing was adequate, conducted in accordance with DOT&E-approved test plans, and observed by DOT&E personnel. DOT&E published a combined IOT&E and LFT&E report, with a classified annex, in January 2023.

The Army implemented hardware and software corrective actions to address system failure modes and cybersecurity vulnerabilities observed during IOT&E in July 2022. The developmental testing to verify these fixes is ongoing and will complete in December 2024 at Yuma Test Center, Arizona. The program office completed a software update and regression testing in August 2024 at Detroit Arsenal, Michigan to correct vulnerabilities identified during the 2022 adversarial assessment.

The Army is finalizing design changes to the Automatic Fire Extinguishing System (AFES) to fix the vulnerabilities observed in FUSL testing and AFES testing in FY22. The Army is planning AFES validation testing in 2QFY25 at Aberdeen Proving Ground, Maryland.

In the DOT&E combined IOT&E and LFT&E report published in January 2023, DOT&E recommended making the interior of the MCmd reconfigurable to better support crews conducting analog operations and developing a fire direction-specific variant to better facilitate crews’ ability to conduct fire direction center operations. The Army currently is not pursuing initiatives to make the interior of the MCmd reconfigurable nor are they developing a fire direction-specific variant. However, the Army will continue to conduct post fielding assessments in these areas.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E published a combined IOT&E and LFT&E report, with a classified annex, in January 2023 assessing the AMPV as operationally effective, suitable, and survivable against specified kinetic threats. The Army is working on design changes to the AFES, computer screens, and other sub-components to address the recommendations from the January 2023 report and the FY23 Annual Report.

As recommended in the FY23 DOT&E Annual Report, the Army implemented fixes on several deficiencies identified during the IOT&E, including improved mortar hatch spring, engine control software, access point seals, computer screen stability, and subsystem access. These fixes were verified through developmental and cybersecurity tests conducted in FY24.

DOT&E and ATEC will confirm the efficacy of these fixes in 1QFY25 on vehicles at Yuma and at the

Detroit Arsenal, and DOT&E will include an assessment in the FY25 Annual Report.

RECOMMENDATIONS

As discussed in the FY23 Annual Report, the Army should:

1. Consider initiatives to make the interior of the MCmd reconfigurable to better support crews conducting analog operations.
2. Consider developing a fire direction center-specific variant to better facilitate crews' ability to conduct fire direction center operations.
3. Continue to address the survivability recommendations provided in the classified annex to the combined IOT&E and LFT&E report.

Additionally, the Army should:

1. Finalize the AFES design changes and conduct validation testing.

Army Integrated Air and Missile Defense (AIAMD)

In November 2023, the Army Integrated Air and Missile Defense (AIAMD) program participated in the Army's Integrated Fires Test Campaign 2023 (IFTC 23), supporting the Lower-Tier Air and Missile Defense Sensor (LTAMDS) operational assessment. In July 2024, DOT&E approved an updated annex to the program's TES that covers AIAMD participation in IFTC 24 and an FOT&E that will be conducted during IFTC 25.

SYSTEM DESCRIPTION

The AIAMD program provides an Integrated Air and Missile Defense (IAMD) Battle Command System (IBCS) to integrate Engagement Operations Centers (EOCs), Sentinel air-surveillance radars, Patriot radars, and Patriot 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 distributed operations and mobile communications nodes to extend IFCN connectivity. Future hardware and software updates will integrate additional sensors and weapons, such as LTAMDS and the Indirect Fire Protection Capability Increment 2 (IFPC Inc 2).

MISSION

Air Defense Artillery forces will use IBCS 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 deployed forces.

PROGRAM

AIAMD is an Acquisition Category ID program, developing hardware using the major capability acquisition pathway and conducting agile software development using the software acquisition pathway. DOT&E published a classified IOT&E report in March 2023 to inform the program's full-rate production decision. The Army intends to integrate new and existing sensors and weapons through a series of future increments.

In July 2024, DOT&E approved the AIAMD 2024 T&E Annex. The annex covers testing of future IBCS capability updates, including participation in IFTC 24, which began in September 2024, and a dedicated FOT&E to be conducted during IFTC 25 in 3QFY25. In addition to evaluation of capability updates, the FOT&E will evaluate the correction of deficiencies discovered before and during IOT&E. The Army plans to continue to submit annual T&E annexes.

The Army is considering fielding some AIAMD components OCONUS in FY25. This may delay the schedule for IFTC 25, but will not affect the scope of the dedicated FOT&E.

» MAJOR CONTRACTORS

- Northrop Grumman Corporation – Huntsville, Alabama
- Raytheon, a subsidiary of RTX – Huntsville, Alabama and Andover, Massachusetts
- Lockheed Martin Corporation – Dallas, Texas

TEST ADEQUACY

AIAMD participated in IFTC 23, which took place in November 2023, in support of the LTAMDS operational assessment. DOT&E approved the IFTC 23 test plan and observed the testing. DOT&E determined that IFTC 23 was inadequate to support an assessment of operational effectiveness due to immature and unaccredited LTAMDS modeling and simulation (M&S) tools. AIAMD is also participating in IFTC 24 to support LTAMDS and IFPC Inc 2 operational assessments. Testing began in September 2024, in accordance with the DOT&E-approved test plan and was observed by DOT&E. IFTC 24 is planned to end in 1QFY25.

As the Army continues to integrate systems into the AIAMD architecture, the M&S tools for those sensors and weapons must also be verified, validated, and accredited to support credible assessments of operational effectiveness in realistic threat environments.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

AIAMD started to collect additional operational test data in FY24. Performance evaluations are unchanged from DOT&E's

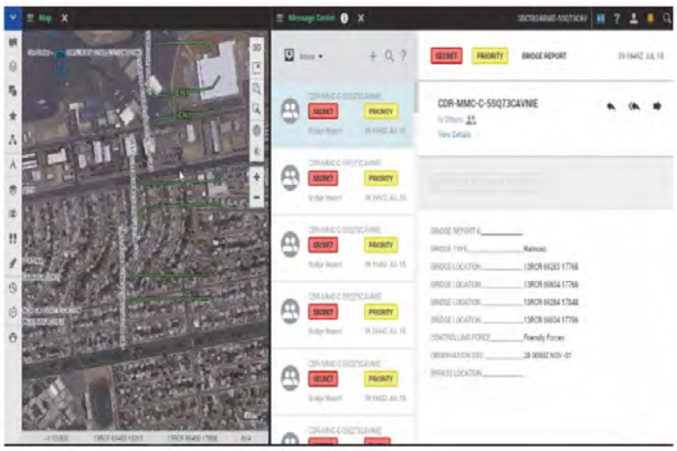
classified March 2023 IOT&E report.

RECOMMENDATIONS

The Army should:

1. Complete and demonstrate the deficiency corrections recommended in DOT&E's classified IOT&E report, as recommended in the FY23 Annual Report.
2. Continue to develop an integrated suite of M&S tools to support follow-on testing of IBCS and generate the data necessary to support the verification and validation of these tools to provide operationally representative assessments of these increasingly complex IAMD systems, as recommended in the FY22 and FY23 Annual Reports.
3. Continue development of the AIAMD 2025 T&E Annex to prepare for dedicated FOT&E during IFTC 25.

Command Post Computing Environment/ Tactical Server Infrastructure (CPCE/TSI)



In FY24, the Army conducted an operational cooperative vulnerability and penetration assessment and adversarial assessment (AA) of the Command Post Computing Environment/Tactical Server Infrastructure (CPCE/TSI). CPCE/TSI is cyber survivable when employed with trained Army cyber defense soldiers using integrated cyber defense tools. In July 2024, DOT&E published a classified CPCE cyber survivability report that finds the Increment 2 performed the same against nearsiders and outsiders compared to CPCE Increment 1. The Army continues to adopt an Agile development process for the program based on feedback from unit exercises.

SYSTEM DESCRIPTION

CPCE 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. The Increment 2 builds upon the previously tested Increment 1 and Increment 0 capabilities. The 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 CPCE software and applications reside on TSI hardware and previously fielded Battle Command Computing Services servers at tactical echelons that span from Army Service component commands to battalion level. TSI provides the command post foundational infrastructure consisting of server hardware, computing power and storage, and applicable server software required to support Mission Command Systems.

In addition to the software, TSI also integrates and hosts the enterprise services that are required to provide mission command capability to units.

MISSION

The Army intends for commanders and staff at battalion through corps levels to use CPCE to conduct mission command throughout all four phases of the Army operations process, to include planning, preparation, execution, and continuous assessment of unit missions. As the Army further develops its Common Operating Environment, commanders and staff will use CPCE as a collection point for data from sensors, aviation, logistics, fires, intelligence, and safety information, including mounted, dismounted and home station command units.

PROGRAM

CPCE is an Acquisition Category II major capability acquisition pathway program. A full deployment decision for Increment 1 occurred December 2021. DOT&E published an FOT&E report to support this decision. The program office developed an updated TEMP, which DOT&E approved in January 2023. The Army restructured the program in October 2023 to move to a more Agile software approach instead of pursuing a full deployment decision. This resulted in a down-scope of the original follow-on operational test to focus on the cyber portion of the software to support a software release. DOT&E published a classified CPCE cyber survivability report in July 2024. The Army is still refining the details of the Agile software approach into formal acquisition strategies.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

The Army conducted a cooperative vulnerability and penetration assessment in February 2024, and an AA in March 2024, at Schofield Barracks, Hawaii. DOT&E observed both tests. The cooperative vulnerability and penetration and AA test environments leveraged the network architecture environment developed by the 25th Infantry Division.

Testing was adequate to support an assessment of the cyber survivability of CPCE. DOT&E published a classified CPCE cyber survivability report that finds the Increment 2 performed the same against nearsiders and outsiders compared to CPCE Increment 1. Testing was conducted in accordance with the DOT&E-approved test plans, however, because this event fell under a unit's training exercise, the test objectives were lower priority. As a result of this, cyber testing captured limited mission effects that stemmed from cyber compromises.

If unit exercises will be used in the future, there should be a greater emphasis toward integrating test objectives within the unit's training objectives to ensure a more robust test. Due to the down-scope of the test to focus solely on cyber, there was no instrumentation required. As recommended in the FY22 Annual Report, the Army should complete the improvement of CPCE data instrumentation to support test adequacy and confidence in data collection for determining effectiveness and suitability during future developmental and operational tests and demonstrate instrumentation effectiveness in a CPCE test event.

The Army is also in the process of changing the operational mission for CPCE. In April 2024, the Army executed Operation Lethal Eagle at Fort Campbell, Kentucky; Fort Knox, Kentucky; and Camp Atterbury, Indiana, where the Army hoped to move the system complexity from the brigade up to the division and obtain key observations from the unit. These observations will impact many network and command and control systems beyond CPCE. While not a formal test, the Army is leveraging this exercise and a Joint Readiness Training Center rotation to inform future Army programs. The Army should codify this process formally going forward and develop a future TEMP to better inform acquisition decision making.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

In December 2021, DOT&E published a FOT&E Report that found CPCE Increment 1 operationally effective and not suitable due to reliability issues. FY24 testing did not support an additional assessment of operational effectiveness and suitability.

» SURVIVABILITY

CPCE Increment 2 is cyber survivable in a cyber-contested environment compared to the Increment 1. CPCE maintained a strong cybersecurity defense posture when employed with trained Army cyber defense soldiers using integrated cyber defense tools. The full description of CPCE cyber survivability against an operationally realistic cyber threat is detailed in the classified cyber survivability report published in July 2024.

RECOMMENDATIONS

The Army should:

1. Continue the improvement of CPCE data instrumentation to support test adequacy and confidence in data collection during future developmental and operational tests and demonstrate its effectiveness in a CPCE test event, as recommended in the FY22 Annual Report.
2. Ensure that any future test event that leverages a unit training exercises also prioritizes test objectives.
3. Codify future Army exercises and training events that will be used to support acquisition decisions within a TEMP and submit it to DOT&E for approval.

Common Tactical Truck (CTT)

In January 2023, DOT&E placed the Common Tactical Truck (CTT) on oversight and in April 2024, approved the CTT TES. The Army conducted an operational demonstration (Ops Demo) in August and September 2024. The Army will use performance test data from the Middle Tier of Acquisition (MTA) rapid prototyping phase to develop a Capability Development Document (CDD) for the CTT. This new CDD will be the basis for a follow-on full and open competition. The Army plans to conduct limited test to support contract award and transition to a major capability acquisition program at Milestone C (MS C) in FY28.

SYSTEM DESCRIPTION

CTT is a Family of Vehicles (FoV) modernization effort to replace the Heavy Expanded Mobility Tactical Truck, Palletized Load System, Line Haul Tractor, and Medium Tractor vehicles, by leveraging the best commercial practices and technologies. Desired attributes to consider include predictive logistics, advanced driver assistance technology, and readiness for autonomous capability. The Army envisions the CTT FoV to include modular designs and interchangeable repair parts across the fleet. The CTT FoV initial concept consists of a cargo and load handling system, off-road tractor, line-haul tractor, and tanker, as well as base platforms for air defense, missile systems, radar systems, bridging systems, and boat systems. These concepts will be further refined as the Army develops requirements.

MISSION

Army commanders intend to use the CTT to deliver all classes of supply, bridging, irregularly shaped cargo, and containerized cargo across all tactical mobility environments, as far forward on the battlefield as the mission requires. CTT FoV variants will employ modern military and commercial technology while conducting line-haul and local-haul operations as well as self-load and -unload of standard flat racks, bridging assets, and shipping containers in order to enhance the commander's operational flexibility when delivering cargo.

PROGRAM

The Army Acquisition Executive designated the CTT program as an MTA rapid prototyping effort in January 2023. The CTT program is managed by the Program Executive Office, Combat Support and Combat Service Support (PEO CS&CSS). DOT&E placed the program on oversight in February 2023 and approved the TES in April 2024.

The Army conducted an Ops Demo in August through September 2024. The results will inform the PEO CS&CSS for future requirements development while assessing the current state of truck technology. The prototypes will be returned to the vendors following the Ops Demo. The Army will release a request for proposals in FY26 for test assets. The CTT program is aiming to transition to the major capability acquisition pathway at MS C in FY28 and begin low-rate initial production (LRIP). The Army is requesting funding to produce 7,217 CTTs by FY35, pending future approved Army Acquisition Objective requirements.

» MAJOR CONTRACTORS

Major contractors supporting MTA-RP phase:

- American Rheinmetall Vehicles, LLC – Sterling Heights, Michigan
- Mack Defense, LLC – Allentown, Pennsylvania
- Navistar Defense, LLC – Madison Heights, Michigan
- Oshkosh Defense, LLC – Oshkosh, Wisconsin

TEST ADEQUACY

The Army completed an Ops Demo in August and September 2024 to obtain soldier feedback on the operation of the twelve CTT prototypes (three per vendor), including an assessment of the integration of commercial safety systems, and inform CDD requirements. DOT&E provided input to the Ops Demo and observed it, but the test plan did not require DOT&E approval, as the intention was to inform requirements, not a preliminary assessment. The Ops Demo was not intended to support an assessment of operational effectiveness, suitability, or survivability, but it did provide the Army insight on performance, safety, reliability, interoperability limitations, and capabilities. DOT&E expects the Army to submit a MS C TEMP in FY28.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

The Ops Demo was not intended to provide sufficient data to assess operational effectiveness or suitability, only to provide the Army insight on performance, safety, reliability, interoperability limitations, and capabilities of the commercial protypes that will help shape the CDD requirements. The current data available are insufficient to provide a preliminary assessment of CTT operational effectiveness and suitability. DOT&E will report on CTT's progress towards operational effectiveness and suitability prior to program transition from the MTA rapid prototyping pathway.

» SURVIVABILITY

The Army is not testing the survivability of the CTT prototypes during the MTA rapid prototyping phase, because these systems will not be fielded. The prototypes will be returned to the vendors and the Army will issue a new competitive contract to develop test assets for MS C and LRIP production. The Army will conduct limited testing to support a single vendor contract award. The Army will complete cyber and kinetic survivability testing after the program transitions to MS C.

RECOMMENDATIONS

The PEO CS&CSS should:

1. Continue developing the CDD for CTT.
2. Develop a MS C TEMP to support the MS C decision in FY28.

Directed Energy Maneuver-Short Range Air Defense (DE M-SHORAD)

In February 2024, the Army deployed the four Directed Energy Maneuver-Short Range Air Defense (DE M-SHORAD) prototype vehicles to support OCONUS operations. This deployment prevented the start of scientific and technical testing planned by the Rapid Capabilities and Critical Technologies Office (RCCTO). In June 2024, the Army Test and Evaluation Command (ATEC) conducted a three-day controlled assessment during the unit's OCONUS deployment. The limited data from this event will not be adequate to support DOT&E's early assessment of the system's operational effectiveness, lethality, suitability, and survivability. The Army continues collecting relevant operational insights by conducting an In-Theater Assessment (ITA) during the unit's OCONUS deployment.

SYSTEM DESCRIPTION

The DE M-SHORAD integrates sensor and shooter capabilities onto a Stryker Mortar Carrier Double V-Hull A1 vehicle to defend supported forces against unmanned aircraft systems that are within Groups 1 – 3; fixed- and rotary-wing aircraft threats; and rockets, artillery, and mortars. The primary weapon is a 50-kilowatt spectral beam combined laser, powered by lithium nickel cobalt aluminum oxides (Li-NCA) batteries that are recharged by diesel generators onboard the vehicle.

DE M-SHORAD is planned to augment M-SHORAD Increment 1 vehicles armed with kinetic weapons (e.g., Stinger missiles, 30mm chain gun, and 7.62mm machine gun) as part of short-range air defense (SHORAD) battalions.

MISSION

Commanders will employ the DE M-SHORAD units and vehicles to provide air defense to maneuver units and fixed sites across the battlespace. The vehicle will be used to defeat unmanned aerial systems, rockets, artillery and mortar rounds, and fixed- and rotary-wing aircraft. DE M-SHORAD vehicles are organized as platoons of four vehicles assigned to Army SHORAD battalions.

PROGRAM

DE M-SHORAD is a prototyping effort led by RCCTO under their Other Transaction Authority. The program does not have an acquisition strategy and it's undetermined when the DE M-SHORAD will transition to an acquisition pathway. The Army has procured four prototype vehicles and awarded an Other Transaction Authority contract for two additional prototype vehicles of similar design.

- In May 2019, the Secretary of the Army initiated the DE M-SHORAD program, approving the initial Directed Energy Strategy and directed RCCTO's Directed Energy Program Office to develop and deliver the DE M-SHORAD prototype system.
- In September 2023, after completing contractor and government acceptance testing, RCCTO delivered four prototype DE M-SHORAD vehicles to the 4-60th Short-Range Air Defense Artillery Battalion at Fort Sill, Oklahoma, establishing the first DE M-SHORAD platoon.
- In January 2024, the Army Aviation and Missile Command issued an urgent materiel release authority for the first four prototypes. The Air Transportability Test Loading Agency awarded C-17 transportability certification in January 2024.

DOT&E placed the DE M-SHORAD program on oversight in March 2024. The program does not have a DOT&E-approved TES.

The Army deployed the DE M-SHORAD prototype vehicles OCONUS to support ongoing operations. Since the vehicles have been placed into operational use during the OCONUS deployment, DOT&E is required to publish an early fielding report, which will be released in FY25.

» MAJOR CONTRACTORS

- Kord Technologies, Inc., a wholly owned subsidiary of KBR, LLC – Huntsville, Alabama
- RTX – Arlington, Virginia
- General Dynamics Land Systems – Warren, Michigan

TEST ADEQUACY

In February 2024, the Army deployed the four DE M-SHORAD prototype vehicles to support OCONUS operations. This deployment prevented RCCTO from starting the scientific and technical testing planned for FY24. Adequate testing to demonstrate DE M-SHORAD's operational effectiveness, lethality, suitability, and survivability cannot begin until either the prototype vehicles return to CONUS or the additional prototype vehicles are built and delivered to the Army.

In June 2024, ATEC conducted a three-day controlled assessment. The test plan was not provided to DOT&E for review and approval, nor was it observed by DOT&E. Given the limited data, DOT&E is unable to provide an early evaluation of DE M-SHORAD's operational effectiveness, lethality, suitability, and survivability.

The Army is utilizing the deployment to conduct an ITA of DE M-SHORAD. The ITA is not being conducted in accordance with a test plan, nor being observed by ATEC or DOT&E.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

DOT&E has insufficient data to assess DE M-SHORAD's operational effectiveness, lethality, suitability, and survivability. Since the vehicles have been placed into operational use during the OCONUS deployment, DOT&E is required to publish an early fielding report, which will be released in FY25.

RECOMMENDATION

The Army should:

1. Develop a TES for DOT&E's approval to adequately assess DE M-SHORAD's operational effectiveness, lethality, suitability, and survivability.

Dismounted Assured Positioning, Navigation, and Timing System (DAPS)

In November 2023, the Army conducted Dismounted Assured Positioning, Navigation, and Timing System (DAPS) GEN II IOT&E. The DAPS GEN II IOT&E was conducted in accordance with a DOT&E-approved test plan and was adequate to inform a full-rate production (FRP) decision. DOT&E published a classified IOT&E report in May 2024, and the Program Executive Officer, Intelligence, Electronic Warfare and Sensors (PEO IEW&S) approved the DAPS GEN II FRP in August 2024.

SYSTEM DESCRIPTION

DAPS is a handheld Military-Code (M-Code) GPS receiver that integrates multiple Positioning, Navigation, and Timing (PNT) sources to provide Army forces with access to trusted PNT information in conditions where GPS signals may be degraded or denied. DAPS supports the Army's transition to M-Code GPS and will replace the Defense Advanced GPS Receiver (DAGR) currently used by Nett Warrior equipped soldiers.

DAPS GEN 1.0 includes a boot attached inertial module to improve position and navigation accuracy based on soldier footsteps. Soldiers interface with the DAPS GEN 1.0 using the Nett Warrior End User Device (EUD). DAPS GEN 1.2 has an internal rechargeable battery as well as internal inertial module and alternative satellite reception capabilities. DAPS GEN 1.2 can be used in a stand-alone mode or with the Nett Warrior EUD interface. DAPS GEN II is an improved version of DAPS GEN 1.2 with an external rechargeable battery, redesigned screen and soldier interface, and improved PNT data fusion capability. DAPS GEN II can be used in a stand-alone mode, with the wrist-wearable device, or with the Nett Warrior EUD interface.

The Army is experimenting with the DAPS GEN II in a vehicle-mounted configuration to determine if the DAPS would be suitable to replace DAGR in some mounted applications.

MISSION

A unit equipped with DAPS will use their trusted PNT information to conduct operations in conditions that impede or deny access to GPS signals, such as dense vegetation, built-up urban and mountainous terrain, and in the presence of electromagnetic interference or enemy electronic warfare.

PNT information derived from the DAPS directly enables positioning of forces; navigation across the operational environment; communication networks; situational awareness applications; and protection, surveillance, targeting, and engagement systems that contribute to combined arms maneuver.

PROGRAM

DAPS GEN 1.0 and DAPS GEN 1.2 are quick reaction capabilities developed in response to an Army-directed requirement that culminated in a limited equipping of four infantry brigade combat teams (IBCT). As of 4QFY24, one IBCT has been equipped with 754 DAPS GEN 1.0 units and three IBCTs have been equipped with 2471 DAPS GEN 1.2 units. All DAPS GEN 1.0 and GEN 1.2 deliveries are complete.

In early FY22, the Army selected TRX Systems Inc. as the vendor for the DAPS GEN II rapid prototyping program. In March 2023, DAPS GEN II transitioned from rapid prototyping to a major capability acquisition program at Milestone C with an updated DOT&E-approved TEMP. In November 2023, the Army conducted the DAPS GEN II IOT&E, and in August 2024, PEO IEW&S approved the DAPS program to proceed to FRP. In May 2024, DOT&E published a classified IOT&E report supporting the Army's FRP decision. The DAPS GEN II program is on track to achieve initial operational capability by March 2025. The DAPS TEMP is being updated to support post-FRP decisions and T&E activities.

» MAJOR CONTRACTORS

- Integrated Solutions for Systems, Inc. – Auburn, Alabama (DAPS GEN 1.0)
- TRX Systems Inc. – Greenbelt, Maryland (DAPS GEN 1.2 and DAPS GEN II)

TEST ADEQUACY

In November 2023, the Army conducted the DAPS GEN II IOT&E and cyber survivability adversarial assessment at Fort Huachuca, Arizona, in accordance with a DOT&E-approved test plan and TEMP. The IOT&E and adversarial assessment were observed by DOT&E and were adequate to determine that DAPS GEN II is operationally effective, suitable, and survivable. The Army addressed FY23 Annual Report recommendations to verify deficiency corrections prior to conducting the IOT&E.

PERFORMANCE

» EFFECTIVENESS

The DAPS GEN II is operationally effective, though exhibited decreased position and notification accuracy under very challenging threat environments. The DAPS GEN II performs better than the legacy DAGR in GPS-contested environments and improves soldiers' situational awareness, supports navigation, and allows the unit to maintain operational tempo while moving between mission objectives. Additional details are contained in the May 2024 classified IOT&E report.

» SUITABILITY

The DAPS GEN II is operationally suitable. The DAPS GEN II experienced no essential function failures during the IOT&E. The most prevalent non-essential function failure was due to software integration issues with the wrist-wearable device. Operational availability was 99 percent, due to the rapid reparability of faults. Failure modes found during previous testing had been corrected prior to IOT&E, which improved the system's overall reliability. Training was sufficient for soldiers to operate the DAPS GEN II, though they expressed the need for training on how to adjust the threat notification frequency and sensitivity. Additional details are contained in the May 2024 classified IOT&E report.

» SURVIVABILITY

The DAPS GEN II is cyber survivable to outsider and nearsider threats. The DAPS program mitigated vulnerabilities found during previous testing, minimizing an adversary's attack opportunities. Additional details are contained in the May 2024 classified IOT&E report.

RECOMMENDATIONS

The Army should:

1. Improve the DAPS GEN II ability to determine GPS signal assurance and valid position location under very challenging GPS threat environments.
2. Add a training module on adjusting threat notification parameters.
3. Improve DAPS GEN II software integration with the wrist-wearable device.

Extended Range Guided Multiple Launch Rocket System/Guided Multiple Launch Rocket System Alternative Warhead (ER GMLRS/GMLRS AW)

In October 2023, the Army executed three system qualification test (SQT) shots of the Extended Range Guided Multiple Launch Rocket System (ER GMLRS). The program continued to experience reliability failures with the new side-mounted proximity sensor (SMPS), predominantly on the ER GMLRS Alternative Warhead (AW) variant. The SMPS enables an optimal height of burst (HOB) for both the ER GMLRS AW and Unitary warhead variants.

In November 2023, the Army delayed additional testing of the ER GMLRS AW variant and ER GMLRS Unitary with height of burst mode, pending development of a redesigned SMPS. The Army Acquisition Executive also approved the transition of ER GMLRS from an engineering change proposal (ECP) to a subprogram under the GMLRS program and entry into Milestone C (MS C) in FY26. In February 2024, the Army conducted one mission of the planned ER GMLRS operational test with only the Unitary warhead variant in point detonate mode.

The Army plans to continue testing with three additional ER GMLRS SQT shots with the AW variant in 2QFY26 and complete operational testing with two multiple rocket missions with both ER GMLRS AW and Unitary variant rocket 4QFY26 to include the redesigned SMPS.

In August 2024, the Army decided ER GMLRS will enter a full-rate production (FRP) decision 1QFY27. Since ER GMLRS will be a subprogram under the GMLRS program and will start at MS C, DOT&E will write an ER GMLRS operational assessment to inform the FY26 MS C decision. Following integration and testing of the new ER GMLRS SMPS, DOT&E will publish an ER GMLRS IOT&E report that encompasses all production representative testing of ER GMLRS to inform the FRP decision in 1QFY27.

SYSTEM DESCRIPTION

The ER GMLRS is a GPS-guided, all-weather, day-night, surface-to-surface long-range precision rocket. It is designed to increase the maximum range from 70 kilometers out to 150 kilometers, enhance maneuverability, adjust the attack trajectory to vertical at select ranges, and incorporate an SMPS to enable an optimal HOB for both the ER GMLRS Unitary and AW rocket variants.

Both the ER GMLRS Unitary and AW variants have a 200-lb class high explosive warhead. The Unitary warhead produces blast fragmentation upon detonation and the AW accelerates two layers of preformed penetrators upon detonation. The ER GMLRS has multiple warhead detonation modes. The Unitary rocket is capable of HOB detonation at a commanded distance above the ground, point detonation upon target impact, and delay detonation after a commanded delay time following target impact has elapsed. The Army intends to employ the AW rocket in HOB detonation mode only.

MISSION

Army commanders will use the ER GMLRS rockets to engage point or area targets, including air defense, command posts, and high value targets, without the hazard of unexploded sub munitions.

PROGRAM

In June 2017, the Army initiated the ER GMLRS program as an ECP to the ER GMLRS AW and Unitary rockets. In August 2020, DOT&E approved the ER GMLRS TEMP Annex. The program experienced numerous delays caused by design issues, temporary facility shutdowns due to COVID-19, and production line issues.

Between October 2022 and November 2023, the program experienced reliability failures with the new SMPS during integrated testing, predominantly with the ER GMLRS AW variant. In November 2023, the Army delayed additional testing of the ER GMLRS AW variant, pending development of a redesigned SMPS. All testing was in accordance with the approved TEMP Annex.

In November 2023, the Army Acquisition Executive approved the transition of ER GMLRS from an ECP to a subprogram under the GMLRS program with entry at MS C in 3QFY25. In 1QFY25, the MS C decision shifted until the redesign of the SMPS and remaining integrated test shots are completed with the redesigned SMPS in FY26.

In January 2024, the Army approved initial fielding of the ER GMLRS Unitary variant in point detonate mode. In February 2024, the Army conducted one mission of the planned operational test with two ER GMLRS Unitary rockets in point detonate mode to support their ER GMLRS Unitary fielding decision. The ER GMLRS Unitary height of burst and the AW variant was not part of the operational test due to the SMPS reliability failures.

Following integration of the redesigned SMPS into the ER GMLRS, the Army plans to conduct three additional SQT shots with the ER GMLRS AW variant rocket 2QFY26 and continue the operational testing with two multiple rocket missions with both ER GMLRS AW and Unitary variant rockets 4QFY26, with the redesigned SMPS. DOT&E will publish an IOT&E report that encompasses all production representative testing of the ER GMLRS to inform the FRP decision of 1QFY27.

» MAJOR CONTRACTOR

- Lockheed Martin Missiles and Fire Control – Grand Prairie, Texas (assembled in Camden, Arkansas)

TEST ADEQUACY

The testing of the ER GMLRS to date is incomplete to assess operational effectiveness, lethality, suitability, and survivability. The ER GMLRS TEMP Annex, approved by DOT&E in August 2020, includes a test program with 14 test rockets (with spares) 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. The Army does not plan to test ER GMLRS Unitary in delay mode before fielding it to units. The Army continues to refine testing for employment of different threat electronic warfare countermeasures. The Army should test without terrain masking during future electronic warfare test shots.

In February 2024, DOT&E approved the test plan for the first mission of the ER GMLRS operational and evaluation test in accordance with the DOT&E-approved TEMP Annex. DOT&E requested the Army provide updates on the program's acquisition strategy, planned modifications to the SMPS, and the timing of the material release and details for fielding Unitary and AW variants. DOT&E also recommended the Army update the ER GMLRS TEMP Annex and resubmit it for approval prior to a future MS C decision.

In February 2024, the Army conducted one mission of the planned ER GMLRS operational test with two Unitary rockets in point detonate mode at White Sands Missile Range, New Mexico. The Army conducted the first mission of the ER GMLRS operational test in accordance with the DOT&E-approved test plan, which was observed by DOT&E. The test consisted of new equipment training, a pilot test, and a flight test phase. During the pilot test, soldiers executed dry fire missions, reload operations, and survivability moves. During the flight test phase, soldiers executed a multiple rocket mission against a threat representative target with ER GMLRS Unitary variant rockets in point detonate mode.

In FY26, DOT&E will publish an operational assessment report, based upon ER GMLRS testing to date with the old SMPS design and the redesigned SMPS, to support the Army's MS C decision FY26.

Following integration of the redesigned SMPS into the ER GMLRS, the Army plans to conduct three additional SQT shots with the ER GMLRS AW variant rocket and two multiple rocket missions with both ER GMLRS AW and Unitary variant rockets. The Army projects execution of the ER GMLRS SQT shots 2QFY26 and the remaining missions of the operational testing 4QFY26. DOT&E will publish an IOT&E report that encompasses all production representative testing of the ER GMLRS testing, to inform the FRP decision in 1QFY27.

PERFORMANCE

» EFFECTIVENESS

Insufficient data are available to evaluate the operational effectiveness of the ER GMLRS. During testing to date, the Army has demonstrated ER GMLRS is accurate and capable of exceeding the legacy objective range requirement of 70 kilometers.

The Army experienced increased mission processing times of ER GMLRS fire missions that could negatively impact the timely delivery of fires. The Army is investigating the cause and potential solutions related to this issue.

» LETHALITY

Insufficient data are available to evaluate the lethality of the ER GMLRS against threat representative targets.

The ER GMLRS warhead lethality is dependent on HOB, angle of fall, and target location error. All lethality data collected to date with a HOB are from AW and Unitary rockets with the old SMPS that is undergoing redesign and replacement.

The Unitary rockets in point detonate mode had good effects against the threat representative target during the operational test event in February 2024.

» SUITABILITY

Insufficient data are available to evaluate the suitability of the ER GMLRS.

As of the testing to date, the ER GMLRS has not demonstrated its key performance parameter reliability requirement with statistical confidence. Additional flight tests may be required to demonstrate reliability depending upon the impact of the redesigned SMPS on the ER GMLRS production representative configuration.

» SURVIVABILITY

The Army conducted a cooperative vulnerability and penetration assessment in October 2023 and Phase 1 of an adversarial assessment in January 2024. The Army used the findings from these two events to inform the Army's execution of Phase 2 of the adversarial assessment, concurrent with the limited operational test event in February 2024. DOT&E will publish a classified report on its findings prior to the Army's planned MS C decision in FY26

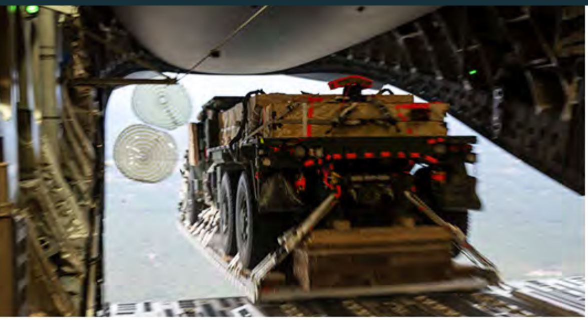
Additional cyber survivability testing may be required, depending upon the impact of the redesigned SMPS on the ER GMLRS production representative configuration.

RECOMMENDATIONS

The Army should:

1. Continue to provide the ER GMLRS T&E stakeholders with regular updates on the planned modifications to the SMPS.
2. Continue to coordinate for employment of different threat electronic warfare countermeasures without terrain masking during the remaining IOT&E shots.
3. Publish a revised ER GMLRS TEMP Annex for DOT&E approval.
4. Continue to develop a plan to demonstrate the key performance parameter reliability requirement with statistical confidence.
5. Consider testing ER GMLRS Unitary rockets in delay mode.
6. Due to changes in the acquisition schedule, the Army must allow adequate time for DOT&E assessment and reporting to inform the FRP decision.

Family of Medium Tactical Vehicles A2 (FMTV A2)



Following the FOT&E conducted in April 2023, the Family of Medium Tactical Vehicles A2 (FMTV A2) manufacturer implemented vehicle design changes to improve reliability and maintainability based on issues identified in previous testing. In October 2023, DOT&E published a combined FOT&E and LFT&E report with classified annex. From November 2023 through June 2024, the Army conducted live fire and airdrop testing of the FMTV A2 Medium Tactical Vehicle (MTV) cargo truck Low Velocity Air Drop (LVAD) variant. DOT&E observed the live fire testing and assessed that the MTV cargo truck LVAD variant with armor demonstrates the same survivability as the baseline FMTV A2 trucks. DOT&E observed the LVAD events which the Army used to certify the FMTV A2 MTV cargo truck LVAD variant for airdrop from U.S. Air Force (USAF) C-17 and C-130 aircraft. The Army plans to complete the airdrop testing and certifications of the Light Medium Tactical Vehicle (LMTV) cargo truck LVAD and MTV dump truck LVAD variants by 2QFY25.

SYSTEM DESCRIPTION

The FMTV transports a wide variety of cargo, such as containers, pallets, flat racks, general supplies, personnel, and equipment, to and within tactical units, as well as resupply to forward areas. FMTVs are designed to operate worldwide on primary and secondary roads, trails, and cross-country terrain of all surface types in all weather conditions. During peacetime operations, the FMTV A2 is required to operate primarily on highways, consistent with commercial practices for trucks in this payload range.

FMTV variants are based on two common chassis with varied payloads and mission equipment. The trucks can be produced with or without the armored cab and operated with or without an underbody armor protection kit. Additional kits include a materiel handling crane and a self-recovery winch. The following variants are available on each FMTV chassis:

- LMTV chassis – a 3-ton cargo truck, a 2.5-ton van, and a 3-ton LVAD cargo truck.
- MTV chassis – an 8-ton cargo truck, an 8-ton cargo truck with an extended cargo bed, a tractor, an 8-ton LVAD cargo truck, an expansible van, a 7-ton LVAD dump truck, a wrecker, an 8.8-ton load handling system (LHS) truck, and a 10-ton dump truck.

LVAD variants have a non-armored collapsible cab that enables transporting the vehicle on USAF C-130 and C-17 aircraft and airdropped to support airborne operations. Armor must be installed post-drop to achieve kinetic protection.

The Army further modifies these standard variants for specific missions. Currently, air defense units will use modified MTV cargo trucks to carry equipment for the Sentinel Radar and the Army Integrated Air and Missile Defense system. Earlier models of the FMTV were adapted to carry the Medium Extended Air Defense Systems and the High-Mobility Artillery Rocket System.

The FMTV A2 also includes three types of companion FMTV trailers: an LMTV trailer, an MTV trailer, and an LHS trailer. The FMTV trailers were not redesigned or modified for use with the FMTV A2. The MTV tractor pulls all standard Army semi-trailers up to the 40-ton class, including the low-bed construction equipment transport, flatbed cargo, and fuel tank semitrailers.

The FMTV A2 is an integration of commercially based components and a continuation of the same capabilities and interfaces available with the existing FMTV fleet. The design incorporates a set of hardware and software improvements, upgrades to expand truck capabilities, and includes:

- Increased cargo-carrying capacity. Earlier models of the LMTV and MTV trucks carried a maximum cargo load of 2.5 and 5 tons, respectively.
- Improved mobility from increased engine horsepower, an adjustable suspension system, and higher wheel capacity.
- Upgraded vehicle data bus with a simplified electrical system that supports improved

LMTV cargo truck conducting a resupply mission during the FOT&E at Fort Bliss, Texas diagnostic and troubleshooting capabilities and future upgrades.

- Increased electrical power capacity to support current operations and provide growth potential for future upgrades.
- Enhanced vehicle safety with Electronic Stability Control incorporated into the anti-lock braking system.
- Augmented crew survivability with the armor protection of the FMTV A1P2 and a new underbody armor protection kit.

MISSION

The Army employs the FMTV to provide multi-purpose transportation and mobility in maneuver, maneuver support, and sustainment units. Transportation and supply units conduct line and local haul missions carrying cargo, soldiers, and equipment with the LMTV and MTV cargo trucks and their associated LMTV and MTV trailers. Medical units employ the MTV LHS and FMTV LHS trailer to transport, load, and offload shipping containers with unit equipment. Maintenance units use the MTV wrecker to recover all immobile light- and medium-wheeled vehicles, including all FMTV variants. Engineering units employ the MTV dump truck to haul and dump construction material during quarry operations. Airborne units use the LVAD MTV cargo truck, LVAD MTV dump truck, and LVAD LMTV cargo truck variants to move soldiers, equipment, supplies, and construction materials during airborne operations, aerial resupply, and airfield repair operations.

PROGRAM

The FMTV A2 is an Acquisition Category IC program. DOT&E approved the Army's operational test plan for the FOT&E for all variants except the three LVAD vehicles in March 2023 and published a combined FOT&E and LFT&E report with classified annex in October 2023, assessing its operational effectiveness, suitability, and survivability.

During FY24, the FMTV A2 LVAD cab, which is identical across all three LVAD trucks, underwent live fire testing, which included underbody and side improvised explosive device threats and exploitation testing. DOT&E will publish a classified LFT&E report with the results of this testing in 2QFY25.

The FMTV LVAD MTV cargo truck airdrop testing was conducted from November 2023 through August 2024. The airdrop testing of the FMTV A2 LVAD MTV cargo truck observed by DOT&E during FY24 confirmed our previous assessment that the FMTV A2 is operationally effective and suitable. The FMTV A2 LVAD LMTV cargo truck and MTV dump truck airdrops are scheduled to begin in 1QFY25 and completed in 2QFY25.

Testing will support a full materiel release decision in 3QFY26. In accordance with the DOT&E-approved TEMP for the FMTV A2 program, only the test plan for the LFT&E of the LVAD variants required DOT&E's approval.

The Army will procure 2,691 FMTV A2s on the current base contract, which expires in February 2025. The Army plans on a 3-year extension contract expiring in FY28 with a planned, competitive, follow-on contract starting production in FY28 for quantities yet to be determined based on Army objectives. To date, Oshkosh has produced 1087 FMTV A2s. Unit fielding will start in 1QFY25 and continue through FY41 and

FMTV A2 MTV Cargo Truck Low-Velocity Air Drop Variant beyond, until the Army Acquisition Objective is complete. The Army is still determining the exact quantities of each variant, but it is expected that the LMTV and MTV cargo trucks will be procured in the greatest quantities.

» MAJOR CONTRACTOR

- Oshkosh Defense, LLC – Oshkosh, Wisconsin

TEST ADEQUACY

Following the FOT&E conducted in April 2023, the Army has implemented modification work orders to correct deficiencies identified in previous testing, which included exchanging fuel-sending units, adding an additional oil passage in the wheel ends to aid in lubrication and heat dissipation, and rerouting wiring harnesses and hoses to avoid abrasion. Oshkosh is developing an engineering change proposal to fix the accuracy of the fuel level sending unit.

From November 2023 through February 2024, the Army Test and Evaluation Command conducted airdrop testing of the FMTV A2 MTV cargo truck LVAD variant at Fort Liberty, North Carolina, to collect the required data to certify airdrop from for the USAF C-17 and C-130 aircraft. Since the airdrops are developmental testing, the Army provided the test plan to DOT&E for awareness prior to conducting these tests. DOT&E observed the airdrop tests completed in FY24.

Live Fire Test of the FMTV A2 MTV Cargo Truck Low-Velocity Air Drop Variant

From December 2023 through June 2024, the Army conducted LFT&E to confirm the LVAD cabdid not degrade force protection and vehicle survivability against the expected kinetic threats. Specifically, the Army conducted ballistic exploitation of the LVAD cab against small arm threats, side improvised explosive devices, and one under-vehicle blast mine test of the MTV LVAD cargo truck. The Army executed the LFT&E at Aberdeen Proving Ground, Maryland, in accordance with DOT&E-approved test plans. DOT&E observed these tests, which were adequate to assess the LVAD vehicle's survivability. DOT&E will publish a classified LFT&E report with the results of this testing in 2QFY25 to support the full materiel release decision.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

In FY24, the Army demonstrated the FMTV A2 MTV LVAD cargo truck variant could be successfully airdropped from the USAF C-17 and C-130 aircraft with no major vehicle damage. The Army's airdrop certification of the FMTV A2 MTV cargo truck LVAD variant consisted of a tie-down and suspension provision testing and Simulated Airdrop Impact Testing at Fort Liberty, North Carolina to demonstrate the vehicle's rigging procedures for airdrop. The FMTV A2 MTV cargo truck LVAD variant successfully completed these tests and was cleared for airdrop testing from an aircraft in November 2023.

The Army conducted three airdrop events for the FMTV A2 MTV cargo truck LVAD variant in December 2023 (USAF C-17), January 2024 (USAF C-130), and February 2024 (USAF C-17). All three drops were successful, and no major vehicle damage occurred. After each airdrop, soldiers drove the FMTV A2 MTV cargo truck LVAD variant 30 miles over paved and unpaved terrain to demonstrate its availability to immediately support airborne operations. Then the vehicles were placed in an aircraft hangar overnight to determine if the airdrop and subsequent vehicle operations caused any leaks and to inspect for damages. The Army plans to certify the LMTV LVAD cargo truck and MTV dump trucks for airdrop from C-17 and C-130 aircraft by 2QFY25.

» SURVIVABILITY

The armored FMTV A2 LVAD cab and MTV cargo truck demonstrated the same survivability to kinetic threats as the non-LVAD armored FMTV A2 vehicles. The FMTV A2 vehicle's protection, to include the LVAD variants, against the expected kinetic threats remains unchanged.

RECOMMENDATIONS

The Army should:

1. Continue to address DOT&E's recommendations from the FY23 Annual Report and the October 2023 combined FOT&E and LFT&E report for the FMTV A2.
2. Complete the remaining LVAD events required to certify the FMTV A2 LVAD LMTV cargo and LVAD MTV dump truck variants for airdrop by USAF C-17 and C-130 aircraft.

Future Unmanned Aircraft System – Air Launched Effects (FUAS ALE)

In FY24, the Army continued rapid prototyping efforts for the Future Unmanned Aircraft System – Air Launched Effects (FUAS ALE) program through the Middle Tier of Acquisition (MTA) rapid prototyping acquisition strategy. Consistent with their acquisition strategy, the Project Manager Uncrewed Aircraft Systems requested and was granted an extension of the MTA from three years to five years. The updated timeline will enable the program to conduct an operational demonstration (Ops Demo) in 4QFY26. An updated abbreviated Capability Development Document approved in 3QFY24 will inform requirements for this Launched Effects (LE) program.

SYSTEM DESCRIPTION

Air Launched Effects (ALE) are a family of systems designed to autonomously or semi-autonomously deliver effects as a single agent or as a member of a team. ALE is a key element to the success of the Future Vertical Lift ecosystem. ALE provides capabilities beyond a traditional intelligence, surveillance, and reconnaissance role. ALE will address capability gaps in defeating enemy Integrated Air Defense Systems, electronic warfare, and Integrated Fires Complexes, when conducting operations in a peer anti-access/area denial environment.

The defeat of these anti-access/area denial capabilities allows Army Aviation to effectively support large-scale combat operations and multi-domain operations in 2028 and beyond.

ALE will extend tactical and operational reach, lethality, and protection as an attritable or optionally recoverable aircraft. The operational intent of the ALE is to detect, identify, locate, and report threats. Moreover, ALE will present a credible decoy, disrupt threat communications, targeting and acquisition systems, and deliver lethal and non-lethal effects across multiple scenarios and domains in a multi-domain operations environment.

The initial ALE prototype system consists of a common air vehicle, mission system, payloads, laptop equipped with scalable control interface software, and associated support equipment. The payloads are modular and interchangeable and allow the User the ability to adapt to each mission need. Two payloads will be part of the current system, to include a decoy payload and a detect, identify, locate, and report payload. An Anduril Altius roll release canister carries the ALE on the host platform.

MISSION

The ALE is capable of pre-mission planning, dynamic re-tasking, receiving mission updates before and after launch, and providing battlefield updates (including battle damage assessment). ALE can operate as a single asset, or as a member of a coordinated team or swarm. When operating as a swarm, ALE can leverage multiple systems of the same effect, concentrating on a system target or threat from multiple directions to increase the magnitude of the effect. Through high levels of system autonomy, ALE can self-optimize to redistribute tasks upon loss or gain of a team member. ALE executes assigned missions consistent with commander's intent without requiring direct intervention from a manned operator or higher echelon unmanned command platform in the loop. Upon launch, ALE utilizes the Integrated Tactical Network to distribute reconnaissance, surveillance, and target acquisition data to populate the common operational picture shared throughout the battlefield.

ALE is a crucial piece of the advanced teaming concept synergistically enhancing survivability, threat identification, targeting and lethality of Army Combat Aviation Brigades and ground force assets. ALE deploys as the forward most element of the advanced team in areas of expected enemy contact in order to initiate Integrated Air Defense System. During mission execution, the advanced team employs all or some of the ALE capabilities (detect, identify, locate, report, decoy, disrupt, lethal) dependent on the nature of the environment and opposing threat scenarios.

PROGRAM

The FUAS ALE program uses the MTA rapid prototyping approach. DOT&E has not yet approved a TES for FUAS ALE MTA rapid prototyping. An Ops Demo was scheduled for 4QFY24 to inform a transition to an MTA rapid fielding approach. The Ops Demo was canceled. However, the Project Manager Uncrewed Aircraft Systems requested and was granted an extension of the MTA from three years to five years. The updated timeline will enable the program to conduct the Ops Demo in 4QFY26. The residual capabilities of the program upon completion of the MTA rapid prototyping in 4QFY24 are: (1) technical data from the vendors to inform future LE MTA rapid prototyping efforts in support of further developing LE for the Army, (2) 16 air vehicles are slated for be sent to the 160th Special Operations Aviation Regiment for further testing and development; the number of systems may be reduced based on the number of air vehicles that are salvageable post flight tests.

» MAJOR CONTRACTORS

- Anduril – Atlanta, Georgia
- Collins Aerospace, a subsidiary of RTX – Cedar Rapids, Iowa
- Northrop Grumman Corporation – Northridge, California
- Technology Service Corporation – Huntsville, Alabama
- Aurora Flight Sciences, a subsidiary of The Boeing Company – Manassas, Virginia

TEST ADEQUACY

The lack of program maturity and operational testing precludes DOT&E from making a preliminary assessment of FUAS ALE's test adequacy. The program was not able to conduct a scheduled Ops Demo in FY24, due to unspecified issues with the system. The system went through a vendor-led Host Platform flight test in September 2024. The test successfully demonstrated limited capability of the air vehicle, to include the following capabilities: launch from a MH-60, scalable control interface with dynamic re-tasking, and auto-land recovery.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

The lack of program maturity and operational testing precludes DOT&E from making a preliminary assessment of the operational effectiveness, suitability, or survivability of FUAS ALE.

» LETHALITY

The lack of program maturity and operational testing precludes a preliminary assessment of Future Unmanned Aircraft System-Air Launched Effects lethality. The FUAS ALE program is not intended as a lethal option for the Army, instead this program was directed to produce payloads with capability to serve as a decoy or as a detect, identify, locate, and report effects.

RECOMMENDATION

The Army should:

1. Document lessons learned from the current MTA rapid prototyping efforts and provide those lessons across the enterprise to inform similar rapid prototyping efforts and ensure interoperability that span multiple Program Executive Offices across the Army and the Services.

HERCULES M88 Upgrade Recapitalization (M88A3)

The Heavy Equipment Recovery Combat Utility Lift and Evaluation System (HERCULES) M88 Upgrade Recapitalization (M88A3) upgrades powerpack, suspension, hoist, and winch of the existing M88A2 to recover the heaviest systems across the Army. In July 2024, the Army's M88A3 equipped crew executed a Soldier Touchpoint, demonstrating single vehicle recovery, and turret lift and carry, of an 80-ton Abrams main battle tank. In August 2024, the Army began full-up system-level (FUSL) live fire events, which are expected to complete in 3QFY25. Upgrades will be applied to the initial run of production vehicles in 3QFY25. FOT&E is scheduled for 2QFY27.

SYSTEM DESCRIPTION

The M88A3 is an upgrade to the existing M88A2, which supports units performing armored vehicle repair and recovery. The Army's support battalions require an organic recovery vehicle with mobility, survivability, lift, winch, and tow capabilities necessary to effectively recover the heaviest tracked vehicles in the Army. The M88A3 will fill the M88A2's capability gap of Single Vehicle Recovery of 80-ton vehicles with upgrades applied primarily to the powerpack, suspension, hoist, and winch.

MISSION

Commanders employ the M88A3 to provide single vehicle towing, winching, and hoisting operations and evacuation of heavy tanks and other tracked combat vehicles. The M88A3-equipped units will operate as part of the brigade support battalion in both the field maintenance company and forward support company, service and recovery sections providing field-level maintenance and recovery support to maneuver battalions. M88A3-equipped units will perform recovery operations in support of combat-equipped M1, M1A1, and M1A2 Abrams Main Battle Tank platforms and future heavy combat vehicles. Recovery operations will also cover lighter systems across the armored brigade combat team (e.g., Armored Multi-Purpose Vehicle, Bradley Fighting Vehicle, Joint Assault Bridge, Armored Vehicle-Launch Bridge, and Composite Joint Assault Bridge). Disabled combat vehicle recovery will be conducted if the disabled vehicle cannot be repaired on the spot. The M88A3 will tow the disabled vehicle to a maintenance collection point based on mission, enemy, terrain, troops, time, and commander's intent.

PROGRAM

The M88A3 is an Acquisition Category IC program using an Other Transaction Authority to complete the engineering change proposal. DOT&E approved a TEMP in September 2023. A TEMP update is planned for FY25 to capture production verification test and FOT&E scope. The Army intends to conduct an FOT&E in 2QFY27 and plans to equip the first unit in 1QFY28.

» MAJOR CONTRACTOR

- BAE Systems, Inc. – Anniston, Alabama

TEST ADEQUACY

In FY24, the Army conducted a Soldier Touchpoint in July 2024. DOT&E did not approve this test plan but provided input to the Army. FUSL live fire testing began August 2024 in accordance with a DOT&E-approved test plan. DOT&E personnel observed both the Soldier Touchpoint and FUSL testing.

The Army conducted the Soldier Touchpoint in July 2024 with three soldiers from 1-35 Armor Battalion, 1st Armored Division. The crew performed mobility, towing, pick and carry, and recovery operations using the M88A3 on test courses at Aberdeen Test Center, Maryland. Soldiers provided system performance and usability feedback, which should be implemented prior to first unit equipped in FY27.

The Army began FUSL testing in August 2024, with completion expected in 3QFY25, to compare crew survivability, system survivability, and system functionality restoration of a combat-loaded M88A3 against the current M88A2, using realistic threats. The Army conducted underbody blast events in FY17 to demonstrate the M88A2 performance.

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Soldier Touchpoint and FUSL data analyses are ongoing, precluding a DOT&E evaluation of the M88A3's operational effectiveness, suitability, and survivability. Details from those events will be incorporated in DOT&E's combined FOT&E and LFT&E report to be published in 1QFY28.

RECOMMENDATIONS

The Army should:

1. Implement soldier feedback recommendations provided during the Soldier Touchpoint to maximize operational effectiveness and survivability.
2. Submit a TEMP update for DOT&E approval, capturing production verification testing in an FOT&E.

Integrated Fires Test Campaign (IFTC)

Left: Lower Tier Air and Missile Defense Sensor (LTAMDS)
Right: Integrated Fire Protection Capability Increment 2 (IFPC Inc 2)

In November 2023, the Army conducted operational testing for the Integrated Fires Test Campaign 2023 (IFTC 23) at White Sands Missile Range, New Mexico. IFTC 23 was the first in a series of IFTC events that the Army plans to conduct annually. The purpose of IFTC is to provide the Army an opportunity to test the integration of sensors and shooters in the Army Integrated Air and Missile Defense (AIAMD) command and control (C2) architecture. The test campaign provides an opportunity for demonstrating system-of-systems integration and is also a source of operational evaluation data for individual programs of record. The Army began operational testing for IFTC 24 in September 2024 at White Sands Missile Range, New Mexico.

CAMPAIGN OVERVIEW

The Army intends for IFTC to facilitate a more comprehensive evaluation of the Army's air and missile defense systems, testing them as a single, integrated system of systems, as opposed to individual components. The Army also intends for IFTCs to reduce overall T&E costs across the Program Executive Office Missiles and Space (PEO MS) by combining test events for multiple systems.

The Army's stated IFTC objectives are: (1) synchronize component experimental, developmental, and operational testing to achieve resource and T&E efficiencies by tailoring common architectures, threats, and force structures and support component acquisition data requirements; (2) identify requirements and/or test indirect fire capabilities to close operational capability and materiel performance gaps which are described in detail within programs' corresponding test plans; and (3) accelerate existing materiel release and certification processes through agreements with external process stakeholders to achieve an annual fielding cadence.

IFTC ASSESSMENT

During IFTC 23, the Army integrated its Lower Tier Air and Missile Defense Sensor (LTAMDS) into the AIAMD C2 architecture. The Army conducted three days of software- and hardware-in-the-loop (S/HWIL) and four days of uncontested live air testing; the testing included one LTAMDS radar connected to a single AIAMD Engagement Operations Center with its Integrated Collaborative Environment tent, with four simulated Patriot launchers. The Army conducted the testing almost entirely within a simulated HWIL environment and was intended to support both an annual update for the AIAMD program and an operational assessment for LTAMDS. During IFTC 24 the Army plans to expand the number of systems by including the Integrated Fire Protection Capability Increment 2 (IFPC Inc 2) launcher and associated Sentinel A3 radar.

» TEST DESIGN

The test design process for IFTC 23 did not differ substantially from individual system testing, as it was designed to evaluate only the LTAMDS system. See the Missile Defense System article in the Annual Report for additional details on LTAMDS. The AIAMD program participated in IFTC 23 but had no individual operational test objectives. The Army Test and Evaluation Command developed a set of limited operational scenarios that were tailored to existing LTAMDS capabilities. While IFTC 24 includes the addition of the IFPC Inc 2 launcher system and a Sentinel A3 radar, the two developmental systems (LTAMDS and IFPC Inc 2) will operate on their own individual AIAMD networks throughout all phases of the test, allowing for system-specific operational scenarios.

» TEST UNIT

The 3-43 Air Defense Artillery (ADA), previously designated as the AIAMD test battalion, acted as the primary system operators for IFTC 23. They will also operate the AIAMD software during IFTC 24, with support from the 1-51 ADA, which will be responsible for movement and emplacement of IFPC Inc 2 launchers.

» MODELING AND SIMULATION (M&S)

The test designs for IFTC 23 and IFTC 24 rely heavily on use of M&S tools developed under individual programs of record that span PEO MS. These M&S tools must be verified, validated, and accredited and then integrated together to provide a simulated operational test environment. DOT&E determined that IFTC 23 was inadequate to support an assessment of operational effectiveness for the LTAMDS system, due to immature and unaccredited LTAMDS M&S tools. These M&S challenges persist in IFTC 24 for both LTAMDS and IFPC Inc 2. The Army should focus on efficiently using developmental testing to support M&S tool development, verification, validation, and accreditation.

» SCHEDULE

The IFTC schedule is driven almost entirely by individual program schedules. IFTC 23 was intended to serve as the first operational assessment for LTAMDS, while IFTC 24 will serve as an operational assessment for both LTAMDS and IFPC Inc 2.

IFTC 25 will not include LTAMDS or IFPC Inc 2 and will serve only as the FOT&E for the AIAMD system. See the AIAMD article in this Annual Report for additional details. IFTC 26, as currently envisioned, will be the first opportunity to demonstrate multiple new developmental sensors and shooters on the same AIAMD network, including both the LTAMDS and Sentinel A4 radars, as well as the Patriot and IFPC Inc 2 launchers. IFTC 26 is intended to support T&E of the Army's contribution to the Guam Defense System.

» TEST RESOURCES

Operational testing of air defense systems requires fixed- and rotary-wing aircraft to provide live tracking of air targets. As the Army lacks sufficient fixed-wing assets, the IFTC provides an opportunity to reduce overall asset demand and leverage the size of the event to gain support from external communities such as the Air Force and Navy.

The Army is assessing courses of action to send LTAMDS and IFPC prototypes into theater prior to their operational testing. The assessment includes the possibility of sending the systems overseas to support combatant commands. The PEO should ensure retention of adequate test assets in CONUS to support continued development and testing in the event prototype systems are forward-deployed.

» JOINT PARTICIPATION

IFTC 23 did not include any participants outside of the Army's air and missile defense community. Previous AIAMD program testing included the Ground/Air Task-Oriented Radar operated by the Marine Corps. The Army has stated an intent to include joint participants in future IFTC events.

RECOMMENDATIONS

The Army should:

1. Ensure that the M&S tools required for IFTC performance evaluations are validated, verified, and accredited prior to test execution.
2. Ensure adequate test assets are available in CONUS in the event these prototype systems are forward-deployed.
3. Coordinate with the Navy and the Missile Defense Agency to ensure that future IFTC events include appropriate joint participation, including when testing the Defense of Guam architecture in IFTC 26.

Integrated Personnel and Pay System – Army (IPPS-A) Increment II

The Integrated Personnel and Pay System – Army (IPPS-A) Increment II Release 3 Limited User Test (LUT) operational test was conducted from June 2022 to February 2024. This annual report describes the major problems discovered during the LUT. The IPPS-A Program Management Office (PMO) is using the Scaled Agile Framework to rapidly address the problems, with a verification of fixes (VoF) operational test planned in 3QFY25. DOT&E plans to assess the operational effectiveness, suitability, and survivability of IPPS-A in 4QFY25, following the VoF test.

SYSTEM DESCRIPTION

IPPS-A is the Army's future online Human Resources (HR) and pay solution that transforms antiquated personnel and pay systems to a 21st century Talent Management System. IPPS-A will become the authoritative data source as the necessary functionality of the legacy systems is subsumed.

The capabilities available in IPPS-A Increment II Release 3 are limited to personnel information for the three components of the Army: Active Duty, Reserves, and the National Guard. The IPPS-A PMO plans to continue to develop IPPS-A to deliver a full set of necessary capabilities to support pay functionality as well.

IPPS-A is a web-based tool available 24 hours a day and accessible to soldiers, HR professionals, combatant commanders, personnel and pay managers, and other authorized users throughout the Army.

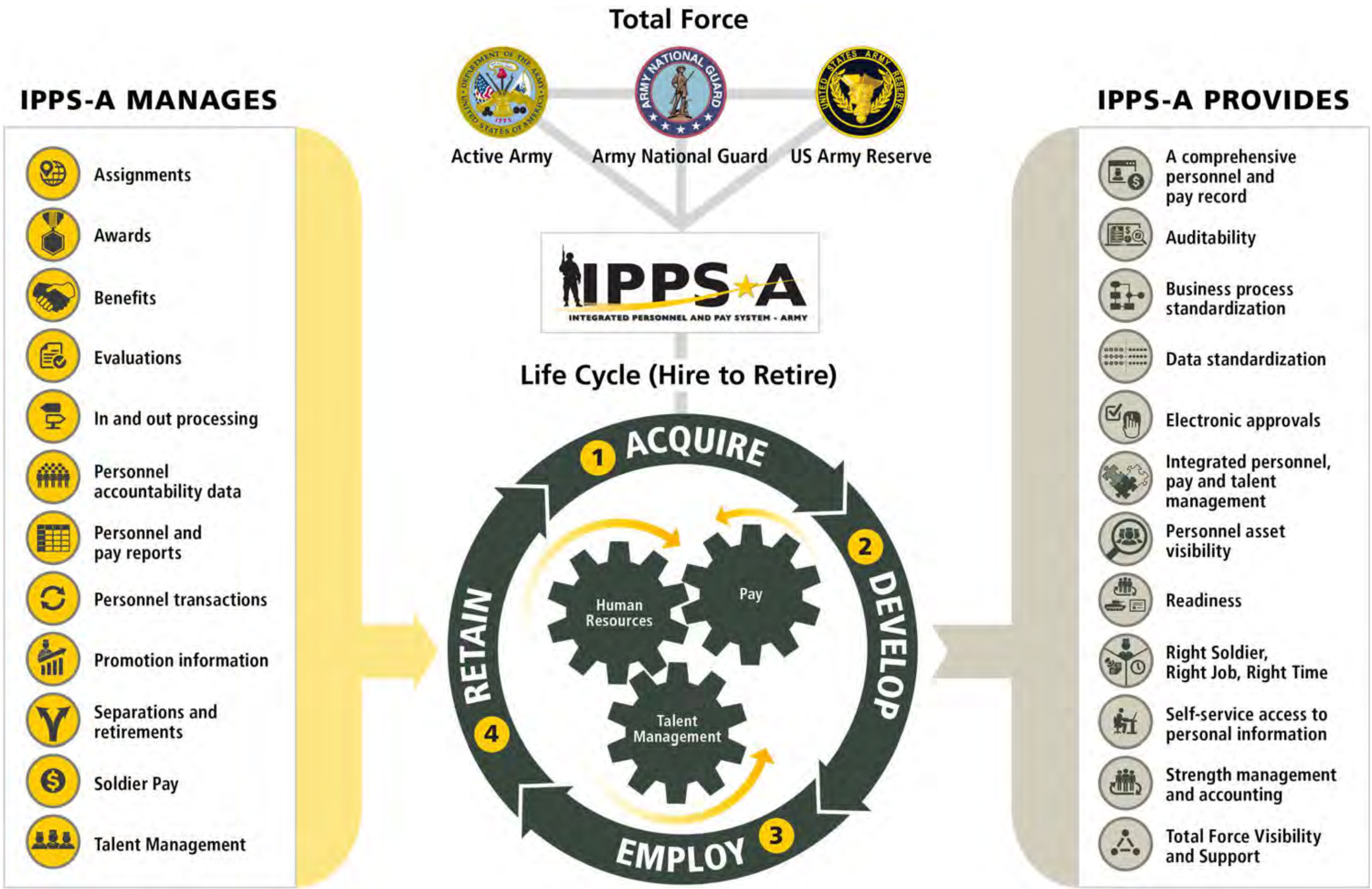
IPPS-A is intended to be a single, integrated personnel and pay system that soldiers can use to conduct self-service personnel transactions such as a change of address, which is projected to reduce the need for face-to-face interaction with HR professionals.

MISSION

Commanders will employ IPPS-A as a comprehensive system for personnel accountability and unit strength information to support command decisions, regardless of component or geographic location. Army components will use IPPS-A to manage their members across the full operational spectrum, capturing timely and accurate data through mobilization and demobilization.

PROGRAM

IPPS-A is a Business System Category 1 program for which DOT&E approved the IPPS-A TEMP in August 2018. Subsequently,



DOT&E approved an update to the TEMP to address IPPS-A Increment II Release 3 in October 2020. DOT&E approved the operational test plan for the IPPS-A Increment II Release 3 LUT in September 2021. The IPPS-A Increment II Release 3 LUT informed an FY23 limited deployment authority to proceed decision to allow deployment of the IPPS-A Release 3 software.

The IPPS-A PMO is addressing problems discovered during operational testing using Scaled Agile Framework development processes and has started development of IPPS-A Army military pay capability, which will provide full pay functionality for all three components of the Army.

» MAJOR CONTRACTORS

- CACI International, Inc. – Chantilly, Virginia
- Nakupuna Companies – Arlington, Virginia

TEST ADEQUACY

The Army Test and Evaluation Center (ATEC) conducted, and DOT&E observed a LUT on IPPS-A Increment II Release 3, which was executed in accordance with the DOT&E-approved operational test plan. The LUT, which the Army extended when DOT&E requested additional data, was conducted from June 2022 to February 2024. The additional data were from two sources: PMO help desk tickets and a User Assessment Test, led by the PMO and the Functional Management Division. ATEC collected adequate data to evaluate cyber survivability during a cooperative vulnerability and penetration assessment and an adversarial assessment held concurrently with the LUT. The Army plans a VoF operational test in 3QFY25 to address the problems discovered during the LUT. DOT&E plans to assess the operational effectiveness, suitability, and survivability of IPPS-A in 4QFY25, following the VoF test.

PERFORMANCE

» EFFECTIVENESS

Many users found the data displayed in IPPS-A Increment II Release 3 unreliable. IPPS-A Increment II Release 3 struggles with data correctness and requires the use of workarounds to complete some critical business processes. One year following the deployment of Release 3, users continue to consistently submit high-priority help desk tickets. The number of new critical and high-priority tickets submitted each week remained consistent from May 2023 through February 2024, at which point data collection completed. As of February 2024, users continued to consistently report pay-impacting help desk tickets, indicating that pay-impacting errors in IPPS-A Increment II Release 3 appear harder to resolve than anticipated.

Interface problems contributed to many submitted help desk tickets. The mission-critical/pay-impacting inbound interfaces in the Assignments, Hire/Rehire, Promotions, and Talent Management business processes did not meet the accuracy threshold and require the use of workarounds to complete functionality, confirming what testers observed during capability testing. DOT&E noted improvement as the system progressed through each event from LUT Phase 1 to User Acceptance Test to LUT Phase 2, but some interfaces still did not meet specified requirements.

» SUITABILITY

Users found IPPS-A was nonintuitive because the system used nonstandard Army terms, including in error codes. Another contributing factor is that the backlog of open help desk tickets remains large, despite improvements in the ticket resolution rate. The help desk ticket resolution rate is improving but remains slow, with 50 percent of tickets closed within 13 days on average. Moreover, the stable and large backlog of tickets suggests that the help desk is at capacity and not well positioned for the future software releases, should a similar rate of deficiencies be submitted by users.

IPPS-A met all but one of its specified reliability requirements. The Army collected reliability data from January 2023 until March 2023. During this period, there were three unplanned outages and three planned outages that prevented users from accessing IPPS-A. The mean time to repair an unplanned outage was 2.2 hours.

The operational availability was 98 percent. The one requirement that was not met is the mean time between system aborts, which was 194.3 hours, less than the required 672 hours.

» SURVIVABILITY

The IPPS-A PMO is working to address the cyber survivability findings discovered during the LUT, which are classified.

RECOMMENDATIONS

The Army should:

1. Resolve the remaining deficiencies in IPPS-A Increment II Release 3 capabilities and conduct a verification of fixes in an operationally representative environment before deployment of IPPS-A Army military pay capability, to ensure identified deficiencies are addressed.
2. Resolve the need for workarounds to conduct critical business processes that include pay-impacting data fields.
3. Conduct operational testing on IPPS-A Army military pay capability in an operationally realistic environment with all representative interfaces that will fully evaluate the mission prior to deployment and support the full deployment authority to proceed.
4. Use the IPPS-A Increment II Release 3 data to forecast and prepare for the likely increase in user-submitted help desk tickets upon the operational deployment of IPPS-A Army military pay capability, to ensure adequate support for an extended period of increased help desk operational demands.

Integrated Tactical Network (ITN)

There was no operational testing of the Integrated Tactical Network (ITN) in FY24. The Army is in the process of updating acquisition strategies for the tactical network based on a concept called Command and Control Fix (C2 Fix).

SYSTEM DESCRIPTION

The ITN is an effort to rapidly prototype and field equipment to modernize Army tactical communications. It is a system of systems utilizing commercial and non-developmental items and services to supplement currently fielded program of record components in support of the Army's Network Modernization Strategy. It provides system interoperability and continuity through the procurement of enhanced tactical communication equipment, ancillaries, and related services. The ITN brings new commercial components and network transport capabilities to lower echelons within the Army's tactical network environment. The ITN products are designed around two-year product cycles called capability sets.

The first capability set (CS), known as CS 21 ITN, consists of the commercial off-the-shelf single-channel tactical radios, dual-channel headsets, variable height antennas (VHAs), high-capacity line-of-sight radios, tactical radio gateways, and mobile broadband kits (MBKs) that enable communications through Secret and sensitive but unclassified – encrypted (SBU-E) enclaves. The SBU-E enclave allows commanders the flexibility to balance security and connectivity based on mission need. CS 21 provides an end-to-end network design that is tailored specifically to provide an expeditionary capability to an infantry unit. The prototyping activities for the next capability set (i.e., CS 23) tailored the CS 21, as well as emerging technologies, to support Stryker formations.

MISSION

ITN-equipped brigade combat teams (BCTs) conduct multidomain operations in the joint operating environment with essential mission command capabilities throughout a full range of military operations. ITN-equipped BCTs conduct mission command with a network in congested and contested environments at the point of need. The CS 21 equipment is intended to provide tactical voice and data across the tactical brigade down to dismounted soldiers. The CS 23 ITN is an extension of the technologies in CS 21. CS 23 integrates many of these capabilities onto Stryker platforms and units, while CS 21 focused solely on the infantry BCT formation. Soldiers using the ITN will have additional options available for their primary, alternate, contingency, and emergency communications plans, as well as the ability to switch communications paths when faced with challenging environments.

PROGRAM

The ITN consists of two Middle Tier of Acquisition (MTA) programs: one rapid prototyping (ITN) and the other rapid fielding (CS 21 and 23). Successful products developed during rapid prototyping have the potential to transition to the rapid fielding program. The Army transitioned tactical radios, dual-channel headsets, VHAs, gateways, and MBKs. Program Executive Office Command Control Communications – Tactical is the office of primary responsibility to integrate the systems identified by the Army's Network Cross Functional Team into the ITN.

The Army originally intended for the ITN to modernize Army tactical communications at battalion- and brigade-level networks. The June 2022 DOT&E-approved TES covered CS 21 and 23. The ITN is now transitioning to support division-centric networks, and the Army is working to define those specific changes through a series of unit exercises associated with a concept they are calling C2 Fix.

The Army signed a rapid fielding acquisition decision memorandum in June 2023 to continue nonrecurring engineering efforts for the rapid fielding program until it transitions at the outcome determination in July 2025. The details of this transition are still in development as of this writing.

The Army closed out the rapid prototyping program at the outcome determination in August 2024. The Army should codify any future testing within a DOT&E-approved TES document to support acquisition decision making.

» MAJOR CONTRACTORS

MBK

- 4K Solutions – Midland, Georgia
- Verizon – New York, New York (cellular plan for MBK)

VHA

- Hoverfly Technologies Company – Orlando, Florida
- Lockheed Martin Corporation – Bethesda, Maryland
- Teledyne FLIR, LLC – Wilsonville, Oregon

Other

- General Dynamics Mission Systems– Fairfax, Virginia
- KLAS Telecom – Herndon, Virginia
- PAR Government – Raleigh, North Carolina
- Samsung Galaxy S7 – San Jose, California
- Sierra Nevada Corporation Integrated Mission Systems – Hagerstown, Maryland
- Silvus Technologies, Inc. – Los Angeles, California
- Trellisware Technologies, Inc. – San Diego, California
- L3Harris Technologies, Inc. – Melbourne, Florida
- Thales Group – Clarksburg, Maryland

TEST ADEQUACY

The Army did not perform any operational testing in FY24. Instead, in accordance with recommendations in the FY23 Annual Report, the Army leveraged the 2nd Brigade 101st Airborne Division as part of Operation Lethal Eagle, a large-scale air assault that provided the opportunity to experiment with new technologies, prototype reorganized structures, and employ multi-domain fires. The observations from Operation Lethal Eagle fed the August 2024 Joint Readiness Training Center rotation to provide the Army additional feedback on the C2 Fix. Once the Army formalizes the C2 Fix process into the pending C2 Next (a process still being refined), the Army should codify a TES to support future decision making.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E is unable to assess the operational effectiveness, suitability, and cyber survivability of ITN due to the lack of operational testing by the Army.

RECOMMENDATION

The Army is addressing the recommendations from the FY23 Annual Report and additionally should:

1. Develop and submit to DOT&E a TES to support the Army's future ITN acquisition decisions.

Integrated Visual Augmentation System (IVAS)

In FY24, the Army produced the Integrated Visual Augmentation System (IVAS) 1.1 variant. In FY25, the Army intends to issue the variant using a limited safety release to select units to support its campaign of learning. There is no future operational testing planned for the IVAS 1.0 and 1.1 variants. The Program Management Office (PMO) led several internal test events to assess technical improvements made to the IVAS 1.2 variant and solicit soldier feedback. The Army intends to conduct an operational assessment (OA) of the IVAS 1.2 variant in 3QFY25 to inform a production decision and support transition from the Middle Tier of Acquisition – Rapid Prototyping (MTA-RP) pathway to a new acquisition pathway in 4QFY25 and begin fielding the IVAS 1.2 variant in 1QFY26.

SYSTEM DESCRIPTION

The Army intends IVAS to function as a soldier-worn system to increase soldier lethality in all environments and battlefield conditions at the battalion-level and below. The IVAS includes a heads-up display (HUD), a body-worn computer known as a puck, a 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 ultra-wide-band network enables passive targeting 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 IVAS-equipped soldiers to transmit data within the company.

MISSION

The Army intends for close combat forces to employ IVAS in all environments and battlefield conditions to increase individual soldiers' situational awareness and ability to detect, identify, and engage the enemy with direct fires. IVAS is intended to enhance collective lethality through the combination of improved communication, mobility, mission command, and marksmanship. Squads will train with IVAS in the Squad Immersive Virtual Trainer to provide a high fidelity, live and mixed reality environment that enables the rapid conduct and repetition of select platoon-level battle drills and the immediate conduct of after-action reviews.

PROGRAM

In FY24, the Army produced the IVAS 1.1 variant. In FY25, the Army intends to issue the variant using a limited safety release to select units to support its campaign of learning.

In December 2022, the IVAS 1.2 variant was approved to use the MTA-RP pathway, and the technological insertion was awarded to Microsoft under the existing IVAS production Other Transaction Authority. The Army plans to conduct an OA in 3QFY25 to inform a production decision and support the transition from the MTA-RP pathway to a new acquisition pathway in 4QFY25 and to begin fielding IVAS 1.2 variant in 1QFY26. The PMO is updating and plans to submit the IVAS 1.2 variant TES to DOT&E for approval.

In July 2024, Army senior leaders directed the program manager (PM) to conduct a user assessment (UA) at Joint Base Lewis-McChord, Washington, in August 2024 using two squads of infantry soldiers. The purpose of the UA was to determine if the IVAS 1.2 form factor improves compatibility with current weapons systems, measure the effectiveness of low light and thermal sensors to determine if threshold and objective requirements have been met, and demonstrate the ability for the network architecture to support select robotic autonomous systems. The PM used the data collected to support its recommendations on program progression. DOT&E personnel observed portions of the UA.

Soldier participation in IVAS 1.2 UA, Picatinny, New Jersey, January 2024

» MAJOR CONTRACTOR

- Microsoft Corporation – Redmond, Washington

TEST ADEQUACY

The Army did not conduct operational testing of the IVAS 1.2 variant in FY24. The PMO led several internal events using IVAS 1.2 system prototypes and soldiers, to inform programmatic decisions and assess changes made to the IVAS 1.2 variant based on results from the previous IVAS 1.0 variant operational testing conducted in May 2022. The events focused on design, network, and unit integration concepts transitioned forward from IVAS 1.0 to IVAS 1.2 variants. As these events were not operational tests, the evaluation plans did not require DOT&E approval, but DOT&E did observe the testing.

The Army plans to conduct a cooperative vulnerability and penetration assessment of the IVAS 1.2 variant in 1QFY25. DOT&E approved the test plan in October 2024.

The Army intends to conduct an OA of the IVAS 1.2 production-representative variant in 3QFY25 to inform a production decision and support transition from the MTA-RP pathway to a new acquisition pathway in 4QFY25 and begin fielding the IVAS 1.2 variant in 1QFY26. The Army will submit an OA test plan to DOT&E for approval in 2QFY25.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

In FY24, PMO-led events of the IVAS 1.2 variant prototype system were not intended to occur in an operationally representative environment. The PMO used the results from these internal events to assess technical improvements made to the IVAS 1.2 variant and to solicit soldier feedback to help inform programmatic decisions. DOT&E personnel observed the events. DOT&E will assess operational effectiveness, suitability, and survivability using data from the OA and will publish an OA report in 3QFY25 to inform a production decision and support transition to a new acquisition pathway in 4QFY25.

RECOMMENDATIONS

The Army should:

1. As recommended in the FY23 Annual Report, submit to DOT&E for approval an updated TES for the IVAS 1.2 variant.
2. Continue to plan and resource an OA in an operationally realistic and stressing environment to inform an assessment of operational effectiveness, suitability, and survivability of the IVAS 1.2 variant.

Javelin Antitank Missile System – Medium

The Javelin Antitank Missile System – Medium is undergoing two independent, but complementary upgrades, referred to as the G-model missile and the Lightweight Command Launch Unit (LW CLU). The Army conducted an FOT&E in August 2023 on the LW CLU paired with current inventory missiles. In March 2024, DOT&E published a Javelin Antitank Missile System – Medium FOT&E report with a classified annex, concluding that the upgraded Javelin system is operationally effective, though not operationally suitable, due to a new software fault. The fault has been corrected in the latest software update and will be tested during qualification and acceptance testing. The G-model missile experienced developmental delays due to a flight test failure in FY22, was re-baselined in FY23, and will continue verification of corrective actions in FY25.

SYSTEM DESCRIPTION

The Javelin Antitank Missile System – Medium is a man-portable, shoulder-launched, fire-and-forget weapon system used to defeat threat armored vehicles out to 2,500 meters. The Javelin system consists of a missile in a disposable launch tube assembly (LTA) and a reusable CLU. The CLU mechanically engages the LTA for shoulder firing, has day and night sights for surveillance and target acquisition, and electronically interfaces with the missile for target lock-on and missile launch.

The Javelin system is undergoing two independent, but complementary upgrades intended to control unit cost, reduce size and weight, and address component obsolescence while meeting or exceeding the current F-model missile and Block 1 CLU performance. These system improvements are referred to as the G-model missile and LW CLU. The G-model missile effort is developing a new LTA, electronic battery unit, guidance electronics unit, and missile seeker. Production missiles will be designated FGM-148G. The LW CLU effort incorporates modern daylight and infrared camera technology in a smaller and lighter form factor. The LW CLU is backward compatible with the current inventory of missile models, and the G-model missile will be backward compatible with the legacy Block 1 CLU.

The Army is developing a new Basic Skills Trainer (BST) and the Javelin Outdoor Trainer (JOT) that will be compatible with the upgraded Javelin system.

MISSION

Commanders use Army and Marine Corps ground maneuver units equipped with the Javelin to destroy, capture, or repel enemy assault through maneuver and firepower. Soldiers and marines use the Javelin to destroy threat armor targets and light-skinned vehicles, and to incapacitate or kill threat personnel within fortified positions or in the open.

PROGRAM

Javelin is an Acquisition Category IC program. The Army is upgrading the Javelin weapon system and associated training equipment through multiple engineering change proposals occurring in separate LW CLU and G-model missile development efforts. In March 2024, DOT&E published a Javelin Antitank Missile System – Medium FOT&E report with a classified annex, supporting a LW CLU production decision in October 2024. Fielding of the LW CLU is expected to begin in 1QFY26.

The G-model missile experienced developmental delays due to a flight test failure in FY22. The program was re-baselined in FY23, and analysis of the flight test failure continued through FY24. Verification and validation of corrective actions are planned through FY25. The G-model missile will continue development and testing over the next four years and begin production upon the completion of a successful government-led qualification flight test series.

DOT&E approved an updated TEMP for the Javelin program in April 2020 and a LW CLU-specific TEMP addendum in February 2023.

» MAJOR CONTRACTORS

- Raytheon, a subsidiary of RTX – Tucson, Arizona
- Lockheed Martin Corporation – Orlando, Florida

TEST ADEQUACY

In FY23, the Army Test and Evaluation Command conducted two operational tests of the Javelin system comparing the LW CLU against the Block 1 CLU, both paired with current inventory missiles. A Limited User Test (LUT) was conducted at the Cold Regions Test Center, Fort Greely, Alaska in March 2023, and an FOT&E at Yuma Proving Ground, Arizona in August 2023. Both tests were observed by DOT&E and conducted in accordance with the DOT&E-approved TEMP and respective test plans. The G-model missile was not mature enough to be included in the LUT or FOT&E. Together, these tests were adequate to determine the operational effectiveness and suitability of the Javelin LW CLU as well as the system performance in the arctic and desert environments. DOT&E published a Javelin Antitank Missile System – Medium FOT&E report with a classified annex in March 2024. The cyber survivability portion of the FOT&E report will be updated following the LW CLU adversarial assessment (AA) planned for February 2025.

Previous testing included a cooperative vulnerability and penetration assessment (CVPA) in FY22 and an adversarial cybersecurity developmental test (ACDT) in August 2023. Cyber survivability findings are being corrected in the latest LW CLU software update and will be tested during the planned AA.

An update to the Javelin TEMP is necessary to reflect the significant delays in the G-model missile development. The updated TEMP should include a T&E concept for combined LW CLU and G-model missile, testing as well as demonstrating the maximum effective range of the upgraded Javelin, as first recommended in the FY22 Annual Report.

PERFORMANCE

» EFFECTIVENESS

In the FOT&E report, DOT&E assessed the updated Javelin system, consisting of LW CLU and current inventory missiles, is operationally effective. Soldiers equipped with the LW CLU performed as well or better than soldiers equipped with the Block 1 CLU at engaging targets day or night, and across the arctic, temperate, and hot desert climates. The improved daylight and infrared camera resolution and zoom capabilities make the LW CLU a superior surveillance device when identifying targets beyond the Javelin's 2,500-meter maximum effective range design requirement. Additional details are found in the FOT&E report and classified annex, published by DOT&E in March 2024.

» LETHALITY

DOT&E last evaluated Javelin's lethality in 2019, following testing of the F-model missile, and found that it met or exceeded its lethality

Testing at the Cold Regions Test Center, Fort Greely, Alaska, March 2023 requirement. Details are found in a classified LFT&E report published by DOT&E in February 2019. Government-led lethality testing of the G-model missile will resume following verification of corrective actions planned for FY25.

» SUITABILITY

In the FOT&E report, DOT&E assessed that the LW CLU is not operationally suitable. A new software fault resulted in three system aborts, causing the LW CLU to fail in demonstrating its operational reliability and availability requirements. The Javelin Program Office immediately opened a failure review board and began taking actions to identify and fix the cause of the fault. A root cause was identified, and a fix developed, that has been incorporated in the planned LW CLU software update 4.1. The fix was demonstrated to be effective in both laboratory and environmental chamber settings, addressing a recommendation from the FY23 Annual Report. Software version 4.1 will be fully verified during qualification and acceptance testing, planned for 1QFY25. The LW CLU software update 4.1 should undergo integrated testing with soldier operators prior to equipping the first unit with the LW CLU. Representatives from ATEC and DOT&E should witness the integrated testing. Additional details on the software failure are found in the FOT&E report and classified annex, published by DOT&E in March 2024.

Soldier feedback on the LW CLU was positive, with gunners preferring the improved camera resolution and the smaller, lighter form factor as compared to the Block 1 CLU. Battery performance for both the LW CLU and Block 1 CLU was significantly degraded in the cold temperatures experienced during the LUT. The Army should investigate a long-term replacement strategy for the existing battery to improve cold weather performance.

Soldiers found the new BST was intuitive and easy to use, and they believed that the BST provided the training needed to prepare Javelin gunners to engage targets with the tactical system. Though the JOT systems used during the LUT and FOT&E were pre-production units, soldier feedback indicated that the JOT replicated the target engagement process and supported realistic training. The Army has continued development and testing of the JOT, addressing a recommendation from the FY23 Annual Report.

» SURVIVABILITY

Cyber survivability cannot be fully assessed until the completion of an AA, planned for February 2025. Previous testing included a CVPA of Javelin between August and September 2021, during which four cyber survivability findings were identified. An ACDT was conducted in August 2023 and the findings should be corrected in LW CLU software update 4.1. Fixes should be verified prior to the planned AA. A JOT cyber vulnerability identification event is planned in 3QFY25 and an ACDT in 1QFY26. DOT&E will include an update on the system's cyber survivability in 4QFY25, as an addendum to the FOT&E report.

RECOMMENDATIONS

The Army should:

1. Conduct integrated testing of LW CLU software update 4.1 with soldier operators prior to equipping the first unit. Representatives from ATEC and DOT&E should witness the integrated testing.
2. Address the CVPA and ACDT findings through LW CLU software update 4.1 and conduct fix verification testing prior to conducting the AA in February 2025.
3. As recommended in the FY23 Annual Report, update the Javelin TEMP to reflect delays in the G-model missile development and plan for combined G-model missile and LW CLU testing, as well as demonstrating the maximum effective range of the upgraded Javelin system.
4. As recommended in the FY23 Annual Report, investigate a long-term replacement strategy for the existing LW CLU battery to improve cold weather performance.

Long Range Hypersonic Weapon (LRHW) – Dark Eagle

In 1QFY24, the Army and Navy initiated a risk reduction campaign to complete prior to conducting another flight test for the Long Range Hypersonic Weapon (LRHW) (Dark Eagle). In 3QFY24, during integrated launch sequence testing, the Army replicated the faults experienced during previous flight tests and verified the implementation of the necessary corrective actions. Later in 3QFY24, flight testing continued with a successful launch of the Navy's prototype All-Up-Round (AUR). In 4QFY24, the Army intended to conduct a missile test as part of Joint Flight Campaign (JFC)-IGNITE, follow-on test to JFC-2, from the Army's LRHW (Dark Eagle) prototype transporter-erector-launcher (TEL) but this test did not occur.

SYSTEM DESCRIPTION

The LRHW (Dark Eagle) is a prototype surface-to-surface long range strategic fires system composed of one TEL and two AUR missiles (designed by the Navy) packaged in Army AUR canisters (AUR+C). The initial LRHW battery will include a battery operations center (BOC) and four TELs, each with two AUR+C. The Middle Tier of Acquisition (MTA) rapid fielding effort only consists of the BOC and TELs.

The AUR is composed of the Common Hypersonic Glide Body and a Navy-developed two-stage rocket booster in a canister designed for the Army's LRHW TEL. The Navy, under the Conventional Prompt Strike (CPS) program, is producing the same AUR and placing it in Navy canisters for launch from *Zumwalt*-class destroyers and *Virginia*-class submarines.

MISSION

Army commanders will use the LRHW (Dark Eagle) to engage adversary high-payoff and time-sensitive targets. U.S. Strategic Command, with direction from the National Command Authority, will serve as the employment authority for LRHW missions.

PROGRAM

The Army Rapid Capabilities and Critical Technologies Office was responsible for developing and fielding prototype LRHW equipment to the first unit equipped. In August 2023, the Army determined the LRHW program will use the MTA rapid fielding approach and transferred the LRHW (Dark Eagle) program, consisting of the BOC and TEL, to Program Executive Office Missiles and Space. The Army is still developing the LRHW Master Test Strategy and plans to submit the strategy for DOT&E approval by 4QFY25. The Army intends to field two additional batteries of LRHW to complete the MTA rapid fielding phase by FY27.

The Navy's CPS program designed the AUR+C and elements of the weapons control system for the Army's LRHW (Dark Eagle) program in FY23. The Army plans to integrate the AUR+C with its weapon control system to field a BOC and four TELs to the LRHW unit upon the completion of a successful flight test.

» MAJOR CONTRACTORS

- Lockheed Martin Corporation – Huntsville, Alabama (BOC and TEL, system integration prototype)
- Dynetics, a subsidiary of Leidos – Huntsville, Alabama (TEL trailer and Common Hypersonic Glide Body)

TEST ADEQUACY

As recommended in the FY21 and FY23 Annual Reports, the Army is still developing the LRHW Master Test Strategy. The plan is to submit it for DOT&E approval by 4QFY25. The test strategy should include the following considerations: a concept of employment consistent with the expected operational and threat environment; an operational demonstration that includes strategic-level mission planning; test and evaluation in a full-spectrum contested environment, including representative targets; and validated modeling and simulation (M&S), combined with ground and subscale test data to support evaluation of operational effectiveness, lethality, suitability, and survivability.

As recommended in the FY21 and FY23 Annual Reports, the Army continues to collaborate with the Navy to develop an LFT&E Strategy. The Army needs to incorporate representative targets and environments into flight tests and other live lethality and survivability tests. The Army should continue to collaborate with the Navy and Air Force to identify and leverage common practices, test corridors and infrastructure, test data, and M&S capabilities across the family of hypersonic weapon systems.

The Navy conducted a warhead arena test in 1QFY24 and a sled test in 2QFY24. As noted in the FY22 and FY23 Annual Reports, the initial CPS sled and flight tests did not include operationally representative targets and consequently provided no direct validation of the weapon's lethal effects. The Navy included some threat-representative targets in the recent sled test. The Navy, supported by Lawrence Livermore National Laboratories, is still processing the results of these tests. DOT&E will provide an independent assessment of the operational effectiveness and lethality when the Navy provides the data. The Navy is further investigating methods to obtain effectiveness and lethality data by incorporating representative targets into the CPS flight tests. Until the Army and Navy make an adequate determination of AUR lethality, uncertainty in weaponeering tools could result in excessive employment requirements or failure to meet warfighter objectives.

The Army has not yet evaluated the effects of a full-spectrum (kinetic, non-kinetic, electromagnetic, cyber) threat-contested environment on the performance of the AUR, TEL, or BOC. This includes an end-to-end cyber survivability testing that includes a cooperative vulnerability and penetration assessment and an adversarial assessment. The Army is relying on the Navy's use of a combination of M&S, component testing, and hardware-in-the-loop evaluations to evaluate full-spectrum survivability of the AUR in the representative threat environment.

In 4QFY24, the Army intended to conduct a missile test as part of JFC-IGNITE from the Army's LRHW (Dark Eagle) prototype TEL but this test did not occur. The LFT&E Strategy for the AUR, written by the Navy, and incorporating Army-specific targets and environments, will be submitted for DOT&E approval in 2QFY25.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Insufficient data are available to evaluate the operational effectiveness, lethality, suitability, and survivability of the LRHW system.

RECOMMENDATIONS

As recommended in the FY23 Annual Report, the Army should:

1. Continue efforts to develop the LRHW Master Test Strategy that includes integrated testing, operational testing, live fire testing, and cybersecurity assessments to credibly demonstrate the required Dark Eagle operational effectiveness, lethality, suitability, and survivability and submit for DOT&E approval.
2. Continue collaboration with the Navy on 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.
3. Include full-spectrum survivability demonstration in a contested environment during an operational demonstration.
4. Conduct end-to-end cyber survivability testing to include a cooperative vulnerability and penetration assessment and adversarial assessment.
5. Validate M&S outputs and combine with ground test data to support design of experiments and evaluation of operational effectiveness, survivability, and lethality.
6. Incorporate operationally representative targets and environments into flight tests and other lethality and survivability tests, as recommended since the FY21 Annual Report.
7. Continue collaboration with the Navy and Air Force to identify and leverage common practices, test corridors and infrastructure, test data, and M&S capabilities across the family of hypersonic weapon systems.

M10 Booker

In June 2024, the Army began live fire testing of the M10 Booker and expects completion by 2QFY25. The Army plans to conduct an IOT&E from 1Q – 2QFY25. DOT&E plans to publish a combined IOT&E and LFT&E report in 3QFY25 to support a full-rate production decision that quarter.

SYSTEM DESCRIPTION

The M10 Booker is a new capability that provides infantry brigade combat team (IBCTs) with a mobile, protected, direct fire capability against light armored vehicles, hardened enemy fortifications, and dismounted personnel. The M10 Booker is a fully tracked armored combat assault vehicle that is transportable on C-17 aircraft and manned by a crew of four soldiers. The M10 Booker is able to fire a broad spectrum of currently fielded munitions through use of its 105mm main gun and 7.62mm coaxial machine gun. The M10

Booker design includes a number of force protection features, such as armor, smoke grenade launchers, ammunition stowage blowoff panels, and automatic fire suppression, intended to enhance survivability against direct/indirect fire, rocket-propelled grenades, and underbody threats.

MISSION

The Army intends for IBCT commanders to employ the M10 Booker in direct support of dismounted light infantry units to engage and neutralize enemy personnel, bunkers, machine gun positions, fortifications, and strongpoints, as well as to defeat light armored threats during offensive and defensive operations. IBCTs will use M10 Booker across a range of military operations, including forced and early entry operations in high anti-access/area denial environments, and in direct support of infantry squads, platoons, and companies.

PROGRAM

The Mobile Protected Firepower (MPF) program transitioned from the Middle Tier of Acquisition pathway and entered Milestone C as an Acquisition Category IB program of record in June 2022. DOT&E approved the Milestone C TEMP in May 2022. In June 2023, the Army renamed the MPF program to M10 Booker.

The Army implemented recommendations from DOT&E's April 2022 MPF Operational Assessment report, which included system design changes to reduce toxic fumes when firing the main gun and improvements to the vehicle's cooling system. These improvements will be validated in an operational environment during the IOT&E scheduled from 1Q – 2QFY25. DOT&E approved the Live Fire Test Design Plan and the IOT&E test plan in August 2024. The Army plans to complete LFT&E and IOT&E with a cyber adversarial assessment in 2QFY25 to support a full-rate production decision in 3QFY25.

» MAJOR CONTRACTORS

- Joint Systems Manufacturing Center, a government-owned, contractor-operated facility currently operated by General Dynamics Land System – Lima, Ohio (turret)
- Merrill Technologies Group, Inc. – Saginaw, Michigan (hulls)
- General Dynamics Land Systems – Anniston, Alabama (integration and final assembly)

TEST ADEQUACY

The Army began live fire testing in June 2024 in accordance with the DOT&E-approved Live Fire Test Design Plan and with observation by DOT&E personnel. LFT&E is scheduled for completion in 2QFY25.

The Army plans to conduct an IOT&E consisting of Phase I (gunnery) in 1QFY25, and Phase II (force-on-force; adversarial assessment) in 2QFY25. DOT&E approved the IOT&E test plan in August 2024.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E is unable to report on the operational effectiveness, suitability, or survivability as testing is ongoing. DOT&E will publish a combined IOT&E and LFT&E report in 3QFY25 to support a full-rate production decision.

RECOMMENDATIONS

The Army should:

1. Continue developing a Real-Time Casualty Assessment capability to replicate target effects against non-vehicle targets, such as bunkers, and walls to improve combat realism, and training feedback, as previously recommended in the MPF Operational Assessment report published in April 2022.
2. Complete the LFT&E and IOT&E in accordance with the approved test plans.

Mounted Assured Positioning, Navigation, and Timing System (MAPS)

MAPS anti-jam antenna system on a Stryker vehicle

In February 2024, the Army conducted Mounted Assured Positioning, Navigation, and Timing System (MAPS) Generation (GEN) II IOT&E. The MAPS GEN II IOT&E was conducted in accordance with a DOT&E-approved test plan and was adequate to inform a full-rate production (FRP) decision. In September 2024, DOT&E published a classified IOT&E report assessing MAPS GEN II's operational effectiveness, suitability, and cyber survivability. The Program Executive Officer, Intelligence, Electronic Warfare and Sensors (PEO IEW&S) is expected to make the MAPS GEN II FRP decision in 2QFY25.

SYSTEM DESCRIPTION

MAPS is a vehicle-mounted Positioning, Navigation, and Timing (PNT) system that integrates a Military-Code (M-Code) GPS receiver with multiple alternative PNT sources and an anti-jam antenna system to provide vehicle crews and client systems with access to trusted PNT information in conditions where GPS signals may be degraded or denied. MAPS does not have an integrated screen and relies on other client systems to display PNT information to vehicle crews. MAPS supports the Army's transition to M-Code GPS and will replace the legacy Defense Advanced GPS Receiver (DAGR) in a subset of the Army's technical and combat vehicles.

MISSION

A unit equipped with MAPS employs trusted PNT information to conduct operations in GPS degraded or denied environments, such as dense vegetation, built-up urban and mountainous terrain, and in the presence of electromagnetic interference or enemy electronic warfare.

PNT information derived from MAPS directly enables positioning of forces; navigation across the operational environment; communication networks; situational awareness applications; and protection, surveillance, targeting, and engagement systems that contribute to combined arms maneuver.

PROGRAM

In 2019, the Army Futures Command issued a directed requirement for the PNT Program Manager to conduct a technical assessment of the MAPS GEN II capability to inform requirements and follow-on programs of record. The Commanding General, Army Futures Command, approved the MAPS Capability Development Document in September 2020, documenting the requirement to replace existing GPS receivers and antennas in a subset of Army ground vehicle variants. Following an open competition, the Army selected Collins Aerospace to provide the MAPS GEN II solution. The Army conducted a limited user test in September 2021, which informed the PEO IEW&S decision to enter program of record status at Milestone C as an Acquisition Category II, Major Capability Acquisition program in June 2022. DOT&E approved the MAPS Milestone C TEMP in April 2022.

The MAPS program completed IOT&E in February 2024 in accordance with a DOT&E-approved test plan. DOT&E published a classified report in September 2024. The IOT&E report will support an FRP decision in 2QFY25, and fielding to Stryker Brigade Combat Teams beginning in 4QFY25. A TEMP update supporting post FRP T&E activities is in development and an FOT&E focusing on Armored Brigade Combat Team vehicles is planned for 1QFY26 to support a separate Armored Brigade Combat Team fielding decision.

» MAJOR CONTRACTOR

- Collins Aerospace, a subsidiary of Raytheon Technologies – Cedar Rapids, Iowa

TEST ADEQUACY

In February 2024, the Army, led by the Army Test and Evaluation Command, conducted MAPS GEN II IOT&E and a cyber survivability adversarial assessment at Yakima Training Center in Yakima, Washington, in accordance with a DOT&E-approved test plan and TEMP. The IOT&E and adversarial assessment were observed by DOT&E and were adequate to determine the operational effectiveness, suitability, and survivability of MAPS GEN II's. DOT&E published a classified IOT&E report in September 2024, which will support the Army's FRP decision planned for 2QFY25. The Army addressed recommendations from the FY22 DOT&E Annual Report to verify deficiency corrections prior to conducting the IOT&E.

PERFORMANCE

» EFFECTIVENESS

MAPS GEN II is operationally effective and performs significantly better than the legacy DAGR in GPS-contested environments. MAPS GEN II continues to provide reliable PNT information in conditions where the DAGR could not, and improves soldiers' situational awareness, supports navigation, and allows the unit to maintain operational tempo while moving between mission objectives. Additional details are contained in the September 2024 classified IOT&E report.

» SUITABILITY

MAPS GEN II is operationally suitable and only experienced one essential function failure during IOT&E, meeting its reliability requirement. However, MAPS GEN II does not have an integrated screen and is reliant on the Joint Battle Command – Platform (JBC-P) or other connected client systems to display PNT information to the vehicle crew. The JBC-P experienced three essential function failures during the IOT&E, which reduced the overall PNT system of systems reliability. Operational availability was 99 percent due to the rapid repairability of the failures. Training was sufficient for soldiers to operate the MAPS. However, they expressed a need for additional troubleshooting instruction on the interface between MAPS GEN II and connected client systems. Additional details are contained in the classified DOT&E IOT&E report, published in September 2024.

» SURVIVABILITY

MAPS GEN II is cyber survivable to outsider and nearsider threats. The MAPS Program Office mitigated vulnerabilities found during previous testing, minimizing an adversary's attack opportunities. Additional details are contained in the classified DOT&E IOT&E report, published in September 2024.

RECOMMENDATIONS

The Army should:

1. Continue testing of the MAPS GEN II ability to resist and respond to evolving GPS threats.
2. Consider adding a screen to MAPS GEN II to serve as an alternate display when JBC-P or other connected client systems are not functioning.
3. Provide additional troubleshooting instruction on the interface between MAPS GEN II and connected client systems.
4. Address the recommendations contained in the DOT&E classified report from September 2024.

Next Generation Squad Weapons (NGSW) Weapons and Ammunition (W&A) and NGSW Fire Control (NGSW-FC)

Top: Next Generation Squad Weapon (NGSW) XM7 Rifle
Bottom: NGSW XM250 Automatic Rifle

The Army completed limited lethality testing for the 6.8mm General Purpose (GP) ammunition in August 2023, and an operational demonstration (Ops Demo) on the Next Generation Squad Weapons (NGSW) system in October 2023. DOT&E published a classified combined Ops Demo and limited lethality assessment (LLA) report in May 2024. The Army plans to conduct limited lethality testing for the 6.8mm Special Purpose (SP) ammunition and an operational assessment (OA) in 1QFY25. DOT&E will publish a combined OA and LLA report in 4QFY25.

Next Generation Squad Weapon Fire Control (NGSW-FC)

SYSTEM DESCRIPTION

The NGSW system includes the XM7 Rifle, XM250 Automatic Rifle, 6.8mm ammunition common to both weapons, and XM157 Fire Control mounted on each weapon. The XM7 and the XM250 are the planned replacements for the M4/M4A1 carbine and M249 Squad Automatic Rifle used in the close combat force (CCF) and security force assistance brigades. The XM7 is fielded with seven 20-round magazines and will have selectable safe, semiautomatic, and automatic firing modes. The XM250 is fielded with two 50-round fabric ammunition pouches and three 100-round fabric ammo pouches, and will have selectable safe, semi-automatic, and automatic firing modes. The XM157 is a variable magnification direct view optic with laser range finder, aiming lasers, environmental sensors, ballistic solver, compass, wireless communication, and display overlay. The XM157 will replace the current optics used by the CCF and security force assistance brigades when issued NGSW systems.

The 6.8mm ammunition includes GP, SP, Blank, Reduced Range, Tracers, Marking, and Drill Dummy Inert ammunition.

MISSION

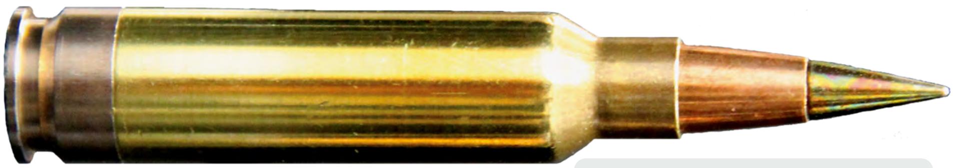
CCFs employ NGSW against threat dismounted personnel and small unit formations equipped with and without protective body armor; in urban, rural, open, and positions under cover; and in all environmental conditions. Operational environments may range from a known traditional or conventional regional environment to an unknown complex environment, such as an international megacity encompassing complex urban terrain. Units equipped with the

NGSW supports the following unit combat operations:

- Movement to Contact
- Attack
- Defense
- Reconnaissance Patrol
- Enter and Clear a Trench
- Enter a Building and Clear a Room
- Hasty Defense

PROGRAM

The NGSW system consists of two distinct Middle Tier of Acquisition (MTA) programs: the NGSW Weapons and Ammunition (W&A) rapid fielding program and the NGSW-FC rapid fielding program. The NGSW W&A program consists of the following components: XM7, XM250, and a common family of 6.8mm ammunition. NGSW W&A was approved as an MTA rapid fielding program in March 2022. The Army approved an urgent materiel release for the weapons in March 2024 and for the ammunition in April 2024. The Army intends to transition NGSW W&A from the MTA rapid fielding pathway to separate major capability acquisition (MCA)



6.8mm GP Ammunition

programs for each component in 3QFY26.

The NGSW-FC rapid fielding consists of the XM157 fire control and was approved as an MTA rapid fielding program in July 2021. The Army approved an urgent materiel release for the fire control in March 2024. The Army intends to transition the NGSW-FC from the MTA rapid fielding pathway to the MCA pathway in 3QFY26.

DOT&E approved the TEMP for both programs in August 2023. The Army issued the NGSW system to the test unit in March 2024 to support the OA in 1QFY25.

The Army plans to conduct an OA of the NGSW system in 1QFY25 to support the planned transition from MTA rapid fielding programs to MCA programs in 3QFY26. DOT&E approved the operational test plan in August 2024.

» MAJOR CONTRACTORS

- SIG SAUER, Inc. – Newington, New Hampshire
- Sheltered Wings, Inc., doing business as Vortex Optics – Barneveld, Wisconsin

TEST ADEQUACY

The Army completed limited lethality testing for the 6.8mm GP ammunition against priority targets in August 2023, and an Ops Demo and cooperative vulnerability and penetration assessment on the NGSW system in October 2023, in accordance with DOT&E-approved test plans. DOT&E personnel observed the testing. DOT&E published a classified combined Ops Demo and LLA report in May 2024.

The Army completed NGSW cold weather natural environment testing in February 2024 and airborne testing in August 2024. The test plans did not require DOT&E approval, but DOT&E observed the tests. DOT&E will include its observations in the combined OA and LLA report.

Natural environment testing for tropical and hot weather environments is scheduled for FY25. The Army plans to evaluate the capability to stow weapons and the effect on crew members' ability for ingress/egress on select wheeled and tracked vehicles as part of the hot weather testing.

The Army plans to conduct limited lethality testing for the 6.8mm SP ammunition against a subset of targets and an OA in 1QFY25. The Army plans to conduct live fire testing for the 6.8mm GP ammunition against the full set of targets in 1Q – 2QFY25. DOT&E plans to publish a combined OA and LLA report in 4QFY25.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

DOT&E published a classified combined Ops Demo and LLA report in May 2024, providing preliminary assessments of the effectiveness, lethality, suitability, and survivability of the NGSW system. Preliminary assessments from the report include:

- The 6.8mm GP ammunition provides increased lethality over the M855A1 (i.e., the GP ammunition for the legacy M4A1 weapon) against the tested targets,
- Soldiers assessed the usability of the XM157 as below average/failing, and
- The XM7 with mounted XM157 demonstrated a low probability of completing one 72-hour wartime mission without incurring a critical failure.

DOT&E identified several recommendations in the combined Ops Demo and LLA report. Since the Ops Demo in October 2023, the program management office has made several technical improvements to the NGSW system to address identified deficiencies from the Ops Demo and the recommendations from DOT&E's report. These changes will be verified at the OA in 1QFY25.

RECOMMENDATIONS

The Army should:

1. Continue to redesign the suppressor to reduce heat signature and burn risk.
2. Continue to reduce noxious off-gassing of the XM250 and XM7.
3. Continue to improve the operational reliability of the XM157, XM250, and XM7.
4. Continue to address the complete list of recommendations found in DOT&E's classified combined Ops Demo and LLA report published in May 2024.

Nuclear Biological Chemical Reconnaissance Vehicle Sensor Suite Upgrade (NBCRV SSU)

The Army will employ the Nuclear Biological Chemical Reconnaissance Vehicle Sensor Suite Upgrade (NBCRV SSU) to enhance freedom of movement in large-scale combat operations requiring point; standoff; and remote chemical, biological, radiological, and nuclear (CBRN) sensing capabilities. In September 2024, the Army completed a Soldier Touchpoint (STP) of Capability Set (CS) 2.1 and desires to issue a conditional materiel release 4QFY25. Live fire testing was completed in October 2024. DOT&E is still reviewing sensor data in order to evaluate effectiveness. The NBCRV SSU may need improvements in suitability and survivability. DOT&E will publish an FOT&E report and classified annex in 3QFY25.

SYSTEM DESCRIPTION

The NBCRV is the Army's mounted CBRN reconnaissance asset available to implement CBRN-related tasks. The NBCRV is intended to provide Army maneuver commanders with critical information to make decisions in a CBRN environment. NBCRV-equipped units are required to conduct CBRN reconnaissance of route, area, or zone; CBRN survey for contamination identification and mapping; and CBRN surveillance of operational areas or named areas of interest

The SSU is intended to address capability limitations, operations and maintenance costs, and obsolescence issues of the current NBCRV. The SSU provides the current NBCRV with a variety of sensors that detect and identify chemical, biological, and nuclear hazards at standoff, as well as directly outside the vehicle. CS 2.1 includes the following suite of sensors as part of the SSU:

- The Improved Mobile Chemical Agent Detector allows operators to detect and identify chemical agents at standoff.
- The Joint Chemical Agent Detector allows the operators to detect and identify chemical agents directly outside of the vehicle.
- The Compact Stand-off Detection System detects aerosol clouds that are capable of containing biological agents. Units can then fly a Small Unmanned Aircraft System (SUAS), equipped with a Biological Aerial Sensor (BAS), to detect biological agents and collect samples that can be used with other systems to identify potential biological warfare agents.
- The Vehicle Integrated Platform Enhanced RADIAC (VIPER) can warn operators inside the vehicle of potential radiation hazards.
- The Mounted Enhanced RADIAC Long-Range Imagining Network (MERLIN) can detect and identify radiological hazards at standoff, without entering into hazardous radiation zones.

The Army is currently defining CS 2.2, which may include new sensors as well as improvements to CS 2.1 sensors, based on test findings.

MISSION

Army commanders will use the NBCRV SSU's point, standoff, and remote CBRN sensing capabilities to get the time and space to make informed, proactive, risk-based decisions, thus enhancing freedom of movement and freedom of maneuver in large-scale combat operations. SSU-equipped units will perform CBRN reconnaissance (route, area, and zone) on primary and secondary roads and cross-country, CBRN surveys (to determine limits of contamination), and CBRN surveillance, as directed by the maneuver force commander. Units equipped with NBCRV SSU will conduct reconnaissance at maneuver speeds to assess CBRN hazards at a remote distance and increase the size of the reconnaissance and surveillance areas.

PROGRAM

The NBCRV SSU is an ACAT II program testing an engineering change proposal to the M1135 Stryker NBCRV, a system already in operations and sustainment. The SSU effort is phased. The Army is seeking a conditional materiel release for CS 2.1.

The Army plans a limited CS 2.1 fielding of up to 10 vehicles from 2025 to 2027. DOT&E intends to write an FOT&E Report in 3QFY25 to support the fielding decision. The Army is planning a full material release decision in 3QFY27 for CS 2.2. DOT&E approved the TEMP for CS 2.1 testing in February 2021 and expects to approve the TEMP update for CS 2.2 testing in 4QFY25.

» MAJOR CONTRACTORS

- General Dynamics Land Systems – Sterling Heights, Michigan
- Teledyne FLIR, LLC – Stillwater, Oklahoma

TEST ADEQUACY

The program has conducted, and DOT&E has observed, all operational tests in accordance with DOT&E-approved test plans and TEMP. The Army conducted laboratory and developmental testing throughout FY22 and FY23 in accordance with the DOT&E approved TEMP. DOT&E has found testing to be adequate to properly assess the effectiveness, suitability, and survivability.

In September 2023, the program completed a limited user test (LUT) and cyber adversarial assessment using two prototype NBCRV SSU vehicles. The DOT&E-approved test plan did not include the DOT&E FY22 Annual Report recommendation to test the fielded and prototype system because the comparison is no longer valid, as the fielded system is designed to sense the threat while being inside the hazardous area while the prototype is sensing the hazard at a distance.

In September 2024, the Army conducted a Program Manager-led STP intended to demonstrate updated tactics, techniques, and procedures derived from the LUT. DOT&E observed the STP. The Army Test and Evaluation Command conducted developmental reliability testing from January to March 2024 to verify fixes made to address reliability issues found during the LUT. DOT&E will publish an FOT&E report in 3QFY25 utilizing data from the LUT and DOT&E observations from these follow-on test events.

The Army Test and Evaluation Command conducted live fire testing for CS 2.1 in October 2024 in accordance with the DOT&E-approved test plan. DOT&E personnel observed the testing and deemed it adequate to inform a live fire survivability assessment. The Army's live fire survivability program included: (1) controlled damage experiments to inform degraded mission capabilities after kinetic attack; (2) ballistic exploitation testing to determine if new welds, seams, and bolts introduce vulnerabilities to penetration from direct and indirect fire threats; (3) fire suppression nozzle inspection to determine if integration of internal components degraded the platform's ability to extinguish fires; (4) slat coverage analysis to calculate the change in covered area; and (5) egress testing to determine if modes of egress were impeded. A classified survivability annex will be published with DOT&E's FOT&E report in 3QFY25.

PERFORMANCE

» EFFECTIVENESS

DOT&E is still reviewing developmental and operational test data to assess sensor performance and their effectiveness in meeting the NBCRV SSU's requirements. The assessment of the September 2024 STP will be documented in DOT&E's report in 3QFY25.

» SUITABILITY

During the 2023 LUT, the unit struggled with some missions. Many of these difficulties were attributed to deficiencies in the training. The Army updated the training plan to address these deficiencies. In August 2024, the Army trained a unit using the new training materials. The Army conducted a soldier touch point in September 2024 to verify if the updated training had positive impacts.

After the September 2023 LUT, the program office instituted a number of fixes to address reliability issues found in testing. The program office conducted additional reliability testing from January to March 2024 to verify the fixes. The final analysis will be reported in DOT&E's FOT&E report in 3QFY25.

The FY22 DOT&E Annual Report recommended working with the SUAS vendor to identify and test batteries to enable the SUAS to accomplish its mission. The SUAS was tested in biological missions in the September 2023 LUT as well as the September STP. DOT&E will report on the battery life's effect on the mission in the DOT&E FOT&E report in 3QFY25.

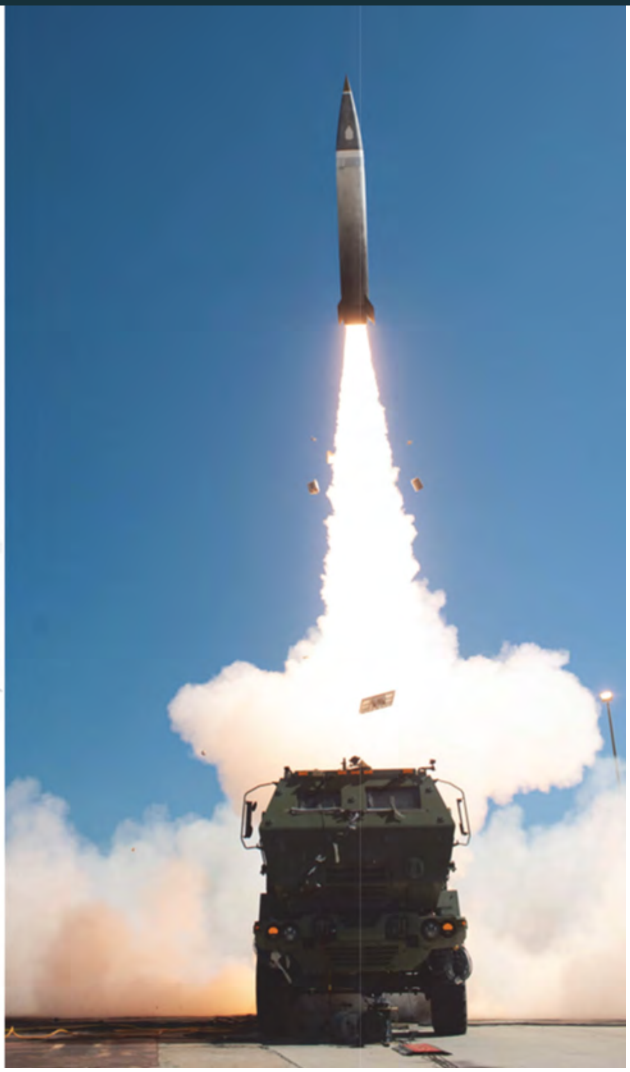
» SURVIVABILITY

The Army conducted cyber survivability in September 2023 and live fire testing in October 2024. DOT&E will present the results in the report scheduled for 3QFY25. The NBCRV SSU demonstrated the expected survivability against operationally relevant kinetic threat engagements. Additional details including threat descriptions and survivability performance will be included in the classified survivability annex to the report. Specifically, the classified annex will assess test adequacy, force protection, and mission functionality of the NBCRV SSU when exposed to enemy forces. The FY22 DOT&E Annual Report recommended integrating the NBCRV SSU onto a more survivable platform, but the Army is not planning to change the platform design due to lack of available assets and resource constraints.

RECOMMENDATIONS

DOT&E will provide recommendations in the FOT&E report scheduled for 3QFY25.

Precision Strike Missile (PrSM)



In November 2023, the Army delivered the first four Precision Strike Missiles (PrSM) as an early operational capability (EOC). The Army shot two PrSM EOC missiles at a maritime target in June 2024. Between November 2023 and August 2024, the Army executed three production qualification test (PQT) events. The Army intends to complete a limited user test (LUT) with the fifth PQT test event in 1QFY25 and the remaining four planned PQT test events by 3QFY25.

SYSTEM DESCRIPTION

The PrSM is a surface-to-surface missile with an all-weather, cluster-munition-compliant capability that is compatible with the fielded Multiple Launch Rocket System launchers. The PrSM will complement the current suite of Guided Multiple Launch Rocket System rockets and replace the Army Tactical Missile System.

MISSION

Army commanders will use the PrSM to engage and destroy preplanned targets and/or targets of opportunity in all weather conditions at extended ranges that fixed-/rotary-wing air strike systems and joint assets cannot attack, due to weather or risk to the pilot/aircraft. These targets include engaging a wide variety of precisely, and imprecisely located targets.

PROGRAM

The PrSM is an Acquisition Category IB Major Defense Acquisition Program. The Army plans to field four increments of the PrSM, with Increment 1 being the baseline capability with a threshold lethal range of 400 kilometers. Future increments will focus on increasing range and engagement against moving and hardened targets.

In June 2021, DOT&E approved the Milestone B (MS B) TEMP, which supported the MS B decision in September 2021. DOT&E's MS B TEMP approval had the following recommendations, which the Army has made some progress on:

1. 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 CONUS, to adequately evaluate the operational effectiveness and lethality of long-range precision fires against operationally representative targets.
2. Exempting 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 effect of GPS jamming on PrSM operational effectiveness and lethality.
3. Given the anticipated software changes between the LUT and IOT&E, and to ensure the cooperative vulnerability and penetration assessment (CVPA) adequately informs the adversarial assessment (AA), the Army must conduct the CVPA and AA in support of both the LUT and IOT&E. This is required to enable early identification of any vulnerabilities and to validate subsequent fixes prior to IOT&E and prior to fielding.

The Army plans to execute a LUT as a risk reduction for the IOT&E in 1QFY25, followed by IOT&E in 3QFY25 in support of the MS C full-rate production (FRP) decision scheduled for 4QFY25. The Army should allow sufficient time for IOT&E data analysis and reporting prior to the FRP decision. The Army is developing the MS C TEMP. The Army expects to field an initial operational capability by 1QFY26 and a full operational capability by 2QFY27.

» MAJOR CONTRACTOR

- Lockheed Martin Missiles and Fire Control – Grand Prairie, Texas

TEST ADEQUACY

Between November 2023 and August 2024, the Army conducted three PQT events. The Army plans to complete the nine remaining PQT shots and the LUT by 3QFY25.

The Army plans to execute IOT&E in 3QFY25 to support the MS C FRP decision in 4QFY25. In September 2024, the Army conducted a CVPA, in accordance with a DOT&E-approved cyber test plan and plans to conduct an AA prior to IOT&E. DOT&E observed the CVPA and plans to observe the AA. DOT&E will publish a combined report of the LUT and IOT&E that encompasses all production representative testing of the PrSM to inform the MS C FRP decision of 4QFY25.

The Army has made progress to incorporate sensor-to-shooter linkage with PrSM. The Army included four threshold range shots and a maximum range shot in the integrated test plan. The Army continues to refine testing for future employment of different threat electronic warfare countermeasures.

The Army has made progress in work toward establishing a long-range flight corridor in the CONUS for future range improvements and increments, to evaluate the operational effectiveness and lethality of long-range precision fires against operationally representative targets.

The Army has made progress in synchronizing the advanced field artillery tactical data system software releases and the development of the M270A2 launcher, as well as a new fire control system, to incorporate these platforms in the integrated testing. After the CVPA, the Army will identify cyber vulnerabilities prior to IOT&E and fielding.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Insufficient data are available to evaluate the operational effectiveness, lethality, suitability, and survivability of the PrSM. DOT&E will publish a combined report of the LUT and IOT&E that encompasses all production representative testing of the PRSM to inform the MS C FRP decision of 4QFY25.

RECOMMENDATIONS

The Army should:

1. Continue efforts to execute the operational test shots in the presence of operationally representative countermeasures using the most updated missile and firing platform software to evaluate the effect of GPS-jamming on PrSM operational effectiveness and lethality.
2. Allow sufficient time for IOT&E data analysis and reporting prior to the FRP decision.
3. Continue working with other stakeholders in the DoD T&E community, to establish a long-range flight corridor in the CONUS for future range improvements and increments, to evaluate the operational effectiveness and lethality of long-range precision fires against operationally representative targets.

Sentinel A4 Radar

The Sentinel A4 Program Office is unable to provide the funding and test resources necessary to execute the IOT&E described in its DOT&E-approved TEMP. In addition, production delays and system immaturity have adversely affected the program's test timelines in support of a 4QFY25 full-rate production (FRP) decision. The Army has therefore not yet finalized its planning for the March 2025 IOT&E.

The AN/MPQ-64A4 Sentinel Radar, or Sentinel A4 Radar, is a three-dimensional, X-band phased array radar system, equipped to support beyond-visual-range air defense engagements. It provides detection, classification, and reporting capabilities against rocket, artillery, and mortar (RAM) threats. Sentinel A4 also has capabilities against cruise missile (CM), unmanned aircraft system (UAS), and fixed-wing (FW) and rotary-wing (RW) aircraft threats. The system consists of a trailer, truck, and other equipment and software required for the two-person crew to move and operate the Sentinel A4 Radar and communicate with the air defense command and control system. The primary radar components and subsystems are mounted on a modified M1095 Medium Tactical Vehicle trailer. The generator and communication equipment are integrated into a M1083 Family of Medium Tactical Vehicles cargo truck.

To continue to meet its mission requirements and address counter-RAM requirements, the Army plans to replace its legacy Sentinel A3 radars with Sentinel A4 radars, which use advanced Active Electronically Scanned Array sensor technologies to improve performance. The Sentinel A4 is a multi-function radar which simultaneously provides search and track against FW and RW aircraft, UAS, CM, and RAM threats.

MISSION

The Army intends to use the Sentinel A4 Radar as a major component of the Army Integrated Air and Missile Defense (AIAMD) system-of-systems architecture. It provides a 360-degree hemispherical surveillance and fire control capability against low to mid-altitude threats, to include CM, UAS, FW and RW aircraft, and RAM threats. The Army also intends for the Sentinel A4 radar to be used in the Defense of Guam architecture.

PROGRAM

Sentinel A4 Radar is an Acquisition Category II program that DOT&E placed on oversight in February 2023. The Milestone Decision Authority approved the program's Milestone C decision in July 2023. The baseline acquisition objective is 240 radars, including the radars being procured for the Defense of Guam mission.

The program office submitted a TEMP in September 2023 for DOT&E's approval, but DOT&E requested the Army address several items and resubmit the document. The updated TEMP was approved in March 2024. The Army plans to conduct IOT&E in 2Q – 3QFY25. DOT&E will publish a classified report following the conclusion of the IOT&E to inform the FRP decision in 4QFY25.

» MAJOR CONTRACTOR

- Lockheed Martin Corporation – Syracuse, New York

TEST ADEQUACY

In 2QFY24, the Sentinel Program Office began delta-developmental testing, which is intended to resolve system deficiencies and complete functional testing that was either deferred or failed during initial developmental testing. Due to delays in delivery of the User Operational Evaluation System test articles, the program office expects delta-developmental testing to conclude in 2Q FY25, which overlaps with the start of IOT&E.

The program office is unable to provide the IOT&E funding outlined in the TEMP DOT&E approved in March 2024. Production delays and system immaturity have also impacted the program office's ability to deliver the resources necessary to conduct the IOT&E described in the DOT&E-approved TEMP. The Army Test and Evaluation Command has developed a descoped plan that fits within the time and budgetary constraints, but the new plan does not reflect the testing in the DOT&E-approved TEMP and will not assess all the Sentinel A4's intended capabilities in an operational environment. DOT&E is working with the Army to determine if the descoped plan will be adequate to evaluate the radar's effectiveness, suitability, and survivability.

The Army plans for the Sentinel A4 to participate in future Integrated Fires Test Campaign operational test events, integrating with AIAMD and other air and missile defense sensors and shooters.

These events rely on modeling and simulation (M&S) tools to execute simulated air battle scenarios that cannot be replicated with real aircraft and threats. The Sentinel A4 program must complete verification, validation, and accreditation of the M&S tools that will support a credible assessment of operational effectiveness in a realistic threat environment.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E will provide an assessment of Sentinel A4 Radar operational effectiveness, suitability, and survivability following the completion of an adequate IOT&E.

RECOMMENDATIONS

The Army should:

1. Provide the resources necessary to execute IOT&E in accordance with the DOT&E-approved TEMP.
2. Develop M&S tools and a verification, validation, and accreditation strategy that supports use of those M&S tools in future Sentinel A4 operational testing, including as part of the Integrated Fires Test Campaign.

Soldier Protection System (SPS)

The Army continues to field the Second Generation Modular Scalable Vest (MSV Gen II) and Third Generation Vital Torso Protection (VTP Gen III) hard armor plates, with fielding expected to complete in 4QFY28. The Army started fielding of the Second Generation Integrated Head Protection System (IHPS Gen II) in February 2024. Since last year's Annual Report, the Army completed First Article Testing (FAT) for multiple vendors and over 250 Lot Acceptance Tests (LATs) for all Soldier Protection System (SPS) systems, with one LAT failure. DOT&E provided a briefing package to the House Committee on Armed Services in November 2023, on female soldier and marine protective equipment systems.

SYSTEM DESCRIPTION

The SPS is a suite of personal protection subsystems. The Army intends to provide equal or increased levels of protection against small-arms and fragmenting threats compared to existing personal protective equipment (PPE) at a reduced weight. 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 their mission. 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 consists of three major subsystems: Torso and Extremity Protection (TEP) system, Integrated Head Protection System (IHPS), and the Vital Torso Protection (VTP) system. Each subsystem is further comprised of multiple components.

MISSION

Units will accomplish assigned missions with soldiers wearing the SPS, which provides protection against injury from a variety of ballistic (small-arms and fragmenting) threats.

PROGRAM

SPS is an Acquisition Category III program comprised of three major subsystems. Each of the three major subsystems is developed, tested, and fielded independently. The Army entered full-rate production of the TEP system in September 2016, the IHPS in October 2018, and the first generation of the VTP system 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
- IHPS Gen II, formerly known as Next Generation-Integrated Head Protection System (NG-IHPS), is replacing IHPS

The Army is modernizing the VTP program to offer multiple Personal Protective Equipment Posture (PPEP) levels and provide warfighter protection scalability, and mobility. The Army is adjusting its ballistic protection requirements to align with these PPEP levels.

The Army started early fielding of MSV Gen II and VTP Gen III plates in 4QFY21 and plans to field through 4QFY28. The target acquisition quantity is approximately 150,000 sets of each of the SPS torso subsystems. The Army started fielding of the IHPS Gen II in February 2024 to the 82nd Airborne Division.

DOT&E, in coordination with the Program Executive Officer Soldier and the Commander of Marine Corps Systems Command, provided a briefing package to the House Committee on Armed Services in November 2023 in response to National Defense Authorization Act for Fiscal Year 2023, on female soldier and marine protective equipment evaluation and what, if any, processes are in place to ensure future body-worn systems are evaluated for fit and appropriate wear through the 98th percentile of all possible sizes.

» MAJOR CONTRACTORS

TEP Vendors:

- 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 (MSV, BCS)
- Carter Enterprises, LLC – Brooklyn, New York (BCS)

VTP Vendors:

- Engense, Inc. – Camarillo, California (ESBI)
- Florida Armor, LCC – Miami Lakes, Florida (ESBI)
- Leading Technology Composites, Inc. – Wichita, Kansas (ESAPI, ESBI)
- Integris Composites – Hebron, Ohio (ESAPI, XSBI)

IHPS Gen II Vendors:

- Avon Protection – Salem, New Hampshire
- Gentex Corporation – Carbondale, Pennsylvania

TEST ADEQUACY

The Army conducts multiple FATs and LATs every year to qualify new vendors and designs. In FY24, the Army completed FAT for multiple vendors to include: MSV and VTP's Enhanced Small Arms Protective Insert (ESAPI) designs. The designs that passed FAT proceeded to LAT. The Army completed all test series at Aberdeen Test Center, Maryland, in accordance with DOT&E-approved test plans. DOT&E observed most of the FAT testing. The Army completed an expanded developmental test (DT) series for VTP Gen III ESAPI against nonstandard fragmenting threats for one vendor in 1QFY24 and expects to complete the series for a second vendor in 1QFY25.

In 1QFY25, the Army conducted expanded DT of the IHPS Gen II to evaluate its protective capabilities against threats that surpass the standard requirements tested in FAT and LAT. The testing also included additional engagement conditions, such as oblique angles and various velocity regimes and comparisons with the legacy IHPS helmet. The Army intends to conduct full-up system level testing in 2QFY25 in accordance with a DOT&E approved test plan to assess potential injuries to soldiers from threats that penetrate the IHPS Gen II, and to compare the results with the legacy IHPS protection. DOT&E plans to publish a survivability report in 3QFY25.

In response to a recommendation in the FY23 Annual Report, the Army has taken steps to expand modeling and simulation capabilities. In 1QFY25, the Army plans to conduct a test series using Gen III VTP backed with ballistic gel to be able to assess potential injuries to soldiers from penetrating threats using modeling and simulation.

Current PPE test methods are limited in the ability to accurately assess soldier injuries. Test mannequins for soft armor vests and hard armor plates do not sufficiently mimic the wearer. The Army developed the Hybrid Foam Mannequin to address these limitations in FY16, but still has not finished the accreditation process. As DOT&E recommended in the FY22 and FY23 Annual Reports, the Army should complete accreditation of the Hybrid Foam Mannequin.

DOT&E published the hard body armor test protocols for FAT and LAT in 2010. The published protocols are based on hard armor plates that have five sizes, but current Army hard armor plates have eight sizes. DOT&E is in the process of updating the outdated hard body armor test protocols for FAT and LAT to apply to current hard armor plate sizes and adopt the latest test and evaluation best practices. Representatives from the Army, Marine Corps, Navy, U.S. Special Operations Command, and Defense Logistics Agency are participating in the development of the protocol and the review process. DOT&E plans to publish an updated protocol in 3QFY25.

PERFORMANCE

» SURVIVABILITY

One MSV Gen II design was submitted and tested in FY24 and met the ballistic FAT requirements. Three VTP ESAPI designs were submitted and tested for FAT in FY24. Two of the three designs met the ballistic FAT requirements and proceeded to LAT testing. There were no VTP XSAPI Gen III or IHPS Gen II designs submitted for FAT testing in FY24.

The Army conducted over 280 LATs across all SPS systems in FY24. There were approximately 180 LATs for MSV, 90 LATs for VTP, and 20 LATs for IHPS Gen II. All lots passed the Army's threshold requirements except for one VTP lot. The Army is exploring courses of action to address this failure.

Additional testing is required to assess IHPS Gen II protection compared to legacy helmets and to assess the degree of potential injuries to warfighters from penetrating threats to the IHPS Gen II. The Army has taken steps to address this recommendation from the FY23 Annual Report, and this testing is planned for 2QFY25.

RECOMMENDATION

The Army should:

1. Start the accreditation process of the Hybrid Foam Mannequin or develop another accredited soldier surrogate for assessing injuries from penetrating threats to hard and soft body armor.

Stryker Family of Vehicles (FoV)

In FY24, the Army conducted Stryker 30mm Medium Caliber Weapon System FOT&E and LFT&E at numerous military test sites. In November 2024, DOT&E published a combined FOT&E and LFT&E report with a classified annex, evaluating the Stryker 30mm variant's operational effectiveness, suitability, and survivability.

SYSTEM DESCRIPTION

The Stryker Family of Vehicles (FoV) has eight variants. This report is focused on the Stryker Medium Caliber Weapon System, referred to as the Stryker 30mm, which integrates the XM813 30mm cannon on to the infantry carrier vehicle Double-V Hull A1 chassis in an unmanned turret. The Stryker 30mm maintains comparable mobility characteristics with the Double-V Hull A1 FoV. It has a crew of two and carries up to nine dismounted soldiers.

The Stryker 30mm is fielded in infantry companies and scout platoons in the infantry battalions, is intended to increase the lethality of the formation, and improves the survivability for the soldier and system against conventional and asymmetric threats.

MISSION

Combatant commanders use Stryker brigade combat teams to conduct decisive action across the range of military operations by providing a significantly large, dismounted maneuver force capable of rapid tactical mobility. The Stryker FoV provides mobile and protected transport to the assigned crew/squad, enables formations with rapid movement to positions of tactical advantage, and provides lethal and destructive direct fire support against enemy forces, denying them freedom of movement on the battlefield. The primary role of the Stryker 30mm is to provide protected transport for infantry squads and scout teams and provide direct fire support for the infantry squad during the dismounted assault.

PROGRAM

The Stryker 30mm is an Acquisition Category II-equivalent engineering change proposal to the existing Double-V Hull A1 fleet. The Milestone Decision Authority is the Program Executive Officer, Ground Combat Systems. DOT&E published a classified combined FOT&E and LFT&E report in November 2024 to support the Army's materiel release decision. The Army intends to produce 269 Stryker 30mm vehicles to field to three of the seven Stryker brigade combat teams.

» MAJOR CONTRACTORS

- General Dynamics Land Systems – Sterling Heights, Michigan
- Oshkosh Defense – Oshkosh, Wisconsin
- Rafael Advanced Defense Systems Ltd. – Haifa, Israel

TEST ADEQUACY

The Army conducted the Stryker 30mm FOT&E and LFT&E from 1QFY24 to 3QFY24 at numerous military test sites. All testing was in accordance with the DOT&E-approved test plans and observed by DOT&E. The testing was adequate to support an evaluation.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E's assessment of Stryker 30mm operational effectiveness, suitability, and survivability can be found in the combined FOT&E and LFT&E report with classified annex, dated November 2024.

RECOMMENDATION

The Army should:

1. Address the recommendations in the combined FOT&E and LFT&E report with classified annex, dated November 2024.

Synthetic Training Environment Live Training Systems (STE-LTS)

In February 2024, the Army conducted the Synthetic Training Environment Live Training System Increment 1 (STE-LTS Inc. 1) Operational Demonstration (Ops Demo). The STE-LTS Inc. 1 Ops Demo will support a Middle Tier of Acquisition (MTA) rapid prototyping (RP) to rapid fielding (RF) transition decision in 1QFY25. DOT&E published an Ops Demo report in August 2024.

SYSTEM DESCRIPTION

STE is the Army's next generation, holistic combined arms collective training capability, intended to enable leaders, soldiers, and units from squad through the Army Service Component Command to train in complex operational environments at the point of need. The STE-LTS program is one of five main signature efforts of the STE and focuses on the development of a next generation live training architecture to enable the realistic exercise of unit combat weapons up to brigade level. STE-LTS seeks to address the brigade combat team weapon types and effects not currently simulated by the Army's legacy live training system, the Instrumented - Multiple Integrated Laser Engagement System (I-MILES). STE-LTS encompasses 12 engagement types and 5 instrumentation enablers that make up the live training capability framework that supports Army combined arms maneuver training. The engagement types include direct fire, counter-defilade fire, indirect fire, dropped, placed, or thrown objects, guided and autonomous weapons, directed and radiant energy weapons, plumes (i.e., chemical, biological, and nuclear), and connections (i.e., information warfare). The training instrumentation enablers include calculations, network, sensors, terrain, and transmitters.

STE-LTS Inc.1 is the first increment of the STE-LTS program. It consists of five training device types intended to replicate employment and simulate the battlefield effects of weapon systems during force-on-force training: (1) hand grenades, (2) Claymore mines, (3) 60mm mortars, (4) 81mm mortars, and (5) Stinger anti-aircraft missiles. Legacy Stinger training devices have reached the end of their life cycle, and the Army does not currently have force-on-force training devices for the other weapon types.

Future planned upgrades will include the following:

- Replacement of the direct fire weapon simulation capabilities of the legacy I-MILES.
- Additional weapon types such as counter defilade and guided weapon systems.
- Next generation weapon systems such as directed energy and cyber weapons.

MISSION

Unit commanders, along with the Army's combat training centers and home station training staff, will use the STE-LTS training technologies to improve individual soldier lethality and survivability, and to improve, accelerate, and sustain unit-level combined arms maneuver proficiency through repetition in a realistic combat environment. STE-LTS next generation systems are intended to replicate more engagement types, improve sensory feedback, increase realism of direct fire engagement, increase realism of battle damage assessments, and improve after action reviews and instrumentation at the combat training centers and home stations.

PROGRAM

The STE-LTS is an MTA RP program comprised of three planned increments of training capability development that will transition to an MTA RF or Major Capability Acquisition (MCA) pathway for product maturation, production, and fielding.

- STE-LTS Inc.1 capabilities will transition to an MTA RF program, pending an outcome determination decision in 1QFY25. DOT&E published an operational demonstration (Ops Demo) report in August 2024 to inform the Army's transition decision. The program office is planning to begin a limited fielding to the Joint Readiness Training Center (JRTC), Fort Johnson, Louisiana, and the National Training Center (NTC), Fort Irwin, California in 3QFY26. A follow-on MCA program of record will continue development and extend the fielding to home stations training facilities.
- STE-LTS Inc. 2 capabilities are intended to replace the direct fire weapon simulation capabilities of the legacy I-MILES while adding additional weapon types such as counter defilade and guided weapon systems. The Army is planning an Ops Demo in 2QFY26 supporting an outcome determination to transition to an MCA program in 3QFY26.
- STE-LTS Inc. 3 capabilities include next generation weapon systems such as directed energy and cyber weapons. An Ops Demo and outcome determination date has not yet been established for inc. 3 capabilities.

The STE-LTS TES covering increments 1 and 2 is in development and should be submitted to DOT&E in 1QFY25 for approval.

» MAJOR CONTRACTORS

- Cubic Corporation – Orlando, Florida (60mm and 81mm mortar training devices)
- Cole Engineering Services, Inc. (CESI) – Orlando, Florida (stinger anti-aircraft missile training devices)
- Serious Simulations, LLC – Oviedo, Florida (hand grenade

and Claymore mine training devices)

TEST ADEQUACY

In February 2024, the Army conducted the STE-LTS Inc. 1 Ops Demo at the JRTC, Fort Johnson, Louisiana, in accordance with a DOT&E-approved test plan. The Ops Demo was observed by DOT&E and adequate to inform a preliminary assessment of system performance and inform an MTA RP to RF transition decision in 1QFY25. DOT&E published an Ops Demo report in August 2024.

PERFORMANCE

» EFFECTIVENESS

Data from the Ops Demo indicate that the STE-LTS Inc. 1 training devices have potential to improve individual soldier and unit collective training through the enhanced realism of having the five additional weapon types in the live force-on-force training environment. Soldier lethality and survivability may be improved as soldiers are exposed to the weapons effects in real time during close combat training.

The Ops Demo report identified several minor issues with weapon employment and effects characteristics that impact the operational realism of force-on-force training. Of particular interest is ensuring that the lethal effects of these weapons are accurately simulated in real time so that soldiers develop an appropriate sense of the effectiveness when employing those weapons, as well as the danger posed when they are employed by the enemy. Additional details can be found in the August 2024 Ops Demo report.

» SUITABILITY

Data from the STE-LTS Inc.1 Ops Demo indicate that improvements in the reliability of training devices and their integration with the JRTC network are needed prior to fielding and widescale use supporting JRTC and NTC training rotations. Each of the training device types had unique reliability and integration failures that when combined, resulted in reduced combat realism during the training evolutions. If corrected, the STE-LTS inc. 1 training devices will enhance combat realism and provided needed individual and unit collective training. Additional details can be found in the August 2024 Ops Demo report.

The STE-LTS Inc. 1 Program Office has acknowledged many of the suitability findings in the DOT&E Ops Demo report and has begun pursuing technical solutions with the device vendors. A follow-on test to validate training device improvements while demonstrating successful network integration was conducted in August 2024 at the NTC. Additional system improvements and testing are being planned for FY25 prior to fielding to the JRTC and NTC.

» SURVIVABILITY

The Army showed through analysis that the STE-LTS Inc. 1 training devices do not present a cybersecurity risk to the JRTC or NTC networks. DOT&E concurred with the Army analysis, and therefore cyber survivability was not assessed. STE-LTS increments 2 and 3 will require a system specific review to determine what cyber survivability testing is required. There are no other survivability requirements for the STE-LTS Inc. 1 training devices.

RECOMMENDATIONS

The Army should:

1. Continue to refine STE-LTS Inc.1 training device employment characteristics to minimize the differences between the training devices and the real weapon systems.
2. Determine and address the cause of inconsistent integration with the JRTC network.
3. Determine and address the cause of identified reliability issues.
4. Verify integration and reliability fixes through integrated testing prior to beginning production.

Terrestrial Layer System Brigade Combat Team (TLS BCT)

In September 2023, the Army conducted an operational demonstration (Ops Demo) for the Terrestrial Layer System Brigade Combat Team (TLS BCT) Stryker BCT (TLS SBCT). Based on the results, the Army decided to separate TLS SBCT into two distinct variants: signals intelligence (SIGINT) and electronic warfare (EW), and as a result, DOT&E did not publish a report.

In November 2023, the Army conducted an Ops Demo for TLS BCT Manpack (TLS BCT MP). DOT&E published a classified TLS BCT MP Ops Demo report in May 2024. TLS BCT MP transitioned into Middle Tier of Acquisition (MTA) rapid fielding (RF) in April 2024. The Army began equipping TLS BCT MP to select infantry BCT (IBCT) units as an early capability in September 2024. The Army is planning an operational assessment (OA) in June 2026 to support fielding to all BCT.

SYSTEM DESCRIPTION

The Army envisions the TLS BCT as the next generation tactical system, delivering an integrated suite of SIGINT, EW, and cyberspace operations capabilities (future objective requirement) to enable multi-domain operations within the SIGINT Collection and EW Team. The Army plans to deploy TLS BCT variants to SBCT, armored BCT (ABCT), and IBCT units.

TLS BCT modernizes the terrestrial layer at the BCT-level by expanding the capabilities to control the electromagnetic spectrum (range of frequencies), thereby allowing commanders greater access and control of the spectrum, using ground assets assigned to the BCT. This expanded ground-based capability will provide indications and warnings, force protection, and situational awareness to influence the commander's decision cycle, improve targeting timeliness and accuracy, and provide the maneuver commander with electronic attack and offensive cyberspace operation options to deny, degrade, disrupt, or otherwise manipulate the targeted force.

The Army intends to integrate the TLS SBCT variant onto the Stryker Medical Evacuation Double-V Hull A1 and the TLS ABCT variant onto one of the Armored Multi-Purpose Vehicle variants. The TLS IBCT variant will be a man-packable configuration known as the Manpack (TLS BCT MP). Each variant is designed to provide the warfighter with critical situational awareness of the enemy through detection, identification, location, exploitation, and disruption of enemy signals of interest (communications and non-communications) while operating on-the-move and at-the-halt.

MISSION

The TLS BCT provides robust line-of-sight and beyond line-of-sight voice and data communications capabilities to interface directly with brigade, division, corps and Army-level collection and analysis elements, and with on-platform mission command systems. The TLS BCT operates on-the-move, at-the-halt, or dismounted. The TLS BCT will operate near the forward lines of operating troops.

PROGRAM

TLS SBCT entered the MTA rapid prototyping pathway in May 2020. DOT&E approved the Ops Demo test plan in August 2023. Following the Ops Demo for TLS SBCT in September 2023, the Army decided to separate the SIGINT capability from the EW capability. The Army is updating the current design for SIGINT-only capability and developing a new design for the EW capability. The Army plans to conduct a follow-on Ops Demo for TLS SBCT SIGINT in June 2026. An Ops Demo for the EW variant will follow sometime later.

TLS BCT MP entered the MTA rapid prototyping pathway in May 2020. DOT&E approved the Ops Demo test plan in October 2023. Following the Ops Demo, the Army transitioned TLS BCT MP to the MTA RF pathway in April 2024. The first TLS BCT MP unit was equipped in September 2024. The Army plans to conduct an OA in June 2026.

The Army has deferred T&E of the TLS ABCT and TLS BCT EW variants.

» MAJOR CONTRACTORS

- Lockheed Martin Corporation – Liverpool, New York (SBCT)
- Mastodon Design, LLC, a CACI International Inc. company – Rochester, New York (IBCT MP)

TEST ADEQUACY

The Army conducted an Ops Demo for TLS SBCT in September 2023 to support an MTA RF transition decision, with observation by DOT&E personnel. The Army was unable to conduct the Ops Demo in accordance with the DOT&E-approved plan due to a lack of accredited threat emitters to test realistic operational signal density and congestion for electromagnetic systems. However, the Ops Demo was adequate to identify operational issues related to combining SIGINT and EW capabilities onto one platform. The Army has decided to separate them into two distinct systems. DOT&E expects the Army to submit a TES for the TLS SBCT SIGINT variant in December 2024. The EW variant will follow sometime later.

The Army completed a cyber tabletop exercise for TLS SBCT in October 2023 at the National Cyber Range, Florida, to assess the system architecture, complete attack space, supply chain, and potential points of cyber ingress. With support from the program office, operational test agencies, cyber test teams, and DOT&E, the Army investigated all ways to potentially cyber compromise the TLS SBCT.

The Army conducted an Ops Demo for TLS BCT MP in November 2023 to support an MTA RF transition decision, with observation by DOT&E personnel. As with TLS SBCT, the Army was unable to conduct the Ops Demo in accordance with the DOT&E-approved plan due to the lack of accredited threat emitters as well as restrictions on jamming duration. However, the Ops Demo was adequate to support the program transition to MTA RF and a decision to field an early capability to select IBCT units. DOT&E published a classified TLS BCT MP Ops Demo report in May 2024. The Army will submit a TES for TLS BCT MP MTA RF phase in April 2025 and test plan for the OA in June 2026.

PERFORMANCE

» EFFECTIVENESS

The TLS SBCT Ops Demo did not provide sufficient data to assess operational effectiveness. The Army will now conduct separate Ops Demos for SIGINT and EW. DOT&E will report on TLS SBCT SIGINT and EW operational effectiveness after the completion of the Ops Demos.

TLS BCT MP demonstrated the potential to be operationally effective. Soldiers equipped with TLS BCT MP were able to detect enemy emitter signals with some error. The TLS BCT MP SIGINT capability did not provide soldiers with information on the source of the emission. TLS BCT MP successfully conducted electronic attack and disrupted enemy voice communications. The Army's intended networks may not provide sufficient data rates to support the TLS BCT MP electromagnetic support missions. Additional details can be found in DOT&E's classified TLS BCT MP Ops Demo report.

» SUITABILITY

The TLS SBCT Ops Demo did not provide sufficient data to assess operational suitability. The Army will now conduct separate Ops Demos for SIGINT and EW. DOT&E will report on TLS SBCT SIGINT and EW operational suitability after the completion of the Ops Demos.

TLS BCT MP demonstrated the potential to be operationally suitable. Limited TLS BCT MP operator training restricted the evaluation of the system to only those tasks conducted during the Ops Demo. TLS BCT MP maintenance training was not executed, tested, and evaluated. TLS BCT MP weight and power demands could limit dismounted mission duration. The TLS BCT MP Ops Demo uncovered one safety concern: TLC BCT MP antennas must be kept at least 10 inches (24 centimeters) away from the human body to ensure a safe separation distance necessary to prevent over exposing soldiers to radiofrequency radiation. Additional details can be found in DOT&E's classified TLS BCT MP Ops Demo report.

» SURVIVABILITY

DOT&E cannot report on the cyber survivability of the TLS SBCT because the Army is making a significant change by separating the SIGINT and EW capabilities. DOT&E expects the Army to include cyber survivability testing in future TESs for the TLS SBCT SIGINT and EW variants.

The Army did not execute any kinetic survivability testing in conjunction with the Ops Demo for TLS SBCT. DOT&E expects the Army to include kinetic survivability testing in future TESs for the TLS SBCT SIGINT and EW variants.

Cyber and kinetic survivability testing are not required for TLS BCT MP.

RECOMMENDATIONS

PEO IEW&S should:

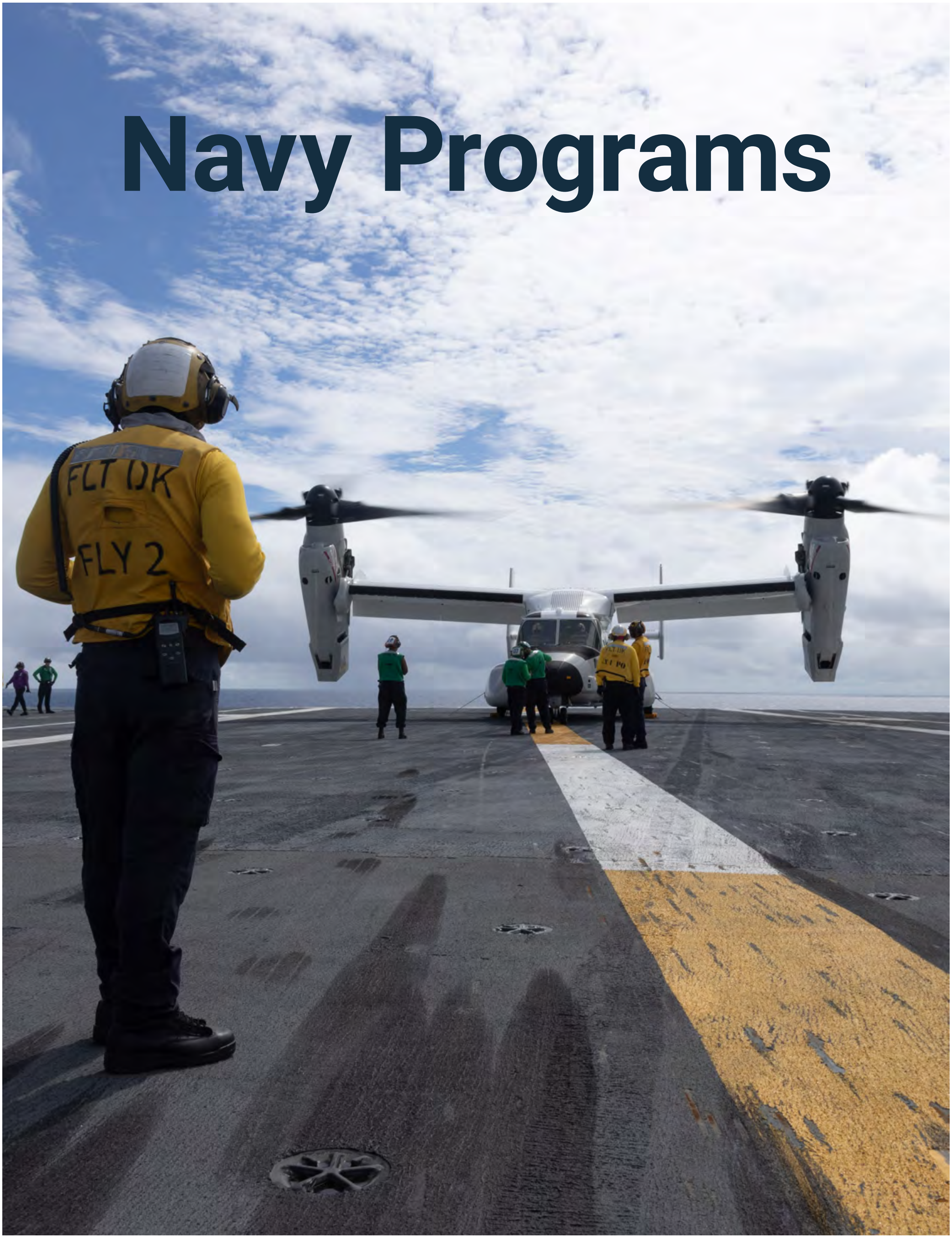
1. Submit a TES for each variant of TLS BCT to DOT&E for approval. For the TLS SBCT variants, these should include cyber and kinetic survivability testing.
2. Address safety concerns discovered during TLS BCT MP Ops Demo.

3. Address software and hardware integration deficiencies discovered during TLS BCT testing to date.
4. Accredit the threat emitters needed for operational testing.
5. Submit test plans for TLS SBCT and Manpack variants.
6. Conduct an operationally realistic OA for TLS BCT MP, to include assessment of the system to enable dismounted soldiers to conduct full end-to-end electromagnetic missions against accredited threat emitters.

DEPARTMENT OF THE NAVY PROGRAMS

This page intentionally left blank.

Navy Programs



This page intentionally left blank.

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

In FY24, the Navy conducted one Advanced Anti-Radiation Guided Missile – Extended Range (AARGM-ER) integrated test (IT) weapon event from an F/A-18F and a cooperative vulnerability and penetration assessment (CVPA). Flight testing planned for FY24 was delayed by software changes required to address problems identified in testing. Developmental captive-carry events began in June 2024 to verify the software updates designed to fix discrepancies discovered during developmental test (DT) and IT events. AARGM-ER free-flight IT events are scheduled to resume in 1QFY25. Formal IOT&E weapons employment test events are scheduled to begin in 2QFY25.

SYSTEM DESCRIPTION

The AGM-88G AARGM-ER is an air-to-ground missile that employs a multi-mode seeker to passively detect and guide on radio frequency (RF) emissions from a threat radar site, and then transition to an active millimeter wave terminal radar seeker to detect, track, and suppress or destroy RF-enabled, surface-to-air missile systems. AARGM-ER uses the same millimeter-wave radar as AARGM, but has a new warhead, a larger diameter, a shorter length to enable F-35A/C internal bay carriage, and a new rocket motor that provides increased lethality at longer range against modern surface-to-air threats. The F/A-18E/F and EA-18G are threshold employment platforms for the AARGM-ER. The F/A-18C/D and F-35A/B/C (internal carriage for the F-35A/C variants and external carriage for all variants) are designated as objective employment platforms.

MISSION

Commanders will use aircraft equipped with AARGM-ER to suppress or destroy enemy air defenses. AARGM-ER will target relocatable threat radars that employ shutdown tactics. The multi-mode seeker of AARGM-ER is intended to counter enemy radar shutdown tactics.

PROGRAM

AARGM-ER is an Acquisition Category IB program. DOT&E approved the AARGM-ER Milestone C TEMP in May 2021 and an updated cybersecurity test strategy in August 2022. The production and deployment phase, along with the award of the low-rate initial production contract, came after the Navy's Knowledge Point-4 program review in July 2021. DOT&E approved the IT portion of the IOT&E test plan in October 2023. The Navy will submit an IOT&E test plan to DOT&E for approval prior to operational testing. The first phase of cyber survivability testing began in September 2023 with a CVPA. IT free flights are scheduled to resume in 1QFY25. The Navy is planning for AARGM-ER initial operational capability in 4QFY25.

» MAJOR CONTRACTOR

- Northrop Grumman Corporation – Northridge, California

TEST ADEQUACY

The program completed six DT weapons employment events between FY21 and FY23, using F/A-18E/F aircraft, in accordance with the DOT&E-approved TEMP. These test events were conducted to identify problems prior to beginning integrated testing. In October 2023, the program attempted one IT weapons employment test event from an F/A-18F against a threat-representative integrated air defense land target at the China Lake Range in California. The test was conducted in accordance with the DOT&E-approved IT plan. DOT&E observed this IT event. AARGM-ER exhibited performance discrepancies during each of the six DT weapons employment events and the single IT weapons employment event. The DT captive-carry test events revealed potential discrepancies, but the compressed schedule challenged the program's ability to implement fixes and resulted in at least four of the seven DT/IT weapons employment test events occurring with unresolved discrepancies. Most discrepancies found during DT and IT flight test events required missile software updates. However, none of the implemented software updates were accomplished as quickly as forecasted, resulting in test delays. The Navy has not accomplished any free flight events with EA-18G aircraft.

Additional weapons employment testing was not accomplished in FY24 due to software updates required to address the problems identified during the IT event and subsequent captive-carry test events. A series of previously unplanned DT captive-carry test events began in June 2024 to confirm the software fixes, characterize performance, support problem identification and correction, and to collect data for modeling and simulation (M&S) verification and validation.

The extended range and advanced capabilities of AARGM-ER, along with the requirement to test against advanced target sets in threat-representative and contested electromagnetic operational environments, exceed the infrastructure capabilities of most test ranges. As a result, range availability has been a challenge for the program, necessitating adjustments to the test plan and contributing to schedule delays. The two most recent weapons employment tests demonstrated progress in this regard, as cooperation among the Air Force's Nevada Test and Training Range, the Navy's China Lake Range, and the Federal Aviation Administration enabled employment of AARGM-ER shots from one range to a complex target set in the other range at almost the threshold employment range of the missile.

The program did not conduct the adversarial cyber developmental test required by the DOT&E-approved cybersecurity test strategy prior to beginning operational cyber survivability testing with the CVPA. The Navy conducted an AARGM-ER CVPA in September 2023, but there were deviations from the DOT&E-approved cybersecurity test plan. The Navy conducted a second CVPA in April 2024, during which the Navy completed all the testing in the DOT&E-approved test plan. However, the significant software changes since April might require additional CVPA testing prior to the adversarial assessment. DOT&E observed both CVPA events.

The program completed five arena tests of the newly designed AARGM-ER warhead between December 2021 and September 2023 and provided data from these tests to DOT&E in June 2024. These data are used to create lethality data files required by the M&S to evaluate effectiveness against modeled targets. The data are also used to optimize system weaponeering and fuzing against a range of operational targets. These tests were conducted in accordance with the approved test plan, with one deviation. DOT&E is analyzing the potential impacts of this deviation from the approved test plan and will work with the program office to determine if testing needs to be re-accomplished.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

The current data available are insufficient to provide a preliminary assessment of AARGM-ER operational effectiveness, suitability, survivability, or lethality. Additional testing and flight data collection of the AARGM-ER are required from both F/A-18E/F and the EA-18G threshold platforms. Successful end-to-end functionality of all AARGM-ER-designed missile components, employed from the threshold range or beyond, has not yet been demonstrated.

RECOMMENDATIONS

The Navy should:

1. Update the IOT&E test plan with DOT&E recommendations and submit for DOT&E approval prior to operational testing.
2. Demonstrate a successful end-to-end operational test of AARGM-ER by employing at or beyond the threshold range out to the objective range, including guidance and warhead lethality, in a threat representative environment, as discussed in the FY23 Annual Report.
3. Increase the completeness and adequacy of data for M&S by incorporating the EA-18G threshold platform for free flight events, with an overall increase of captive-carry events, to better identify discrepancies before initial operational capability and assist during a compressed FY25 testing period, as discussed in the FY23 Annual Report.

Aegis Modernization Program

In FY24, the Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted operational testing on ships with the Advanced Capability Build (ACB) 16, Baseline 9.2.0 and Capability Package (CP) 22-1 variants, of the Aegis Weapon System (AWS). DOT&E will publish an early fielding report for the CP 22-1 variant in 2QFY25. Operational testing continues to demonstrate hardware reliability and software stability concerns with the Aegis Display System (ADS) and the AN/SPY-1 radar. The Navy expects to complete operational assessment of ACB 16 variants (up to CP 22-1) in FY25. The Navy expects to submit a TEMP update for DOT&E approval in FY25 that will provide a test program for the recent CP 24 (Baseline 9.2.4) update of ACB 16.

In March 2024, a Flight III *Arleigh Burke* (DDG 51)-class destroyer with the Baseline 10.0 participated in a live fire test event to evaluate combined Ballistic Missile Defense and Anti-Air Warfare. The Navy expects to conduct operational assessment of Baseline 10.0 through FY28.

SYSTEM DESCRIPTION

The Aegis Combat System (ACS) is an advanced weapon control system comprised of sensors, control elements, and weapons to detect, track, engage, and destroy airborne, surface, and subsurface threats. The ACS's key components include: (1) AWS that comprises the hardware and software to integrate combat systems capabilities, as well as the legacy AN/SPY-1 (series) radar; (2) the AN/SPY-6(V)1 radar on Flight III DDGs; (3) a Phalanx

Close-In Weapon System; (4) a 5-inch diameter multipurpose gun system; (5) the Vertical Launch System that can launch Tomahawk missiles, SM-2, SM-3, and SM-6 Standard Missiles, Evolved Sea Sparrow Missiles (ESSM), and Vertical Launch Anti-Submarine Rockets; (6) AN/SPQ-9B or SPS-67 surface search radars; (7) Surface Electronic Warfare Improvement Program (AN/SLQ-32(V)(series)); (8) Cooperative Engagement Capability; and (9) the AN/SQQ-89(V)15 undersea warfare suite, which also integrates with the MH-60R helicopter when embarked. The Navy's Aegis Modernization Program updates the AWS to support improved integration and advancing capabilities on *Ticonderoga*-class (CG 47) guided missile cruisers and *Arleigh Burke*-class (DDG 51) guided missile destroyers.

MISSION

The Joint Force Commander/Strike Group Commander employs CG 47 ships and DDG 51 ships equipped with Aegis to conduct:

- Area and self-defense anti-air warfare in defense of the strike group.
- Anti-surface warfare.
- Anti-submarine warfare.
- Strike warfare, when armed with Tomahawk missiles.
- Integrated air and missile defense (IAMD).
- Operations independently or in concert with carrier or expeditionary strike groups and with other joint or coalition partners.

PROGRAM

The Aegis Modernization Program is a non-acquisition category program of record. The Navy intends five incremental deliveries within ACB 16: Baseline 9.2.0, Baseline 9.2.1, Baseline 9.2.2, Baseline 9.2.3 (referred to as CP 22-1), and Baseline 9.2.4 (referred to as CP 24). Each baseline update is intended to build on the previous baseline and improve capabilities through a combination of hardware and software upgrades. To support Navy testing, DOT&E approved the ACB 16 (Baseline 9.2) test plan in July 2023. DOT&E approved the TEMP for the test program of ACB 16 (Baseline 9 series) in September 2024. The TEMP requires an update to provide testing for CP 24.

The next Aegis variant, Baseline 10, will have an updated system design architecture from the Baseline 9 series and is required for ships with a SPY-6 variant radar, to include DDG 51 Flight III with the SPY-6(V)1 and FFG 62 class guided missile frigate with SPY-6(V)3F. DOT&E approved a TEMP for the combined test programs of DDG 51 Flight III, SPY-6(V)1, and Baseline 10.0 in September 2022. The Navy took delivery of the first DDG 51 Flight III guided missile destroyer with Baseline 10.0, USS *Jack H. Lucas* (DDG 125), in June 2023. The Navy commenced operational assessment of Baseline 10.0 in FY24 and expects to complete in FY28. The Navy is currently developing a TEMP update for the test program of Baseline 10.1.

» MAJOR CONTRACTORS

- Lockheed Martin Rotary and Mission Systems – Bethesda, Maryland
- Raytheon, a subsidiary of RTX – Arlington, Virginia

TEST ADEQUACY

In October 2023, OPTEVFOR conducted operational testing of ACB 16 (Baseline 9.2.0) on USS *Carl M. Levin* (DDG 120). The testing consisted of an integrated air and missile defense event involving Ballistic Missile Defense and Anti-Air Warfare threat surrogate targets and tracking exercises with simulated engagements against a submarine. The test was conducted in conjunction with the Missile Defense Agency Flight Test Aegis Weapon System (FTM)-48 event. In December 2023, OPTEVFOR conducted operational testing of CP 22-1 on USS *Winston S. Churchill* (DDG 81). The testing consisted of tracking exercises with simulated missile engagements against a surface combatant. Both tests were conducted in accordance with DOT&E-approved test plans and with DOT&E observation.

OPTEVFOR plans to complete operational testing of Baselines 9.2.1 and CP 22-1 in FY25 in accordance with a DOT&E-approved test plan.

OPTEVFOR plans to submit a cyber survivability test plan to DOT&E for approval in FY25 and complete cyber survivability testing of CP 22-1 in FY25.

In March 2024, the Missile Defense Agency, in collaboration with OPTEVFOR, conducted FTM-32 as an integrated test to demonstrate the capability to detect, track, engage, and intercept a Medium Range Ballistic Missile target utilizing a simulated Standard Missile (SM-6). FTM-32 was conducted in accordance with a DOT&E-approved test plan and with DOT&E observation. USS *Jack H. Lucas* (DDG 125) equipped with Baseline 10, participated in the flight test as part of its operational assessment. Significant intended data collection on Baseline 10.0 performance were not attained due to SPY-6(V)1 radar system and AWS challenges during test execution. As a result, insufficient data are available to assess Baseline 10.0 operational effectiveness from this flight test. This event is detailed in the classified DOT&E FY24 Missile Defense System Annual Assessment, to be published in FY25.

The Navy is developing a Combat System Test Bed (CSTB) modeling and simulation suite to support the test strategy for Baseline 10.0. The Navy is developing the CSTB in incremental stages that align with planned operational testing within the Baseline 9 series and Baseline 10.0. The Navy expects to verify, validate, and accredit the CSTB for operational assessment of Baseline 10.0 in FY28.

PERFORMANCE

» EFFECTIVENESS

Insufficient data are available to determine AWS ACB 16, the Baseline 9 series, operational effectiveness. DOT&E will publish a classified IOT&E report after the completion of operational testing that the Navy expects to occur in FY25.

The AWS integration with active missiles including ESSM Block 2, SM-2 Block IIIC, and SM-6, which are intended for close-in air warfare self-defense and area-air defense, could enhance weapon system performance against threat ASCMs. Details are available in the DOT&E classified early fielding reports for ESSM Block 2 utilizing Baseline 9.2.1 (September 2022) and SM-2 Block IIIC utilizing Baseline CP 22-1 (March 2024).

Insufficient data are available to determine Baseline 10.0 operational effectiveness. DOT&E will publish a classified IOT&E report after completion of operational testing that the Navy expects to occur in FY28.

» SUITABILITY

Insufficient data are available to determine AWS ACB 16 operational suitability. However, testing continues to demonstrate hardware reliability and software stability concerns with the ADS and the AN/ SPY-1 radar. DOT&E will publish a classified IOT&E report after the completion of operational testing that the Navy expects to occur in FY25.

Insufficient data are available to determine Baseline 10.0 operational suitability. DOT&E will publish a classified IOT&E report after completion of operational testing that the Navy expects to occur in FY28.

» SURVIVABILITY

Insufficient data are available to assess the cyber survivability of AWS ACB 16. DOT&E will publish a classified IOT&E report after the completion of a cyber survivability evaluation that the Navy expects to occur in FY25.

Insufficient data are available to assess cyber survivability of Baseline 10.0. DOT&E will publish a classified IOT&E report after the completion of IOT&E that the Navy expects to occur in FY28.

RECOMMENDATIONS

The Navy should:

1. Continue to update and correct hardware reliability and software stability issues with the ADS and AN/SPY- 1 radar.
2. Complete development, verification, and validation of the CSTB by FY28 to support operational assessment of Baseline 10 and subsequent upgrades to AWS.
3. Schedule and conduct remaining test requirements for the ACB 16 test program, Baseline 9.2.1 and CP 22-1, in FY25.
4. Provide for DOT&E approval in FY25, a CP 22-1 cyber survivability test plan.

5. Provide for DOT&E approval in FY25, an ACB 16 TEMP update for CP-24.
6. Develop and provide for DOT&E approval, a TEMP update for Baseline 10.1 and Baseline 10.0 updates for DDGs being back-fit with SPY-6(V)4.

AIM-9X Block II Sidewinder

In July 2024, DOT&E published a classified AIM-9X Block II Operational Flight Software (OFS) 9.411 Lethality and Cyber Survivability Annex. The AIM-9X Block II Sidewinder is undergoing several updates. FOT&E of OFS 9.5, a software update that includes performance improvements and two new capabilities, is scheduled to begin in 1QFY25. The current test concept for OFS 9.5 does not include sufficient live missile tests to adequately test the two new capabilities. The program office states the limited number of missiles is due to a program resource limitation. The Services have been notified of DOT&E's concern.

FOT&E of a new hardware configuration, OFS 10.4, that re-hosts the current fleet-released version (OFS 9.411) is scheduled to begin in 2QFY25. The current test concept for OFS 10.4 may be adequate to assess the new hardware, pending a configuration review by DOT&E of developmental test (DT)/integrated test (IT) live missile tests. The TEMP and test execution plan for OFS 10.4 still need to be submitted to DOT&E for review and approval.

SYSTEM DESCRIPTION

AIM-9X Block II is the latest-generation, infrared, short-range, air-intercept missile, designed to detect, acquire, intercept, and destroy a wide range of airborne threats. It is day and night capable, uses a passive infrared seeker, and is capable of large attack angles against a wide variety of enemy aircraft. The designated threshold platforms are the F/A-18C/D/E/F and the F-15C/D. Current and future integration efforts also include the F/A-18A/B, E/A-18G, F-15E/EX, F-16C/D, F-22A, F-35A/B/C, MQ-9, AV-8B, AH-1Z, and A-10.

AIM-9X Block II OFS 9.5 is a software update of the currently fielded OFS 9.411. This update is intended to incrementally improve missile performance and provide new capabilities. OFS 10.4 is a rehost of OFS 9.411 on new hardware, which includes new guidance control unit electronics and a new inertial measurement unit. OFS 10.5 will combine OFS 9.5 with the new hardware and will replace the current sapphire missile seeker dome with a new material.

MISSION

AIM-9X Block II is utilized by the U.S. Navy, Marine Corps, and Air Force, as well as several foreign military forces, to execute short-range offensive and defensive air-to-air combat missions. AIM-9X Block II is also a primary element of the Integrated Air and Missile Defense and Theater Air and Missile Defense Family of Systems.

PROGRAM

AIM-9X Block II is an Acquisition Category IC program. It is a joint program led by the Navy's Air-to-Air Missiles Program Office (PMA-259). The Navy's Operational Test and Evaluation Force is the Operational Test Agency for OFS 9.5, 10.4, and 10.5 FOT&E efforts.

DOT&E published a classified AIM-9X Block II OFS 9.410 FOT&E report in September 2021 and a classified AIM-9X Block II OFS 9.411 Lethality and Cyber Survivability Annex in July 2024. The annex was delayed so the Navy could accredit the cyber test asset and the lethality models, completed in October 2023 and July 2024, respectively. OFS 9.410 and the currently fielded OFS 9.411 are functionally the same software with the same capabilities.

The Services are scheduled to start FOT&E for OFS 9.5 in 1QFY25 and OFS 10.4 in 2QFY25.The current test concept for OFS 9.5 does not include sufficient live missile tests to adequately test the two new capabilities provided by this update due to a program resource limitation. The current test concept for OFS 10.4 may be adequate to assess the new hardware, pending a configuration review by DOT&E of DT/IT live missile tests. The TEMP and test plan for OFS 10.4 still need to be submitted to DOT&E for review and approval. The Services are also in the process of test planning for AIM-9X Block II OFS 10.5, with operational testing expected to begin in 2QFY26.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX – Tucson, Arizona

TEST ADEQUACY

The Navy completed FOT&E of the AIM-9X Block II OFS 9.410 in October 2021, in accordance with DOT&E-approved test plans. DOT&E personnel observed the testing. Testing was adequate to assess the operational effectiveness, lethality, suitability, and cyber survivability of the missile.

The availability of threat surrogates for test remains a challenge when assessing missile effectiveness and lethality. OFS 9.5, 10.4, and 10.5 live missile tests may include limited or no full-scale targets due to test asset availability limitations. Additionally, surrogates for many other modern threats do not currently exist. These test asset limitations put greater importance on modeling and simulation to adequately characterize the performance of the AIM-9X Block II. However, verification, validation, and accreditation of modeling and simulation are also negatively affected, due to the lack of relevant flight test data against representative targets. The Services should fund, develop, and produce modern aerial targets such as fourth- and fifth-generation fighter aircraft, large bomber and mobility aircraft, helicopters, and others as discussed in the Test and Evaluation Resources section of this Annual Report.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

DOT&E assessed AIM-9X Block II OFS 9.410 as being operationally effective and suitable in a FOT&E report completed in September 2021. AIM-9X Block II remains on oversight and DOT&E will continue to evaluate operational effectiveness and suitability in upcoming operational testing.

» LETHALITY AND SURVIVABILITY

AIM-9X Block II OFS 9.411 lethality and cyber survivability evaluation details and recommendations are available in the classified DOT&E AIM-9X Block II OFS 9.411 Lethality and Cyber Survivability Annex of July 2024. The report includes one classified recommendation to improve lethality and four to improve cyber survivability.

RECOMMENDATIONS

The Navy should:

1. Adequately test the operational effectiveness and suitability of the two new capabilities delivered in OFS 9.5.
2. Submit configuration data for OFS 10.4 DT/IT live missile tests to DOT&E for review.
3. Submit the TEMP and test plan to support OFS 10.4 operational testing, in accordance with published timelines to DOT&E for approval.
4. Fund, develop, and produce modern aerial targets, such as fourth- and fifth-generation fighter aircraft, large bomber and mobility aircraft, helicopters, and others, as discussed in the Test and Evaluation Resources section of this Annual Report. This shortfall is beyond the scope of the AIM-9X Block II program and must be addressed at the Department of the Navy and Department of the Air Force levels.

Air and Missile Defense Radar (AMDR) / AN/SPY-6

In March 2024, DOT&E published a classified operational assessment (OA) report on the Air and Missile Defense Radar (AMDR), designated AN/SPY-6(V)1. The OA, conducted in FY23 by the Navy's Operational Test and Evaluation Force (OPTEVFOR), provided an early evaluation of the radar's performance and enables modifications that could optimize performance for IOT&E. In addition, the Missile Defense Agency (MDA), in collaboration with OPTEVFOR, conducted the Flight Test Aegis Weapon System-32 (FTM-32) event in FY24 as an integrated test to demonstrate the capability to detect, track, engage, and intercept a medium-range ballistic missile target. Guided-missile destroyer USS *Jack H. Lucas* (DDG 125) participated in the flight test as part of IOT&E for AMDR / AN/SPY-6(V)1, DDG 51 Flight III, and Aegis Weapon System (AWS) Baseline 10.

SYSTEM DESCRIPTION

AN/SPY-6 is the Navy's next-generation, S-Band, family of radars. AN/SPY-6 uses a radar modular assembly (RMA) as a building block for the radar's antenna. Each individual RMA is a self-contained radar antenna built from a set of active transmit/receive (T/R) digital modules that are electronically scanned. Each RMA block can integrate with other RMA blocks to create antenna assemblies of various size and capability. The large number of T/R modules provides a high degree of fault tolerance through antenna redundancy and graceful degradation.

AMDR has two major components:

- An S-band radar to provide search, track, cueing, missile discrimination, S-band missile communications, surveillance capability for ship self-defense and area air defense, and S-band kill assessment support functions.
- A Radar Suite Controller to provide radar resource management and coordination and an open interface with the ship's combat system.

The AMDR fielded on DDG 51 Flight III *Arleigh Burke*-class guided-missile destroyers is designated AN/SPY-6(V)1. AN/SPY-6(V)1 uses four fixed-antenna assemblies (faces) with each antenna having 37 RMAs. This provides a 360-degree field-of-view about the ship. AN/SPY-6(V)1 integrates with AWS to provide DDG 51 Flight III ships with enhanced surveillance, tracking, and ballistic missile defense (BMD) discrimination. AN/SPY-6(V)1 is designed to operate in high clutter, littoral regions near land, and electromagnetic congested, contested, and complex environments.

The AN/SPY-6 family of radars has other variants such as:

- AN/SPY-6(V)2 is comprised of nine RMAs for the single-face rotating antenna intended for the next flights of the *San Antonio*-class and *America*-class amphibious ships and as a back-fit to the *Nimitz*-class aircraft carriers.
- AN/SPY-6(V)3 is comprised of three fixed-antenna faces with nine RMAs on each antenna face, intended for the *Gerald R. Ford*-class aircraft carrier and the *Constellation*-class frigates.
- AN/SPY-6(V)4 is a planned back-fit modernization to the DDG 51 Flight IIA ships that will use 4 fixed-antenna faces, with each antenna face having 24 RMAs.

MISSION

Navy commanders will use AMDR to detect, track, and support engagements against cruise and ballistic missiles, aircraft, and unmanned aerial vehicles in support of air warfare (AW) missions, BMD, or concurrent AW and BMD known as integrated air and missile defense (IAMD). Commanders additionally use AMDR for contact localization and situational awareness in surface warfare missions. AN/SPY-6(V)4 is expected to support similar missions as AN/SPY-6(V)1. AN/SPY-6(V)2 and AN/SPY-6(V)3 will also support similar missions, except for BMD and IAMD, and additionally support air traffic control.

PROGRAM

AN/SPY-6 is an Acquisition Category IC program. The Navy intends to align IOT&E of the different variants of AN/SPY-6 with IOT&E or FOT&E of the ship platforms they are intended for, resulting in an operationally realistic system-of-systems test approach. DOT&E approved a combined TEMP describing the testing strategy for AN/SPY-6(V)1, DDG 51 Flight III ships, and AWS Baseline 10 in September 2022. OPTEVFOR collected ballistic missile defense data on the AN/SPY-6(V)1 in March 2024 in accordance with a DOT&E-approved test plan and with DOT&E observation. Data were collected in conjunction with the OT&E of DDG 51 Flight III with AWS Baseline 10. During FY23 and FY24, the Navy conducted developmental testing of AN/SPY-6(V)1 as installed on USS *Jack H. Lucas* (DDG 125), as well as at the Advanced Radar Detection Laboratory (ARDEL) on Pacific Missile Range Facility (PMRF), in Kekaha, Hawaii, on the island of Kauai. OPTEVFOR is developing an IOT&E test plan and a cyber survivability test plan for combined operational testing of AN/SPY-6(V)1, DDG 51 Flight III, and AWS Baseline 10. The Navy expects to deliver the IOT&E test plan to DOT&E in FY25 and the cyber survivability test plan in FY26.

The Navy expects to deliver a combined TEMP to DOT&E for approval in FY25 that supports T&E of AN/SPY-6(V)2, AN/SPY-6(V)3 for CVN 79, and the Ship Self-Defense System Baseline 12 combat system, which is a delay from last year when it was expected in FY24. The Navy intends to conduct IOT&E of AN/SPY-6(V)2 and AN/SPY-6(V)3 radars between FY26 and FY30.

The Navy expects to deliver a FFG 62 *Constellation*-class guided-missile frigate TEMP to DOT&E for approval in FY25 that supports IOT&E of AN/SPY-6(V)3. The Navy intends to conduct IOT&E of the AN/SPY-6(V)3 radar for FFG 62 ships between FY29 and FY31.

The Navy intends to cover AN/SPY-6(V)4 testing in a future Aegis Modernization TEMP.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX – Marlborough, Massachusetts

TEST ADEQUACY

In March 2024, DOT&E published a classified AMDR / AN/SPY-6(V)1 OA report. OPTEVFOR conducted the OA of AN/SPY-6(V)1 in FY23 at the ARDEL on PMRF, in Kauai, Hawaii, as detailed in the FY23 Annual Report. The OA evaluated capability of AN/SPY-6(V)1 to detect and track fighter aircraft, anti-ship cruise missile surrogates, unmanned aerial vehicles, helicopters, airborne early warning and control aircraft, and small-boat targets. The OA provided early evaluation of the AN/SPY-6(V)1 radar performance in its AW and surface warfare missions in clear and electromagnetic contested environments and demonstrated the Navy's test method for assessing AN/SPY-6(V)1's classified electromagnetic protection waveforms. The OA additionally informed planning of IOT&E test events. The OA was not intended to determine operational effectiveness and suitability of the delivered AMDR due to the AN/SPY-6(V)1 at ARDEL being an engineering development model (EDM) that uses obsolete T/R Integrated Microwave Modules that will not be used by the delivered system. The AMDR Program Office did not evaluate cyber survivability due to differences between the delivered AMDR and the EDM version of AMDR at ARDEL.

In March 2024, the MDA, in collaboration with OPTEVFOR, conducted the Flight Test Aegis Weapon System (FTM-32) as an integrated test to demonstrate the capability to detect, track, engage, and intercept a medium-range ballistic missile target utilizing a simulated Standard Missile-6 (SM-6). USS *Jack H. Lucas* (DDG 125), equipped with AWS Baseline 10 and AN/SPY-6(V)1 radar, participated in FTM-32 as part of IOT&E. Significant intended data collection on AN/SPY-6(V)1 performance was not attained due to system challenges during test execution. As a result, insufficient data are available to assess AMDR operational effectiveness from this flight test. This event is detailed in the classified DOT&E FY24 Missile Defense System Annual Assessment, to be published in February 2025.

As identified in the FY23 Annual Report and the AN/SPY-6(V)1 OA Report, assessment of the resident AN/SPY-6(V)1 at ARDEL was limited by the following:

- AMDR EDM was not operationally representative. The AMDR program plans to install a low-rate initial production (LRIP) AMDR unit in FY26.
- The current aerial anti-ship cruise missile targets do not emulate more stressing threats, including advanced electromagnetic attack capabilities.
- System setup and software configuration of the AMDR EDM could not evaluate performance of all capabilities that are prohibited from testing in an open-air environment due to security reasons. An anechoic chamber would provide the ability to test these capabilities.

PERFORMANCE

» EFFECTIVENESS

The AN/SPY-6(V)1 OA demonstrated radar performance in a limited set of scenarios. DOT&E provided performance results and risks to IOT&E in the classified AN/SPY-6(V)1 OA report in March 2024.

AMDR performance cannot be fully evaluated from the flight test event, FTM-32, due to unavailable data resulting from system challenges during test execution. DOT&E will report on operational effectiveness of AMDR after OT&E completes, currently expected by the Navy to be FY28.

» SUITABILITY AND SURVIVABILITY

No observations on suitability and survivability can be made due to differences in the AMDR EDM used in the OA to the AMDR being delivered to the fleet. The flight test event, FTM-32, identified concerns that could degrade AMDR reliability if not addressed. DOT&E will report on operational suitability and survivability of AMDR after IOT&E that the Navy expects to complete in FY28.

RECOMMENDATIONS

The Navy should:

1. As stated in the FY23 DOT&E Annual Report and the AN/SPY-6(V)1 OA Report, replace the radar system at ARDEL with a production-representative AN/SPY-6(V)1 in FY26 to enable use in integrated and operational test of capabilities.
2. Develop an AN/SPY-6 test environment, such as an anechoic chamber, to effectively assess critical AN/SPY-6 capabilities that are restricted from evaluation in open-air test environments.
3. Evaluate AN/SPY-6(V)1 during large fleet exercises that provide representative complex electromagnetic spectrum environments.
4. Fund development and procure aerial anti-ship cruise missile targets that emulate modern and stressing threats, including advanced electromagnetic attack, to support AMDR IOT&E.
5. Continue to develop and submit the combined AN/SPY-6(V)2, AN/SPY-6(V)3, and the Ship Self-Defense System Baseline 12 Combat System TEMP for DOT&E approval in FY25.

CH-53K® King Stallion®

In May 2024, DOT&E approved a tailored update to the CH-53K TEMP Revision C. DOT&E directed the Navy to develop and route for DOT&E approval a full TEMP revision (Revision D), which should include an update to the LFT&E Strategy, prior to the start of FOT&E events in FY25. The Navy is working on the revision, with an estimated submission for approval in 2QFY25. In FY24, the Navy conducted operational cyber survivability testing of the Digital Interoperability Medium system, and a developmental cyber test assessment of updated aircraft survivability equipment. Data analyses from these tests are ongoing and will be reported in a DOT&E FOT&E report in FY25. FOT&E tests have been delayed in the last two years and are now scheduled for the first half of FY25.

CH-53K® and King Stallion® are registered trademarks of the Department of the Navy.

SYSTEM DESCRIPTION

The CH-53K is a three-engine, dual-piloted, heavy lift helicopter intended to replace the aging CH-53E helicopter. The CH-53K mission payload external load transport is more than twice the CH-53E capability. The triple hook system is designed to transport independent external loads, which allows for three different location drops per sortie. Other major improvements are the replacement of mechanically actuated flight controls with a fly-by-wire system, and a digital interoperability communications system. CH-53K is equipped with aircraft survivability equipment, which consists of the Department of Navy Large Aircraft Infrared Countermeasures system with advanced threat warning sensors, radar warning receiver, and countermeasure dispensing system.

The Marine Corps will support CH-53K Organizational-Level (O-level), Intermediate-Level (I-level), and Depot-Level (D-level) maintenance concepts. The number of personnel per squadron required to maintain the CH-53K is expected to remain the same as for the CH-53E.

CH-53K Secondary Missions Testing

MISSION

Units equipped with the CH-53K aircraft provide the Marine Air-Ground Task Force with assault support to include maritime special operations, by transporting heavy equipment, armored vehicles, combat troops, and supplies from ships to inland locations under all weather conditions. Secondary CH-53K missions include tactical recovery of aircraft and personnel, helicopter air-to-air refueling, air evacuation, aerial delivered ground refueling, forward arming and refueling point operations, air delivery, and rapid insertion and extraction operations.

PROGRAM

The CH-53K is an Acquisition Category IC program. The program of record stipulates the procurement of 200 aircraft. The program completed IOT&E in 3QFY22 in accordance with a DOT&E-approved test plan. DOT&E provided a combined IOT&E and LFT&E report in December 2022, in support of the full-rate production decision, which the Navy approved later that month.

The Navy submitted a tailored update to CH-53K TEMP Revision C for DOT&E approval, to support execution of integrated tests (IT) and the first period of FOT&E events to determine operational effectiveness, suitability, and cyber survivability of the CH-53K configured with Data Transfer Unit and Defensive Electronic Countermeasures System Replacement (DDSR) and Digital Interoperability (DI) Medium communications systems. DOT&E approved this tailored update in May 2024. DOT&E directed the Navy to develop and route for DOT&E approval a full TEMP revision (Revision D) which should include an update to the LFT&E

Strategy. DOT&E stipulated that Revision D should be completed prior to the start of FOT&E events in FY25. TEMP Revision D scope should include the verification of corrections to deficiencies identified in IOT&E that DOT&E addressed in previous reports.

The Navy conducted two IT periods in FY23 to collect data for secondary missions and aircraft survivability equipment, and one IT for DI Medium in 2QFY24. Moreover, the Navy conducted a cooperative vulnerability investigation and adversarial cybersecurity developmental T&E for DDSR, and a cooperative vulnerability and penetration assessment (CVPA) and an adversarial assessment (AA) for DI Medium in FY24. The CVPA and AA were conducted in accordance with a DOT&E-approved operational test plan and observed by DOT&E. The CVPA and AA did not include assessing DDSR in an operationally relevant environment.

Assessment of test data from this FOT&E will inform the CH-53K fleet prior to the first Marine Expeditionary Unit deployment. DOT&E will publish an FOT&E report after testing is complete.

Phase II LFT&E has not yet been resourced, planned, and scheduled. DOT&E has been reporting since FY17 that the Navy has yet to fund the Phase II LFT&E in accordance with the DOT&E-approved TEMP. The DoD Office of Inspector General opened an audit into the Phase II effort in September 2023 and released a report on their findings in November 2024. In June 2024, DOT&E proposed to the CH-53K Program Office a re-scoped Phase II LFT&E, addressing adequate T&E of updated operationally representative threats to complete the survivability assessment. DOT&E has also proposed a new threat working group to evaluate the survivability of the aircraft in the modern, peer-competitor environment expected at deployment plus 10 years. The program office provided feedback on DOT&E's proposal but a new threat working group to evaluate the modern threat environment has not yet been agreed to or convened.

» MAJOR CONTRACTOR

- Sikorsky Aircraft Corporation, a subsidiary of Lockheed Martin Corporation – Stratford, Connecticut

TEST ADEQUACY

Operational cyber survivability testing and IT of the DI Medium system were conducted in FY24, in accordance with DOT&E-approved operational test plans. DOT&E observed the testing. The FOT&E, previously planned for FY24, is now scheduled for FY25 due to delays in test article aircraft modifications. Following the completion of FOT&E, DOT&E will publish an FOT&E report, to include results from the operational cyber survivability testing and IT, in FY25.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Data analyses for the FOT&E completed thus far are ongoing, precluding an assessment of operational effectiveness or

CH-53K helicopter transports an F-35C between test sites in Maryland and New Jersey, April 2024 suitability in this article. DOT&E will publish the results in an FOT&E report, expected in FY25.

» SURVIVABILITY

Data analyses for the cyber survivability testing completed in FY24 are ongoing, precluding an assessment in this article. DOT&E will publish the results in an FOT&E report, expected in FY25.

As noted in the December 2022 combined IOT&E and LFT&E report, the aircraft survivability assessment for CH-53K will not be complete without the data that would be provided on operationally representative threats during Phase II LFT&E.

RECOMMENDATIONS

The Navy should:

1. Continue to address recommendations found in the December 2022 combined IOT&E and LFT&E report, to include the survivability recommendations from the classified annex, as recommended in the FY23 Annual Report.
2. Conduct a CVPA and an AA to characterize DDSR cyber survivability in an operationally relevant environment.
3. Coordinate with DOT&E to develop a new Phase II LFT&E program to assess CH-53K vulnerability against operationally relevant threats, and fully fund that LFT&E program.
4. Establish a threat working group to evaluate the expected threat environment for the first 10 years of deployment and develop an approach with DOT&E to evaluate the survivability of the aircraft in the modern threat environment.
5. Develop and route for DOT&E approval a full TEMP revision (Revision D).

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

The Navy completed a second FOT&E (FOT&E II) in February 2024 focused on the CMV-22B's Communications Upgrade (CU) system. In July 2024, DOT&E published a classified combined FOT&E and LFT&E report that determined the system's operational effectiveness, suitability, and survivability. The CU system is operationally effective using the Iridium SatPhone. Operational suitability for overall aircraft systems is unchanged from previous reporting. Analysis of the CMV-22B survivability to operationally relevant kinetic threats indicated that the aircraft has similar survivability as the legacy platforms and discovered no new nor unexpected vulnerabilities.

SYSTEM DESCRIPTION

The CMV-22B Osprey is a tiltrotor vertical/short takeoff and landing aircraft that can take off and land as a helicopter, and transit as a turboprop aircraft. The CMV-22B is the replacement of the in-service C-2A Greyhound carrier onboard delivery fixed-wing aircraft. The CMV-22B is based on the MV-22B design, with several changes integrated to support the carrier onboard delivery mission: increased fuel capacity to extend the range, fuel jettison system, public address system for making announcements in the cabin area, high-frequency (HF) radio for over-the-horizon communications, and lighting to assist with cargo loading in the cabin and cargo areas.

To meet the required 1,150 nautical mile mission profile, the CMV-22B has increased the fuel capacity by 524 gallons through the expansion of the two forward external sponson tanks, and the addition of two internal inboard wing auxiliary tanks (WATs) located over the aircraft cabin.

The Navy began installing the CU system into the baseline CMV-22B in FY21. The CU is designed to provide operators with communications and situational awareness enhancements when conducting logistics, search and rescue, and mobility missions. The CU system includes Link 16 tactical data link, Iridium satellite phone (Satphone), and TacView smart tablets. Link 16 provides secure communications and a common operational picture for Link 16 network participants by sharing location information. The Iridium Satphone enables over-the-horizon communications and acts as a backup for beyond line-of-sight communications provided by the HF radio. The TacViews are used to visualize the common operating picture and improve situational awareness via a moving map.

MISSION

The Navy will employ units equipped with CMV-22B aircraft to perform the primary mission of transporting personnel, mail, and cargo from forward logistics sites to aircraft carriers at sea. A detachment of three aircraft will support a carrier strike group. The CMV-22B must be capable of conducting operations in all weather conditions, day and night, in a permissive threat environment. Secondary missions include vertical onboard delivery, vertical replenishment, medical evacuation, Naval special warfare support, missions of state, search and rescue support, and self-deployment into the theater of operations.

PROGRAM

The CMV-22B is an Acquisition Category IC program. The Navy has procured all 48 aircraft under the program. DOT&E approved the CMV-22B TEMP and the Alternative LFT&E Plan in March 2020. The Navy declared initial operational capability in 1QFY22 after FOT&E I completed in 4QFY21. DOT&E published a combined FOT&E and LFT&E report with a classified annex in June 2022, detailing CMV-22B performance demonstrated during FOT&E I. DOT&E approved another FOT&E test plan in November 2022 and a cyber survivability test plan in March 2023, to support FOT&E II. DOT&E published a classified

CMV-22B Osprey Flight Operations from USS Carl Vinson (CVN 70), August 2023 combined FOT&E and LFT&E report in July 2024 detailing CMV-22B performance demonstrated. The Navy plans to declare full operational capability in FY25.

» MAJOR CONTRACTOR

- Bell-Boeing Joint Project Office – Amarillo, Texas

TEST ADEQUACY

The Navy completed FOT&E II in 2QFY24. DOT&E observed testing. Testing deviated from the DOT&E-approved test plan but provided sufficient data to assess the operational effectiveness and survivability of the CU system and to reevaluate the operational suitability of the aircraft systems assessed during FOT&E I. The Navy did not conduct the HF radio calls using the CU system, as stipulated in the test plan. Instead, HF call performance data was gathered on non-CU-equipped aircraft as a verification of correction of deficiencies from FOT&E I. The Navy did not complete the maintenance demonstrations for the Link 16 components of the CU system installed on the operational test aircraft because the time to remove and reinstall these components would have negatively impacted the fleet squadron's real-world mission taskings.

A DOT&E-approved known test limitation precluded the evaluation of the CU system suitability. The Navy updated the Link 16 software in the middle of FOT&E II but did not complete in-flight verification testing.

FOT&E II included a verification of correction of deficiencies for a fix to the HF radio, which is on both CU-equipped and non-CU-equipped aircraft.

The Navy conducted a cooperative vulnerability and penetration assessment, and an adversarial assessment of the CU system in 2QFY23 at Naval Air Station Patuxent River, Maryland. Testing was observed by DOT&E and conducted in accordance with the DOT&E-approved test plan and was adequate to assess the survivability of the CU system in a cyber-contested environment.

The Navy previously performed a series of live fire ballistic tests on a full-scale, production representative CMV-22B test article, to evaluate the damage tolerance of the expanded fuel sponson and WATs when impacted by threat projectiles at the Naval Air Warfare Center – Weapons Division China Lake, California, in FY19. During FY24, the Navy completed the system-level vulnerability and personnel protection assessments, and structural analyses to determine the post-damage residual capability of the aircraft in accordance with the DOT&E-approved test plan.

PERFORMANCE

» EFFECTIVENESS

FOT&E II proved units equipped with the CU-installed CMV-22B aircraft are operationally effective using the Iridium Satphone, which demonstrated a high success rate of two-way communications and high voice quality during calls. The Navy implemented Link 16 software corrections during FOT&E II; verification of the software update will be required in a future FOT&E period. HF radio performance on CU-equipped aircraft cannot be assessed with statistical confidence due to the limited number of test points executed. On non-CU-equipped aircraft, HF radios were effective for unencrypted calls, but significantly lower performance was observed for encrypted calls.

Additional details on the operational effectiveness are included in the classified July 2024 report.

» SUITABILITY

The overall aircraft operational suitability assessed during FOT&E II is consistent with the previous assessment from DOT&E's June 2022 report on FOT&E I and discussed in the FY23 Annual Report. Not all metrics could be assessed due to the limited number of test hours executed in FOT&E II.

Assessment of the CMV-22B containerized flight training device and virtual maintenance trainer was deferred from FOT&E I to FOT&E II. The containerized flight training device was usable, but future versions require the incorporation of CU capability and the associated collection of operational test data. The virtual maintenance trainer was usable. Additional operational test data is required, however, to assess the incorporation of new maintenance steps that were implemented after FOT&E II ended.

Additional details on the operational suitability are included in the classified July 2024 report.

» SURVIVABILITY

FOT&E II demonstrated structural damage to the expanded fuel sponson and self-sealing of the WAT fuel bladders is similar to that of the legacy MV/CV-22 variants. Navy testing did not uncover any new failure mechanisms. System-level survivability and personnel protection analyses were also similar to the MV/CV-22. Due to material obsolescence issues, the Navy is working to qualify a new material supplier for V-22 fuel bladders. When that effort is completed, additional ballistic testing will be necessary to ensure continued survivability.

Additional details on system survivability, including cyber survivability of the CU system are included in the classified July 2024 report.

RECOMMENDATIONS

The Navy should:

1. Conduct additional CU testing on operational networks in a future FOT&E period to verify deficiencies are corrected.
2. Conduct additional HF radio testing on CU-equipped CMV-22B aircraft in a future FOT&E period.
3. Include CU capability in the future versions of the training systems and collect suitability data in a future FOT&E period.
4. Continue to implement recommendations in the combined FOT&E and LFT&E report from June 2022, as recommended in the FY23 Annual Report, and implement recommendations from the July 2024 report.

Columbia-Class Submarine

In FY24, the Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted integrated testing for early assessment of the Strategic Weapon System (SWS), used on the *Columbia*-class to launch TRIDENT II D5 missiles at a shore-based test facility. The *Columbia*-class submarine program also continued cyber security evaluations of submarine sonar, combat, and Hull Mechanical and Electrical systems as part of a strategy to maximize resilience of the delivered *Columbia*-class to cyber-attack. The Navy plans to conduct an operational assessment of the *Columbia*-class design and its systems between FY25 and FY26.

SYSTEM DESCRIPTION

The *Columbia*-class replaces the *Ohio*-class fleet ballistic missile submarine (SSBN). *Columbia*-class design is intended to:

- Improve survivability over the legacy *Ohio*-class.
- Maximize availability and not require mid-life refueling, which will allow a fleet of 12 submarines to maintain the same at-sea presence as a fleet of 14 legacy submarines.
- Host the existing TRIDENT II D5 Life Extension (LE) and second variant LE Strategic Weapon System (SWS). The SWS provides missile launch capability and includes fire control, navigation, and support systems.
- Use existing and recapitalized *Ohio*-class basing, maintenance, and training infrastructure. The Navy is leveraging many ship components, such as communications, sonar, tactical control system, and internal computer networks, from other submarine classes to reduce cost and risk.
- Support a mixed-gender crew.
- Support a 42-year service life.

MISSION

The Commander, U.S. Strategic Command (USSTRATCOM) will employ *Columbia*-class submarines as the survivable leg of the U.S. nuclear triad, providing an effective Sea Based Strategic Deterrence (SBSD) model. SBSD is the foundation of our national defense, providing 70 percent of the nation's deployable nuclear warheads.

PROGRAM

The *Columbia*-class submarine program is an Acquisition Category 1D Major Defense Acquisition program. The Navy will procure 12 *Columbia*-class submarines to support USSTRATCOM requirements. The Navy intends the first delivery, the future USS *District of Columbia* (SSBN 826), to conduct its first Strategic Patrol in FY30.

DOT&E approved an update to the *Columbia*-class TEMP and an update to the *Columbia*-class LFT&E Management Plan in June 2023. The Navy plans to submit a test plan for an operational assessment of the *Columbia*-class design and its systems to DOT&E for approval in FY25 and conduct the assessment between FY25 and FY26.

» MAJOR CONTRACTORS

- General Dynamics Electric Boat (GDEB) – Groton, Connecticut
- Newport News Shipbuilding, a division of HII – Newport News, Virginia

TEST ADEQUACY

In FY24, the *Columbia*-class submarine program continued cyber security evaluation and improvement efforts with the *Virginia*-class submarine program. The Navy's strategy is to maximize the cyber survivability of the delivered *Columbia*-class and Block V variant of the *Virginia*-class through participation in the continued development of the AN/BQQ-10 submarine sonar system, Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI), and AN/BYG-1 submarine combat systems that get updated about every two years. DOT&E observes these, and other, system-level evaluations to support planning of future *Columbia*-class cyber survivability evaluations and to identify data that can be used for, and to focus, these assessments.

Between March and September 2024, OPTEVFOR conducted integrated testing of the SWS, which is developmental testing intended to support operational test objectives, at the Strategic Weapon System Ashore (SWSA) facility located at Naval Ordnance Test Unit, Cape Canaveral Space Force Station, Florida. Testing was in accordance with the DOT&E-approved data collection plan and included DOT&E observation. The program and OPTEVFOR exercised offload/onload of a surrogate TRIDENT II D5LE missile, demonstration of a tactically representative launch countdown, and demonstration of fleet maintenance actions on

Columbia-class tactical hardware installed at the SWSA facility.

In FY24, the *Columbia*-class LFT&E program focused on analysis and model validation using surrogate and component testing conducted in FY16-22. The program office continued to work with DOT&E on determination of equipment failure thresholds and personnel injury model techniques for incorporation into the analysis of simulated threat weapon attacks. When completed, the survivability assessment of the submarine, using validated modeling and simulation, will enable assessment of the submarine's vulnerability to threat weapons. The *Columbia*-class Total Ship Survivability Trial (TSST) is scheduled for FY29 and Survivability Assessment Report (SAR) II will be provided in FY26 and SAR III in FY29.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Insufficient data are available to determine the operational effectiveness, suitability, and survivability of the *Columbia*-class. DOT&E will report on the current platform design and its systems after completion of the operational assessment that the Navy expects to occur in FY26. DOT&E will report on operational effectiveness and suitability after completion of IOT&E, which the Navy expects to occur in FY29. DOT&E expects to report on the survivability of the *Columbia*-class upon completion of TSST in FY29 and completion of the final SAR, SAR III, which the Navy expects to provide in FY29.

RECOMMENDATIONS

None.

Conventional Prompt Strike (CPS)

In 3QFY24, the Conventional Prompt Strike (CPS) program conducted an end-to-end flight test of the prototype CPS All-Up Round (AUR). The CPS program and Army's Long Range Hypersonic Weapon (LRHW) – Dark Eagle program intended an additional CPS AUR test flight from the Army's transporter-erector-launcher (TEL) in 4QFY24 but did not execute the flight test due to a system problem. The CPS program expects to conduct demonstrations of the CPS AUR from the Army's TEL and the Navy's ship/submarine-launch canister in FY25.

SYSTEM DESCRIPTION

CPS is a conventional, boost-glide hypersonic weapon system. The CPS AUR missile includes a two-stage solid rocket motor booster and a Common Hypersonic Glide Body containing a kinetic energy projectile warhead. The Navy will integrate CPS into both *Zumwalt*-class destroyers and *Virginia*-class submarines. The Navy will utilize cold-gas ejection ("cold launch") to launch the AUR from both platforms. The Army LRHW system, which is being reported on in a separate article, will fire a common AUR from their TEL, igniting it in the launch canister ("hot launch").

MISSION

U.S. combatant commanders will launch CPS from *Zumwalt*-class destroyers and *Virginia*-class submarines to penetrate air defenses to strike high-value, time-sensitive targets.

PROGRAM

The Navy is employing a three-phase acquisition strategy to deliver CPS. Phase 1 is a Middle Tier of Acquisition (MTA) rapid prototyping effort to develop and demonstrate a prototype hypersonic missile system capability through a four-flight test campaign ending in FY25. Phase 2 is an MTA rapid fielding effort that includes a flight test from a *Zumwalt*-class destroyer and is intended to field CPS on the first *Zumwalt*-class destroyer in FY27. Phase 3 is a Major Defense Acquisition program that the Navy intends to field CPS aboard the remaining two *Zumwalt*-class destroyers and aboard *Virginia*-class submarines. The program office approved an initial Life Cycle Sustainment Plan in July 2024 to address product support and fielding aboard both the *Zumwalt*-class destroyers and the *Virginia*-class submarines.

DOT&E conditionally approved the Navy's Master Test Strategy (MTS) for the CPS MTA rapid prototyping program in March 2023, provided the CPS Program Office submits the combined Phase 2 and Phase 3 TEMP and the LFT&E Strategy in 2023. Changes in CPS development objectives and delivery schedule delayed submittal of these T&E documents through FY24. The Navy is working with DOT&E to resolve DOT&E concerns with their test strategy in the combined Phase 2 and Phase 3 TEMP and the LFT&E Strategy and expects to deliver them for DOT&E approval in early FY25.The CPS Program Office expects to submit test plans for DOT&E approval in FY25 to conduct a demonstration of the CPS AUR from the Army's TEL and an Operational Demonstration (Ops Demo) from the Navy's ship/submarine-launch canister.

In April 2024, the Navy issued a memorandum that changed the CPS rapid prototyping test program to complete on the fourth flight test instead of a fifth flight test due to a change in program objectives. DOT&E acknowledged this change, noting concern for the limited opportunity to identify and make CPS improvements prior to its fielding.

In FY24, the LRHW – Dark Eagle program continued development of a prototype LRHW Battery Operations Center and TEL system. Details of these efforts, and integration of the AUR missile and weapons control system, are reported in the LRHW – Dark Eagle article of this Annual Report.

» MAJOR CONTRACTORS

- Lockheed Martin Space – Littleton, Colorado
- Dynetics, a subsidiary of Leidos – Huntsville, Alabama (Common Hypersonic Glide Body)

TEST ADEQUACY

In 3QFY24, the CPS program conducted an end-to-end developmental flight test of the prototype CPS AUR from the Pacific Missile Range Facility in Kauai, Hawaii. The Navy's Operational Test and Evaluation Force developed a data collection plan and DOT&E observed this event for potential use of collected data in operational assessment. This test did not utilize a Navy- or Army-representative launcher. In 4QFY24, the CPS program and the LRHW – Dark Eagle program attempted a fourth CPS flight test using the Army's TEL. This test did not occur due to a system problem that the CPS program office identifies as now corrected. In FY25, the CPS program and the LRHW – Dark Eagle program expect to demonstrate launch capability from a TEL in a third CPS missile flight test and launch capability from a representative launch canister of the *Zumwalt*-class destroyers and *Virginia*-class submarines in a fourth CPS missile flight test.

The Navy conducted a warhead arena test in 1QFY24 and a sled test in 2QFY24. As noted in the FY22 and FY23 Annual Reports, the initial CPS sled and flight tests did not include operationally representative targets and consequently did not provide direct validation of the weapon's lethal effects. The Navy included some threat-representative targets in the recent sled test. The Navy is further investigating methods to obtain lethality and effectiveness data by incorporating representative targets into the CPS flight tests. The Navy expects to provide an LFT&E Strategy for DOT&E approval in FY25.

In FY24, the Navy completed its 10th cyber survivability evaluation of the CPS AUR missile design and its supporting combat system as developmental test to identify the attack surface and potential vulnerabilities. These events will inform cyber vulnerability risk of the Phase 1 CPS prototype but are not a comprehensive evaluation of the vulnerabilities of the delivered prototype or mission effects. Cyber survivability evaluations are planned for both *Zumwalt*-class destroyers and *Virginia*-class submarines in Phases 2 and 3; CPS will require comprehensive evaluation prior to fleet deployment with the system installed.

The Navy has only evaluated to a limited extent the effect of a contested environment on CPS AUR missile performance. The Navy plans to use a combination of modeling and simulation (M&S), component testing, and hardware-in-the-loop evaluations to assess CPS performance in the contested environment. The full M&S federation is expected to be complete and provide results at the end of the IOT&E period. Adequate testing in the full-spectrum contested environment is required, however, to determine CPS effectiveness under combat conditions.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, AND SUITABILITY

Insufficient data are available to assess operational effectiveness, lethality, and suitability of the Phase 1 CPS prototype. DOT&E will provide assessment of CPS prototype effectiveness, lethality, and suitability after the Ops Demo that the CPS Program Office expects to occur in FY25.

» SURVIVABILITY

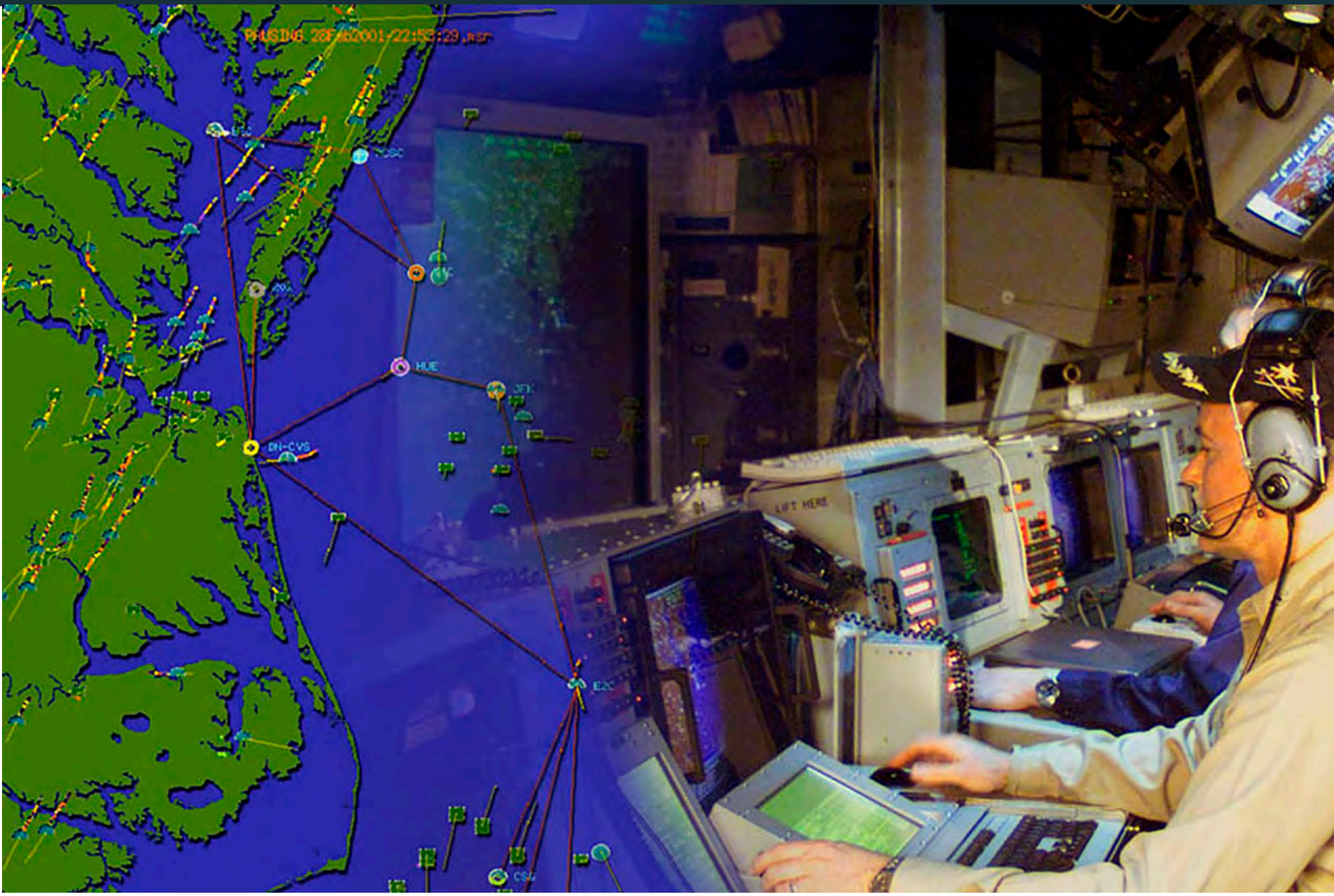
Analysis of the Phase 1 CPS cyber survivability is in progress. DOT&E will report assessment of the CPS prototype cyber survivability after completion of the Ops Demo that the CPS program expects to occur in FY25.

RECOMMENDATIONS

The Navy should:

1. Submit the combined CPS Phase 2 and Phase 3 TEMP for DOT&E approval in early FY25, to support the determination of operational effectiveness, suitability, and survivability of CPS through those phases. Ensure that the combined CPS Phase 2 and Phase 3 TEMP incorporates the full-spectrum contested environment.
2. Submit a CPS LFT&E Strategy, in conjunction with the combined Phase 2 and Phase 3 TEMP, for DOT&E approval in early FY25, to support the determination of lethality of the CPS AUR against threat-representative targets. This effort should be coordinated with the Joint Technical Coordinating Group for Munitions Effectiveness, to include data required to validate the CPS weaponeering tools for operational use.

Cooperative Engagement Capability (CEC)



In December 2023, the Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted FOT&E of the Cooperative Engagement Capability (CEC) as integrated on the DDG 1000 *Zumwalt*-class destroyers. In March 2024, OPTEVFOR conducted cyber survivability evaluation of CEC as integrated on CVN 78 *Gerald R. Ford*-class nuclear aircraft carrier. The Navy expects to complete FOT&E on these two variants of CEC in FY25. OPTEVFOR conducted no operational test on CEC as integrated on Aegis-equipped ships and expects to complete FOT&E of this variant in FY26.

SYSTEM DESCRIPTION

CEC is a real-time sensor fusion and netting system intended to enhance the situational awareness of equipped units and provide integrated fire control capability. CEC is comprised of a Cooperative Engagement Processor (CEP) and Data Distribution System (DDS). The CEP fuses data from the organic sensors of the employing platform/unit with data from remote sensors of other platforms/units within the network to construct target tracks. CEC integrates with the employing platform/unit combat systems to display these tracks and provide target track data the host combat system can use for target engagement. The DDS exchanges sensor data (e.g., radar and identification, friend or foe (IFF) measurements) between CEC-equipped platforms/units within line-of-sight.

CEC uniquely integrates the sensors and combat system of the host platform/unit. U.S. variants of CEC have three numeric designators. The "B" designator represents a capability upgrade that occurred within the legacy CEC program.

- AN/USG-2/2B for Navy surface ships
- AN/USG-3/3B for Navy E-2C Hawkeye 2000 and E-2D Advanced Hawkeye
- AN/USG-4B for U.S. Marine Corps Composite Tracking Network units

AN/USG-2B has variations due to distinct differences in Navy surface ship combat systems. These variations include the *Gerald R. Ford*-class with the Ship Self-Defense System, the *Zumwalt*-class with the Total Ship Computing Environment Infrastructure, and Aegis Advanced Capability Build (ACB) 16-equipped ships.

CEC Increment II will provide updates to both hardware and software from the legacy CEC and is intended to provide advanced capabilities and address more stressing threats. The Navy intends a phased delivery of CEC Increment II, with the first phase designated as CEC Block II.

MISSION

Navy commanders use units equipped with CEC to improve battle force air and missile defense capability by combining participating units' sensor data into a single, real-time, composite track picture. Combining data increases units' situational awareness, improves air picture quality, expands the battlespace, increases depth-of-fire, and enables integrated fire control. On aircraft carriers and select amphibious ships, CEC provides accurate air and surface tracking data for the Ship Self-Defense System combat system.

CEC Increment II is intended to expand the use of CEC to support surface warfare and electronic warfare and to support larger numbers of CEC participant platforms in the DDS network.

PROGRAM

CEC is an Acquisition Category IC program that achieved full operational capability in 2005. The draft CEC TEMP 1415 Revision 6 Change 1, dated April 2022, provides the test strategy for CEC as integrated with *Gerald R. Ford*-class and *Zumwalt*-class ships, Aegis ACB 16-equipped ships, and E-2Ds. DOT&E did not approve TEMP 1415 Revision 6 Change 1 due to inconsistencies between the TEMP and the resources required to execute the documented test strategy. DOT&E will continue to review and approve, as appropriate, related operational test plans to complete the legacy CEC test program. DOT&E approval of the *Zumwalt*-class IOT&E test plan in January 2024 supported operational test of the AN/USG-2B *Zumwalt*-class variant in FY24. DOT&E approval of the *Gerald R. Ford*-class cyber survivability test plan in February 2024 supported cyber security evaluation of the AN/USG-2B *Gerald R. Ford*-class variant in FY24.

CEC Increment II is a separate Acquisition Category II program from the legacy CEC program. In FY24, the Navy began development of the TEMP for CEC Block II, the first phase of CEC Increment II.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX – Arlington, Virginia

TEST ADEQUACY

In December 2023, OPTEVFOR conducted FOT&E of the AN/USG-2B *Zumwalt*-class variant, in conjunction with the *Zumwalt*-class IOT&E. Testing was conducted in accordance with a DOT&E-approved test plan and was observed by DOT&E. However, a supporting CEC unit experienced equipment failure and could not participate in the test. As a result, testing did not achieve a primary objective to evaluate CEC data distribution capabilities. The Navy intends to collect on CEC data distribution during USS *Michael Monsoor* (DDG 1001) pre-deployment workup and conclude evaluation of the AN/USG-2B *Zumwalt*-class variant in FY25. OPTEVFOR completed cyber survivability evaluation of AN/USG-2B *Zumwalt*-class variant in FY24.

Between February and March 2024, OPTEVFOR conducted cyber survivability testing of the AN/USG-2B *Gerald R. Ford*-class variant aboard USS *Gerald R. Ford* (CVN 78), in accordance with a DOT&E-approved test plan and with DOT&E observation. The test occurred with CVN 78 pierside and was informed by the land-based test site evaluation detailed in the FY23 Annual Report. OPTEVFOR intends to complete cyber survivability testing of the AN/USG-2B *Gerald R. Ford*-class variant from the CVN 78 when it is underway in FY25. OPTEVFOR intends to conclude FOT&E of the AN/USG-2B *Gerald R. Ford*-class variant in FY25, in conjunction with the platform's remaining IOT&E that includes operationally relevant scenarios for CEC employment.

OPTEVFOR conducted no evaluation of the AN/USG-2B Aegis variant in FY24. The Navy intends to complete FOT&E of this variant of legacy CEC in conjunction with Aegis ACB 16 operational testing on a guided missile cruiser in FY26.

In FY24, the Navy took no action on DOT&E's recommendation in the FY20 Annual Report to conduct testing on the AN/USG-3B variant of CEC as employed by E-2D.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Insufficient data are available to determine the operational effectiveness and suitability of the AN/USG-2B *Zumwalt*-class, *Gerald R. Ford*-class, or Aegis variants. DOT&E will submit FOT&E reports, or a combined report, for the AN/USG-2B *Zumwalt*-class and *Gerald R. Ford*-class variants after completion of their respective FOT&Es that the Navy expects to occur in FY25. DOT&E will submit an FOT&E report for the AN/USG-2B Aegis variant after completion of FOT&E that the Navy expects to occur in FY26.

» SURVIVABILITY

Cyber survivability assessment of the AN/USG-2B *Zumwalt*-class variant is classified. DOT&E will submit an FOT&E report for the AN/USG-2B *Zumwalt*-class variant after completion of FOT&E that the Navy expects to occur in FY25.

Insufficient data are available to determine the cyber survivability of the AN/USG-2B *Gerald R. Ford*-class and Aegis variants. DOT&E will submit FOT&E reports for the AN/USG-2B *Gerald R. Ford*-class and Aegis variants after completion of their FOT&Es that the Navy expects to occur in FY25 and FY26, respectively.

RECOMMENDATIONS

The Navy should:

1. Complete FOT&E on the AN/USG-2B *Zumwalt*-class and *Gerald R. Ford*-class variants in FY25, and the AN/USG-2B Aegis variant in FY26, as recommended in the FY23 Annual Report.
2. Provide a CEC Increment II Block II TEMP for DOT&E's approval in FY25, as recommended in the FY23 Annual Report.
3. Address the recommendations from the FY20 and FY23 Annual Reports that pertain to the AN/USG-3B variant of CEC on E2D.
4. Ensure that cyber survivability evaluations on Aegis ACB 16 platforms comprehensively assess CEC.

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

In FY24, USS *Gerald R. Ford* (CVN 78) completed a 262-day deployment, returning to home port in January 2024. While deployed, CVN 78 and its embarked air wing executed operational missions in support of combatant commander requirements. After its return to home port, the ship entered its post-deployment maintenance availability, and in March 2024, the Navy completed pierside cyber survivability testing, an operational test event. CVN 78 will resume IOT&E in FY25 with sortie generation rate (SGR), Ship Self-Defense System (SSDS), and Total Ship's Survivability Trial (TSST) testing. These tests will be critical to evaluating the ship's effectiveness and survivability, along with accrediting high-fidelity flight operations and Probability of Raid Annihilation (P_{RA}) models, which are essential for evaluating platform performance requirements.

SYSTEM DESCRIPTION

The *Ford*-class is a new class of nuclear-powered aircraft carriers based on the *Nimitz*-class hull, with significant design changes intended to enhance the *Ford*-class's ability to launch, recover, and service aircraft while reducing required manning capacity by approximately 15 percent. CVN 78 includes a new nuclear power plant that increases electrical capacity to power ship systems, including new Electromagnetic Aircraft Launch System (EMALS) catapults and electromechanical Advanced Arresting Gear (AAG). The originally planned arresting gear engine and wire positioning (consisting of four engines and three wires) was similar to the USS *Ronald Reagan* (CVN 76) and USS *George H. W. Bush* (CVN 77) flight decks. However, the fourth AAG engine has not been installed on the *Ford*-class to date as a cost savings measure. The *Ford*-class also incorporates a larger and more efficient flight deck layout with additional aircraft fueling stations, along with redesigned weapons elevators, weapons handling spaces, and magazine stowage to reduce manning, improve safety, and increase weapons throughput compared to *Nimitz*-class aircraft carriers. The *Ford*-class combat system incorporates the following systems:

- Dual Band Radar (DBR) that combines the phased-array SPY-4 Volume Search Radar and the SPY-3 Multi-Function Radar. CVN 78 is the only ship with DBR; it will eventually be replaced with the SPY-6(V)3 Enterprise Air Surveillance Radar (EASR) fixed variant, the SPQ-9B horizon search radar, and Mk 9 Tracker Illuminator System, as will be installed on PCU *John F. Kennedy* (CVN 79) and follow-on carriers.
- SSDS Mk 2 Mod 6 with Baseline 10 combat management system, which will be upgraded to the new capability build, Baseline 12, on CVN 79 and follow-on *Ford*-class ships.
- AN/USG-2B Cooperative Engagement Capability (CEC) tracking, data fusion, and distribution system, which will be upgraded to CEC Block II and follow-on *Ford*-class ships.
- AN/SLQ-32B(V)6 electronic warfare system equipped with the Surface Electronic Warfare Improvement Program (SEWIP) Block 2.
- Rolling Airframe Missile (RAM) Block 2 and Evolved Sea Sparrow Missile (ESSM) Block 1. CVN 79 and beyond will be upgraded to a mix of new RAM variants Block 2A and 2B, plus a mix of ESSM Block 1 and Block 2.
- The Close-In Weapon System search radar, which operates in stand-alone mode on CVN 78, but will be integrated with AN/USG-2B CEC and SSDS on follow-on *Ford*-class ships.

Ford-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.

MISSION

Carrier strike group (CSG) commanders will use *Ford*-class ships to:

- Provide credible, sustainable, independent forward presence during peacetime without access to land bases;
- Operate in a supported or supporting role with a joint and/or allied maritime expeditionary force in response to crises; and
- Carry the war to the enemy, independent of forward-based land facilities, through joint multi-mission offensive operations by:
  - Operating and supporting aircraft to attack enemy forces ashore, afloat, or submerged;
  - Protecting friendly forces from enemy attack through the establishment and maintenance of battlespace control; and
  - Engaging in sustained operations in support of the United States and its allies.

PROGRAM

The CVN 78 *Gerald R. Ford*-class is an Acquisition Category IC program. DOT&E approved Revision E of the TEMP in September 2022 and Revision B of the LFT&E Management Plan in September 2023. The first ship in the *Ford*-class, CVN 78, was delivered to the Navy in 2017. It completed Post Delivery Test and Trials in April 2021 to demonstrate the basic functionality of the carrier, certify the flight deck, and embark an air wing. CVN 78 also completed Full Ship Shock Trials (FSST) in August 2021 and a Planned Incremental Availability in February 2022. DOT&E approved the first of two planned phases of the IOT&E test plan, and IOT&E began in September 2022. IOT&E is expected to complete in FY27.

The Navy deployed CVN 78 in May 2023, which was earlier than the scheduled timeline for first deployment in TEMP Revision E. In preparation for the first deployment, CVN 78 completed its first Composite Training Unit Exercise (COMPTUEX) in April 2023. DOT&E approved Revision 1 to the IOT&E test plan in March 2023 to include IOT&E data collection opportunities during the COMPTUEX. The Navy's operational requirements necessitated changing CVN 78's original test plan timeline around the operational deployment, and in July 2024, the Navy delivered to DOT&E a revised test plan which replaced the IOT&E original two-phase structure with a more incremental approach. DOT&E approved an imminent test event within that test plan revision, but withheld full test plan approval due to an insufficiently articulated reliability, maintainability, logistics, and availability (RMLA) data collection strategy. The Navy should submit to DOT&E a test plan revision that contains an improved RMLA data collection strategy.

CVN 79 delivery is scheduled for late FY25. CVN 79 will be capable of supporting F-35 operations at delivery. *Enterprise* (CVN 80) construction began in August 2017 and is expected for delivery to the Navy in FY29, 18 months later than reported in the FY23 Annual Report. This delay is due to complications with material availability and industry/supply chain performance. *Doris Miller* (CVN 81) construction began in August 2021 and is expected for delivery to the Navy in FY32. The most significant changes to CVN 79 and beyond are related to the combat system and design changes to support F-35. The Navy is updating the TEMP to include operational testing of the *Ford*-class's capability to support F-35 and CMV-22, along with the self-defense capabilities of CVN 79 and follow-on carriers. The Navy expects to update the TEMP in FY25 before CVN 79 is delivered.

» MAJOR CONTRACTOR

- Newport News Shipbuilding, a division of HII – Newport News, Virginia

TEST ADEQUACY

The Navy began *Ford*-class IOT&E in September 2022 and is conducting it in accordance with TEMP Revision E and the DOT&E-approved portions of the IOT&E test plan Update 1. However, the RMLA data collection gaps identified in the FY23 Annual Report remain. If not rectified, these gaps could result in insufficient data to inform conclusive assessments of RMLA for some key subsystems. In addition to affecting suitability assessments, these data gaps could also affect effectiveness assessments, due to the on-demand nature of many key subsystems and the reliance upon accurate RMLA data in both the self-defense and SGR models.

In FY24, the Navy improved data collection for EMALS reliability and is actively working to improve data collection for AAG reliability. The Navy has not yet shown progress for data collection on the other shipboard systems, but has implemented procedural changes designed to improve data collection within shipboard work centers in support of the FY25 scheduled test events. The Navy will continue to update the IOT&E test plan for the major remaining tests such as SGR, self-defense, and cyber survivability tests.

In March 2024, the Navy conducted pierside shipboard cyber survivability tests to assess *Ford*-class overall cyber survivability and enable post hoc accreditation of the test facilities used in completed land-based cyber survivability testing of EMALS and AAG. This included some testing of the ship's industrial control systems.

Between February and March 2024, the Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted cyber survivability testing aboard CVN 78, in accordance with a DOT&E-approved test plan and with DOT&E observation. The test occurred with CVN 78 pierside and was informed by the land-based test site evaluation detailed in the FY23 Annual Report. The CVN 78 cyber survivability test supported evaluations of the CVN 78 variations of the following programs of record: the SSDS integrated combat system, CEC, and SEWIP. OPTEVFOR will use final analysis of the pierside cyber test of CVN 78 in the planning of the remaining cyber survivability testing with CVN 78 underway; the Navy expects to complete this remaining cyber survivability testing in FY25.

In FY24, the Navy published two vulnerability assessment reports examining the *Ford*-class survivability against above-water and underwater kinetic threats. These reports were based on survivability testing and ship modeling. However, the Navy's ship models require updating to incorporate changes to the as-built *Ford*-class from original design, so their use for survivability assessment is limited. The Navy intends to issue a final survivability assessment report that will include the findings from testing conducted since 2020 and update model-based survivability analysis by 4QFY25. The updated ship models are necessary to support DOT&E's report on the survivability of the *Ford*-class against threat weapons. DOT&E has requested the Navy provide a roadmap for *Ford*-class ship model updates that will support representative survivability assessments.

Evaluation of the *Ford*-class's anti-air warfare capability is coordinated between the CVN 78 TEMP Revision E and the Capstone Enterprise Air Warfare Ship Self-Defense (AW SSD) TEMP 1714 of March 2008. The evaluation includes a series of live missile fire events aboard CVN 78 against a variety of anti-ship cruise missile (ASCM) threat surrogates. In April 2024, DOT&E approved a modified test strategy for these missile fire events that incorporates refined fleet-representative defensive employment tactics against threat ASCMs. Unplanned post-deployment maintenance requirements for various ship systems will delay these tests until early FY25. These tests will demonstrate *Ford*-class ship self-defense capability and are required to validate modeling and simulation (M&S) used to predict CVN 78 performance across the spectrum of threat ASCMs.

The *Ford*-class SGR evaluation is composed of M&S (for both *Ford*- and *Nimitz*-class), a four-day sustained test on CVN 78, a one-day surge test on CVN 78, and observation of flight operations on a *Nimitz*-class carrier. Development of the M&S suite intended to evaluate the SGR, the Sea Strike/Sea Basing Aviation Model (SSAM), is ongoing. The *Ford*-class sustained SGR test is scheduled to occur in late FY25. The Navy plans to apply lessons from the sustained SGR test to the surge SGR test, which is currently unscheduled. DOT&E approved these deferments in Revision 1 to the IOT&E test plan, and the Navy needs to provide an updated test plan for DOT&E approval, prior to conducting these events.

In FY24, the Navy collected flight operations data during the USS *Harry S. Truman* (CVN 75) COMPTUEX to support a *Nimitz*-class SGR M&S suite (part of SSAM) for comparative analysis. The Navy and DOT&E are dependent on SSAM for SGR key performance parameter (KPP) evaluation. However, limited test data places the validation of SSAM at risk, and the two SGR demonstrations are the only planned opportunities to collect high-tempo validation data in a requirement-representative scenario. The Navy can mitigate this risk by adequately resourcing the two SGR demonstrations, maximizing data collection during these events, and characterizing model performance to focus on the most critical live data needs.

The Navy remains in development of an enterprise test strategy that will coordinate ship self-defense evaluation of multiple ship classes, including the *Ford*-class, as modified in CVN 79 and follow-on carriers. The new enterprise test strategy for the CVN 79 and follow-on ships will be coordinated between the CVN

78 TEMP Revision F and the yet-to-be-approved Enterprise TEMP 1910. CVN 79 includes an updated combat system, SSDS Baseline 12, and the new SPY-6(V)3 radar system. The details of this enterprise approach are in the SSDS article of this Annual Report. The Navy has yet to finalize the replacement self-defense test capability for ship self-defense against threat ASCMs following the deactivation of the current self-defense test ship, ex-USS *Paul F. Foster*, expected in FY30. To avoid delays in determining *Ford*-class capability and survivability, the Navy should finalize enduring test capabilities, similar to those provided by ex-USS *Paul F. Foster*, in FY25.

PERFORMANCE

» EFFECTIVENESS

Insufficient data are available to determine the *Ford*-class's operational effectiveness due to IOT&E being incomplete. Observations based on testing to date are below.

Combat System

Self-defense testing against unmanned aerial vehicles and high-speed maneuvering surface targets (small boats) was conducted in July 2022. Details can be found in DOT&E's classified early fielding report (EFR) dated April 2023. The Navy is developing fixes to combat system deficiencies identified in DOT&E's classified interim assessment report dated April 2022. However, the fixes remain largely unfunded to date.

SGR

During USS *Gerald R. Ford*'s FY24 deployment, the ship and its embarked air wing maintained sortie generation rates that were sufficient to meet combatant commander operational taskings. Although the sortie generation rates sustained during particular evolutions, such as Carrier Qualification, have numerically approached those required by the KPP, the aircraft configuration and tempo of these operations did not match the Design Reference Mission and were therefore not representative of the KPP requirement. The reliability and maintainability of CVN 78's EMALS and AAG continue to adversely affect sortie generation and flight operations, which remains the greatest risk to demonstrating operational effectiveness and suitability in 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 in developmental test, but improvements have not been assessed in operational testing. The Navy should verify electromagnetic spectrum compatibility during operational test, particularly when integrated with CSG operations in an advanced electronic attack environment. This will enable capability assessments at differing levels of system use to inform decisions on system employment. The Navy should apply lessons learned from CVN 78 to the future EASR configuration.

» SUITABILITY

Insufficient data are available to determine the *Ford*-class's operational suitability. However, the following five CVN 78 systems are new to the class and are highlighted as the most significant challenges to flight operations.

AAG

The Navy reported that during CVN 78's 262-day deployment, the ship and its embarked air wing completed 8,725 arrested landings utilizing the AAG. However, DOT&E has not received sufficient data to update the reliability statistics reported in the FY23 Annual Report. Naval Air Systems Command (NAVAIR) continues to work on short- and long-term improvements to address AAG reliability degraders. However, challenges in obtaining replacement parts and the reliance on off-ship technical support remain an issue. The Navy is also using IOT&E to inform the decision of whether to retrofit the fourth AAG engine on *Ford*-class aircraft carriers. The fourth AAG engine was incorporated into the *Ford*-class design, but not installed as a cost savings measure. The fourth engine would improve the reliability and availability of AAG, improve the pilot boarding rate, and restore a redundant capability to rig the barricade in the event of AAG engine failure, which the current configuration does not support.

EMALS

The Navy reported that during CVN 78's deployment, the ship and its embarked air wing completed 8,725 catapult launches using the EMALS. However, DOT&E has not received sufficient data to update the reliability statistics reported in the FY23 Annual Report. Despite engineering upgrades to hardware and software, reliability has not appreciably changed from prior years and reliance on off-ship technical support remains a challenge. NAVAIR is continuing development on improvements.

Advanced Weapons Elevators (AWEs)

The Navy reported that, during CVN 78's deployment, the ship's weapons department conducted 11,369 AWE runs, moving 1,829,580 pounds of ordnance to the flight deck. However, the Navy has yet to build and transfer ordnance to the flight deck at rates reflective of the Design Reference Mission. Of note, the crew is reliant on off-ship technical support for correction of hardware and software failures. DOT&E expects the SGR tests to be the first operationally representative demonstration of high ordnance throughput.

DBR

Details on DBR suitability can be found in DOT&E's classified EFR from April 2023. DBR availability declined during the FY23 COMPTUEX with the continuous demand for radar coverage and an intermittent failure observed during operations. Due to the one-of-a-kind nature of the DBR, its availability will depend on the Navy's access to replacement parts throughout the remaining life of the system. The Navy should acquire sufficient DBR replacement parts for the interim period prior to the scheduled replacement of DBR with EASR.

Manning and Berthing

Per the Navy's Shipboard Habitability Program, all new ships are required to have a growth allowance of 10 percent of ship's company when the ship delivers. This Service Life Allowance provides both empty bunks to allow for changes in the crew composition over the ship's life and berthing to support crew turnover, visitors, and personnel temporarily assigned to the ship for repairs, inspections, test, and training. However, sufficient berthing is not installed for the *Ford*-class to conduct combat operations with all hands assigned a bed, due to a lack of berthing capacity for embarked units. If the ship and its embarked units were each at 100 percent manning, the ship would have a shortfall of 159 beds. These berthing shortfalls will affect quality of life onboard and could reduce the Navy's operational flexibility in employing the ship across its full spectrum of missions and logistical support roles for the CSG. Furthermore, there is potential that the berthing shortfalls could increase as the air wing diversifies to include CMV-22, F-35, and MQ-25, none of which are embarked on the *Ford*-class today.

» SURVIVABILITY

The survivability assessment of the *Ford*-class against kinetic threats is based on a combination of FSST, TSST, and related modeling of the class supported by component and surrogate testing. To date, the Navy has completed all planned LFT&E, except for TSST and the final survivability assessment. The TSST is the last scheduled LFT&E event for the ship and will provide critical data on the damage control and recoverability design of the ship.

From June to August 2021, the Navy conducted FSST on CVN 78, including three shock events of increasing severity. In December 2022, DOT&E published a classified FSST report that details findings from the trial, and in July 2023, the Navy published its own FSST report. Both reports identify deficiencies that, if addressed, will improve the class's survivability against kinetic threats. The Navy has yet to issue a Shock Deficiency Correction Plan that will detail the corrective actions planned to rectify adverse findings from the FSST.

The survivability evaluation of the *Ford*-class in a cyber-contested environment was evaluated in March 2024 testing, and earlier land-based testing for EMALS and AAG. DOT&E's full assessment will be published following the underway test.

The survivability of the *Ford*-class in contested and congested electromagnetic spectrum environments is ongoing. Discussions on how to evaluate CVN 78 survivability in these environments are continuing with the Navy.

RECOMMENDATIONS

The following recommendations remain as stated in the FY23 Annual Report. The Navy should:

1. Improve the suitability of AAG, EMALS, AWE, and DBR while minimizing the requirement for off-ship and/or contractor technical support.
2. Reevaluate the timeline and better define the criteria for a decision to retrofit the fourth AAG engine.
3. Resource and execute the testing per Enterprise AW SSD TEMP 1714 and CVN 78 TEMP 1610, including the planned SGR testing, along with completing, verifying, validating, and accrediting the SGR M&S suite; underway cyber survivability testing; and self-defense tests and PRA modeling.
4. Re-examine manning and berthing for future ships of the class to ensure sufficient berthing is available and that 10 percent Service Life Allowance is allocated for future growth.
5. Prioritize and correct deficiencies identified in DOT&E's classified FSST report of December 2022.
6. Submit an update of the *Ford*-class TEMP for DOT&E approval in FY25 that is aligned with the new Enterprise TEMP 1910 and provides the test strategy and test resources to determine operational effectiveness of new and/or upgraded capabilities on CVN 79.
7. Verify electromagnetic spectrum compatibility during operational test to better inform effectiveness and survivability, particularly when integrated with CSG operations in an advanced electronic attack environment.

The following recommendations from the FY23 Annual Report have been updated. The Navy should:

1. Develop an effective strategy to collect data in accordance with the test plan for the remainder of IOT&E.
2. Continue to address the recommendations in DOT&E's classified self-defense interim assessment report from April 2022, and the additional recommendations in DOT&E's classified EFR from April 2023.
3. Continue to fully fund the scheduled replacement of DBR on CVN 78 with the EASR configuration.
4. Continue to develop more robust capabilities to test the cyber survivability of shipboard industrial control systems, similar to those capabilities demonstrated during the March 2024 cyber survivability testing.
5. Provide a strategy to update the survivability assessments included in the vulnerability assessment reports to reflect the ship as built to support delivery of the final survivability assessment report in 4QFY25.
6. Identify, fund, and deliver a replacement for the Navy's self-defense test ship, ex-USS *Paul F. Foster*, to support planned testing of CVN 79 capability.

The Navy should address the following recommendations, which are new:

1. Characterize and validate performance of the SSAM model for SGR.
2. Continue to update the IOT&E test plan for major remaining tests such as SGR, self-defense, and cyber survivability tests and submit to DOT&E for approval.

DDG 1000 *Zumwalt*-Class Destroyer

In FY24, the Navy's Operational Test and Evaluation Force (OPTEVFOR) continued operational test of the DDG 1000 *Zumwalt*-class destroyer with four live fire missile exercises and modeling and simulation (M&S) testbed runs to evaluate anti-air warfare capability against threat anti-ship cruise missiles (ASCMs) and aircraft. The *Zumwalt*-class Program Office reports that ship survivability M&S will not be updated to reflect the as-built configuration or installation of Conventional Prompt Strike (CPS). The *Zumwalt*-class Program Office has yet to fund or schedule Full Ship Shock Trials (FSST). *Zumwalt*-class survivability cannot be determined until the M&S update and FSST are complete.

SYSTEM DESCRIPTION

Zumwalt-class ships are long range, low observable, destroyers. They are equipped with: (1) a 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-6), and Evolved Sea Sparrow Missiles; and (3) two Mk 46 30mm close-in gun systems. The class is currently being modified to incorporate

CPS modules to enhance the class's strike warfare capability.

MISSION

The joint force maritime component commander can employ *Zumwalt*-class destroyers primarily for forward-deployed offensive surface strike missions, with a secondary mission of surface warfare dominance. As designed, the *Zumwalt*-class included undersea warfare capabilities; these capabilities are no longer required for the updated operational environment of the *Zumwalt*-class. The *Zumwalt*-class is designed for independent operations but can be integrated into Carrier or Expeditionary Strike Group operations.

The Navy will install CPS modules on each ship of the class between FY24 and FY28. These modules will provide the *Zumwalt*-class additional strike warfare capability.

PROGRAM

The *Zumwalt*-class is an Acquisition Category IC program. The President's Budget in 2011 truncated the class to three ships. The Navy commissioned USS *Zumwalt* (DDG 1000) in 2016, USS *Michael Monsoor* (DDG 1001) in 2019, and expects the delivery of USS *Lyndon B. Johnson* (DDG 1002) in FY27 after CPS install.

The Navy continues to update the *Zumwalt*-class TEMP due to significant modifications to the operational requirements and warfighting concept of operations. The Navy changed the *Zumwalt*-class's primary mission from land attack to open-ocean surface strike in 2019. The Navy codified additional changes in a June 2021 revision to the Operational Requirements Document, to include the integration of CPS. The Navy intends to update test requirements of the *Zumwalt*-class in the next revision of the TEMP, based on revised employment of the class.

The *Zumwalt*-class IOT&E started in October 2021. Completion of the IOT&E period has been delayed by a combination of factors, but DOT&E expects IOT&E to complete in FY25 after test of the *Zumwalt*-class primary mission, open-ocean surface strike. Test of the *Zumwalt*-class with CPS, and other features being installed through FY27, will occur in FOT&E. Evaluation of SM-6 integration of *Zumwalt*-class is also planned for FOT&E. DOT&E recommends a shock trial during FOT&E after completion of the Navy's shock qualification program, which will complete following installation of CPS.

» MAJOR CONTRACTORS

- Bath Iron Works, a subsidiary of General Dynamics Corporation – Bath, Maine
- HII – Pascagoula, Mississippi
- Raytheon, a subsidiary of RTX – Arlington, Virginia

TEST ADEQUACY

In FY23, the Navy completed a cyber cooperative vulnerability and penetration assessment and an adversarial assessment between November 2022 and March 2023. Testing encompassed Internet Protocol (IP) networks aboard the ship along with industrial control systems associated with its hull, mechanical, and electrical systems. These tests were adequate to assess cyber survivability of the class, were in accordance with the DOT&E-approved test plan, and were observed by DOT&E.

In FY24, OPTEVFOR continued operational test of the *Zumwalt*-class in accordance with DOT&E-approved test plans and DOT&E observation. The Navy conducted four live fire anti-air warfare tests in December 2023. Data collected from these tests were adequate to demonstrate the *Zumwalt*-class's ability to defeat ASCM raids in representative scenarios.

In FY24, OPTEVFOR continued Probability of Raid Annihilation M&S testbed runs with completion expected in FY25. These M&S runs are intended to predict the *Zumwalt*-class's probability of defeating inbound ASCMs and aircraft across an expanded set of scenarios from the previously identified live fire test events. The Navy expects to complete validation of the testbed in FY25 and expects to accredit it for this use. DOT&E continues to work with OPTEVFOR to ensure appropriate use of the M&S testbed for the determined uncertainties from the validation process.

The Navy plans to evaluate the *Zumwalt*-class primary mission of offensive surface strike with a Tomahawk missile launch in FY25, including shipborne strike planning events. Evaluation of *Zumwalt*-class employment of CPS will occur during FOT&E, in conjunction with CPS program testing, in FY27.

Torpedo defense testing, conducted with DDG 1000 in October 2021, provided data on the class's ability to evade torpedoes. However, full evaluation of the class's effectiveness against undersea threats has not been completed.

The Navy has yet to fund or schedule an FSST for the *Zumwalt*-class. As previously identified in the FY22 and FY23 Annual Reports, this test is required to adequately assess ship survivability against underwater threat weapons and determine residual mission capability following such an occurrence.

The Navy reports that budget and schedule shortfalls preclude updates to vulnerability and recoverability M&S to reflect the as-built *Zumwalt*-class or inclusion of CPS when installed. The Navy intends to complete a Final Survivability Assessment Report in FY25 that includes survivability findings related to earlier ship design. DOT&E will not be able to provide a complete assessment of the *Zumwalt*-class's vulnerability to threat weapons until M&S reflects the as-built ship and FSST is complete.

» EFFECTIVENESS

Insufficient data are available to determine *Zumwalt*-class operational effectiveness or change the preliminary assessment provided in DOT&E's classified early fielding report from November 2022. DOT&E will publish an IOT&E report of the *Zumwalt*-class operational effectiveness after completion of operational test that the Navy expects to occur in FY25. DOT&E will publish an update to this report after test of the *Zumwalt*-class employment of CPS that the Navy expects to occur in FY27.

» SUITABILITY

Insufficient data are available to determine *Zumwalt*-class operational suitability or change the preliminary assessment provided in DOT&E's classified early fielding report from November 2022. DOT&E will publish an IOT&E report of the *Zumwalt*-class operational suitability after completion of operational test that the Navy expects to occur in FY25. DOT&E will publish an update to this report after test of the *Zumwalt*-class employment of CPS, as well as evaluation of the technological refresh of the class's Command, Control, Communication, Computer, Cyber and Intelligence systems, that the Navy expects to occur in FY27.

» SURVIVABILITY

Assessment of *Zumwalt*-class cyber survivability is classified. DOT&E will publish a classified report of the *Zumwalt*-class cyber survivability after completion of IOT&E that the Navy expects to occur in FY25.

Due to vulnerability and recoverability M&S not yet being validated, and not reflecting the ship as-built, data remain insufficient to determine *Zumwalt*-class survivability against threat weapons. DOT&E will require that the survivability M&S be updated and validated as part of the upcoming TEMP revision.

Failure and recoverability mode testing aboard DDG 1001, conducted in 2022, provided insight into the recoverability of the class after damage. However, testing was not sufficient to resolve associated LFT&E critical issues due to limitations on the systems under test. DOT&E will address the strategy for completing the LFT&E assessment of the *Zumwalt*-class's mission system recoverability as part of the upcoming TEMP revision.

RECOMMENDATIONS

The Navy should:

1. Complete remaining IOT&E events as recommended in the FY23 Annual Report.
2. Submit for DOT&E approval a revision of the TEMP for modifications to the operational requirements

and employment of the *Zumwalt*-class to include installation of CPS.

3. Submit for DOT&E approval an update to the LFT&E Strategy that includes FSST and evaluation of the as-built *Zumwalt*-class following the installation of CPS.
4. Fund and schedule an FSST prior to the first deployment of a *Zumwalt*-class ship with CPS installed as recommended in the FY23 Annual Report.
5. As noted in the FY22 and FY23 Annual Reports, document the risk to the warfighter associated with incomplete component shock qualification and lack of an FSST, prior to deployment.
6. As recommended in the FY22 and FY23 Annual Reports, sufficiently fund modernization and sustainment of the DDG 1000 class to include improvements determined from failure and recoverability mode testing as documented in the Navy's report on the event.

DDG 51 Flight III Destroyer

In March 2024, the Missile Defense Agency (MDA), in collaboration with the Navy's Operational Test and Evaluation Force (OPTEVFOR), conducted the Flight Test Aegis Weapon System-32 (FTM-32) event as an integrated test to demonstrate the capability to detect, track, engage, and intercept a medium-range ballistic missile target. The lead ship for DDG 51 Flight III, USS *Jack H. Lucas* (DDG 125), participated in the flight test as part of IOT&E for Air and Missile Defense Radar (AMDR) / AN/SPY-6(V)1, DDG 51 Flight III, and Aegis Weapon System (AWS) Baseline 10. The Navy expects to complete IOT&E in FY28.

SYSTEM DESCRIPTION

DDG 51 Flight III is an evolutionary development of the DDG 51 program. The DDG 51 Flight III is a combatant ship equipped with the following:

- Aegis Combat System (ACS) including the AWS, used for integrated air and missile defense, surface warfare, anti-submarine warfare, and strike missions and self-defense and area-defense against current and future threats.
- AMDR / AN/SPY-6(V)1, a three-dimensional (range, altitude, and azimuth), multi-

function, active electronically scanned array radar.

- AN/SPQ-9B horizon search radar to detect air and surface contacts.
- AN/SQQ-89 undersea warfare suite, which includes the AN/SQS-53 sonar and the TB-37U Multi-Function Towed Array.
- Close-In Weapon System Block 1B for ship self-defense.
- Cooperative Engagement Capability (CEC) tracker and radar data sharing network.
- Surface Electronic Warfare Improvement Program (SEWIP) Block 2 (AN/SLQ-32(V)6) for electronic support.
- Five-inch diameter gun for surface warfare and land attack.
- MH-60R helicopters that support surface and undersea warfare.
- Mk 32 Surface Vessel Torpedo Tubes for over-the-side Mk 54 Torpedoes.
- Mk 38 25mm guns for small boat and unmanned aerial systems defense.
- Vertical Launch System that can launch Tomahawk; Standard Missiles 2, 3, and 6; Evolved Sea Sparrow Missile (ESSM) Blocks 1 and 2, and Anti-Submarine Rockets.

The Navy added a starboard enclosure to the DDG 51 Flight III to accommodate berthing for 30 additional sailors. This modification necessitated stacking the ship's two 7-meter boats. Additionally, the fantail was widened and additional ship structure was added to provide sufficient weight and buoyancy Service Life Allowances.

MISSION

Navy commanders will use DDG 51 Flight III destroyers to provide joint battlespace threat awareness and defense capability to counter current and future threats in support of:

- Integrated Air and Missile Defense
- Surface Warfare
- Anti-Submarine Warfare
- Strike Warfare

PROGRAM

DDG 51 Flight III, an Acquisition Category IC program, will be the fourth major configuration in the DDG 51-class program acquisition cycle. The Navy accepted delivery of DDG 51 Flight III lead ship, USS *Jack H. Lucas* (DDG 125), in June 2023. DDG 51 is in full-rate production with ships from the following configurations:

- Flight I: 21 ships delivered (DDG 51 – 71)
- Flight II: 7 ships delivered (DDG 72 – 78)
- Flight IIA: 45 ships delivered (DDG 79 – 123)
  2 ships under construction (DDG 124 and 127)
- Flight III: 1 ship delivered (DDG 125)
  10 ships under construction (DDG 126, 128 – 136)
  13 ships on contract (DDG 137 – 149)

DOT&E approved a combined TEMP describing the testing strategy for DDG 51 Flight III, AWS Baseline 10, and AN/SPY-6(V)1 in September 2022. Included in the TEMP was an LFT&E Strategy that focuses on evaluation of susceptibility, vulnerability, recoverability, and force protection against threats likely to be encountered in combat. The LFT&E Strategy includes a combination of surrogate testing, survivability modeling and simulation (M&S), and at-sea testing. Included in the at-sea testing is a two-shot Full Ship Shock Trial scheduled for FY26. DDG 51 Flight III IOT&E commenced in March 2024.

» MAJOR CONTRACTORS

- Bath Iron Works, a subsidiary of General Dynamics Corporation – Bath, Maine
- HII – Pascagoula, Mississippi

TEST ADEQUACY

In March 2024, USS *Jack H. Lucas* (DDG 125) participated in FTM-32, an integrated test to demonstrate the capability to detect, track, engage, and intercept a medium-range ballistic missile target utilizing a simulated Standard Missile-6 (SM-6). This event is detailed in the classified DOT&E FY24 Missile Defense System Annual Assessment, that will be published in 2QFY25. Significant intended data collection on DDG 51 Flight III's performance were not attained during test execution due to challenges with the ship's ACS and AN/SPY-6(V)1 during test execution. As a result, insufficient data are available to assess DDG 51 Flight III operational effectiveness from this flight test.

Evaluation of DDG 51 Flight III capability to defeat incoming threat anti-ship cruise missiles is constrained by available aerial test targets, or threat surrogates, that do not fully emulate the most stressing threats. Aerial targets provide demonstration of warship capability in the represented scenario and provide validation data to accredit M&S and estimate capability beyond the limited live test scenarios.

In October 2023, the Navy commenced blast fragility testing at Aberdeen Proving Ground in Aberdeen, Maryland. Testing was completed in accordance with the DOT&E-approved test plan and observed by DOT&E. The first series of tests evaluated the blast resistance of representative electrical equipment and provided data to set equipment fragility thresholds within survivability M&S. The Navy expects the second series of test to evaluate the blast resistance of Navy Standard doors and hatches to complete in FY25 and enable the setting of their thresholds with survivability M&S.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

No data are available to determine DDG 51 Flight III operational effectiveness, suitability, and survivability. DOT&E will report on the operational effectiveness, suitability, and survivability of DDG 51 Flight III after IOT&E and LFT&E are complete, currently expected by the Navy to be FY28.

RECOMMENDATIONS

The Navy should:

1. Fund development and procure aerial anti-ship cruise missile targets that emulate advanced and stressing threat ASCMs.
2. Determine and correct issues that limited evaluation of DDG 51 Flight III performance in FTM-32.

E-2D Advanced Hawkeye

In FY24, the Navy continued operational testing (OT) on the E-2D with Delta System Software Configuration Build 4 (DSSC-4). DSSC-4 improves the Advanced Hawkeye's command and control capability and is the fourth in a series of biennial hardware and software upgrades to the E-2D. The Navy deployed DSSC-4 in FY24 and plans to complete DSSC-4 testing in FY25. As a result of the Navy's decision to deploy DSSC-4 before the completion of OT, DOT&E published an early fielding report (EFR) in June 2024, based on testing completed to date. The Navy intends to continue developmental testing on the first iteration of DSSC-5 software, DSSC-5.1, through 1QFY25 and commence OT in 3QFY25.

SYSTEM DESCRIPTION

The E-2D Advanced Hawkeye is a carrier-based, airborne tactical command and control platform that enables offensive and defensive carrier strike group missions including airborne early warning. Its sensors and communications systems are designed to detect, track, and identify air and surface targets in blue-water, littoral, and overland environments.

The following subsystems and capabilities enable the Advanced Hawkeye to perform its mission:

- AN/APY-9 phased array radar that combines mechanical and electronic scan modes
- Tactical Targeting Network Technology data link
- Multifunctional Information Distribution System
- Cooperative Engagement Capability
- Communications suite
- Electronic support measures
- Electronic protection
- Aerial refueling

The E-2D Advanced Hawkeye Program also includes all simulators, interactive computer media, and documentation to conduct maintenance, as well as aircrew initial and follow-on training.

MISSION

Carrier strike group and joint force commanders use the E-2D Advanced Hawkeye to provide all-weather airborne early warning, airborne battle management, and command and control functions, and to support Navy Integrated Fire Control and theater air and missile defense missions. Additional missions include surface surveillance coordination, air interdiction, offensive and defensive counter air control, close air support coordination, time-critical strike coordination, search and rescue coordination, and communications relay.

PROGRAM

The E-2D is an Acquisition Category IC program. In FY23, the Navy fielded DSSC-4 prior to completing the OT requirements. DOT&E published an EFR in June 2024, in advance of DSSC-4's first operational deployment. Between 3QFY23 and 1QFY24, the Navy conducted its fourth follow-on test and evaluation period (OT-D4) for DSSC-4 to complete the remaining OT requirements. During OT-D4, the Navy assessed DSSC-4 improvements in beyond-line-of-sight communications, sensor integration, and tactical targeting networking technology. The Navy is also planning a fifth follow-on test and evaluation period (OT-D5) for DSSC-5.

DSSC-4 serves as the baseline for integration of communication and data processing capabilities that the Navy will fully deliver in DSSC-5. After DOT&E approved TEMP Revision F, the Navy decided to release DSSC-5 capabilities in two increments: DSSC-5.1 and DSSC-5.2. The Navy is working on a TEMP update to address those changes.

The TEMP presents a modeling and simulation framework for developing DSSC capabilities using the E-2D Systems Test and Evaluation Laboratory (ESTEL). The Navy intends to certify ESTEL capabilities in an incremental fashion, but as of this writing, the ESTEL is not accredited for use during OT.

» MAJOR CONTRACTOR

- Northrop Grumman Aeronautics Systems – Melbourne, Florida

TEST ADEQUACY

The evaluation of DSSC-4 involves a cumulative collection of integrated testing and OT data. Shortfalls in E-2D aircraft systems' maturity, reliability, and test resource availability challenged data collection during OT-D4, but OT was adequate for DOT&E to evaluate DSSC-4's operational effectiveness, suitability, and cyber survivability.

In 1QFY24, the Navy conducted DSSC-4 operational effectiveness and suitability testing in accordance with a DOT&E-approved FOT&E test plan. Testing occurred on the Atlantic Test Ranges using an Aegis land-based test site at Wallops Island, Virginia.

DOT&E observed these events. The Navy intended to conduct OT on the Hawkeye Integrated Training System at the Collins Aerospace facility in Sterling, Virginia, in FY24, but testing was delayed until FY25 to resolve deficiencies with the Hawkeye Integrated Training System software.

As reported in the FY23 Annual Report, the Navy conducted a DSSC-4 cyber survivability test in accordance with a DOT&E-approved test plan. Testing occurred in 1QFY23 at Patuxent River, Maryland. That test included a cooperative vulnerability and penetration assessment (CVPA) and an adversarial assessment (AA). The test, observed by DOT&E, was adequate to support a partial cyber evaluation, but it was not adequate to characterize the impact of E-2D operations from all cyber-attacks outlined in the test plan.

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

In June 2024, DOT&E assessed the operational effectiveness, suitability, and cyber survivability of the E-2D with DSSC-4 in a classified EFR. DOT&E will publish a classified, final DSSC-4 FOT&E end-of-test report in FY25.

During OT-D4, E-2D operational test aircraft suffered shortfalls in overall availability, reliability, and logistic supportability. DOT&E's July 2020 FOT&E report on the previous variant, DSSC-3, had similar assessments on the suitability of the E-2D.

The Navy did not meet all DSSC-4 cyber test objectives because of insufficient supporting information provided to the cyber assessment team and data link reliability problems encountered during cyber testing. The DSSC-4 cyber assessment failed to meet all test objectives, and DSSC-5 will introduce new mission-critical capabilities, so the Navy should conduct a cyber assessment for the DSSC-5 aircraft and software configuration.

RECOMMENDATIONS

As recommended in the FY23 Annual Report, the Navy should:

1. Increase aircraft availability and reliability at operational test squadrons to facilitate efficient execution of large, complex test events.
2. Continue to leverage large-force exercises and Navy Aegis Combat Systems ships' qualification trials to maximize OT data collection opportunities in operationally representative environments.
3. Develop a TEMP update to address planned DSSC-5 capabilities not covered in the current TEMP Revision F.
4. Accredit the ESTEL for use during OT of future DSSC builds.

Additionally, the Navy should:

1. Conduct cybersecurity testing for DSSC-5 in accordance with DOT&E guidance.

F/A-18 Infrared Search and Track (IRST) Block II

F/A-18 Infrared Search and Track (IRST) Block II completed operational testing in 4QFY24. Data analysis is ongoing, but operational test events were adversely affected by IRST Block II system reliability failures. The Navy conducted operational testing with Infrared Optimized Configuration (IROC) pods, which are an operationally equivalent pod designated for flight test. Low-Rate Initial Production (LRIP) pods, which may have increased reliability, are expected to deliver in September 2024. Test details for the IROC pods will be available in DOT&E's classified IOT&E report due out in 2QFY25.

SYSTEM DESCRIPTION

The ASG-34A(V)1 F/A-18E/F IRST is a centerline-mounted pod with 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 sensor assembly integrates onto the front of the redesigned FPU-13/A centerline fuel tank assembly. The fuel capacity of the FPU-13/A is 340 gallons compared to the 480-gallon FPU-12/A centerline fuel tank it replaces. The IRST acts as a complementary sensor to the aircraft's AN/APG-79 fire control radar in a heavy electronic attack or radar-denied environment. It operates autonomously, or in combination with other sensors, to support the guidance of beyond-visual-range air-to-air missiles.

MISSION

The F/A-18E/F Super Hornet will employ the IRST Block II as a complementary long-wave infrared sensor to the AN/APG-79 fire control radar in a heavy electronic attack or radar-denied environment. IRST Block II provides passive search, detect, track, and engage capabilities against airborne targets at long range and will support the guidance of beyond-visual-range air-to-air missiles, including the AIM-120 Advanced Medium-Range Air-to-Air Missile and AIM-9X Sidewinder Block II.

PROGRAM

The F/A-18 IRST Block II is an Acquisition Category IC program. DOT&E approved the Milestone C TEMP in May 2021, and the IOT&E test plan in March 2024. The Navy conducted developmental testing during FY23 and FY24, and IOT&E was conducted in FY24 in support of full-rate production. The Navy conducted operational testing with IROC pods, which are operationally equivalent pods designated for flight test. The Navy intends to field the IRST Block II LRIP pods, which may have increased reliability, to carrier-based F/A-18E/F Super Hornet squadrons in 1QFY25 to improve lethality and survivability in air superiority missions against advanced threats. IROC pods will not be released to the fleet and were only intended for developmental and operational testing.

» MAJOR CONTRACTORS

- Lockheed Martin Corporation – Orlando, Florida
- Boeing Defense, Space & Security – St. Louis, Missouri

TEST ADEQUACY

The Navy executed IOT&E between April and September 2024. Testing was conducted in accordance with DOT&E-approved test plans and observed by DOT&E. IOT&E, which included integrated test events conducted with instrumented aircraft from the developmental test squadron, was adequate to provide an assessment of the long-range detection and tracking capability, suitability, and cyber survivability of the IRST Block II pod. IOT&E data analysis is currently ongoing. Once complete, DOT&E will publish a classified IOT&E report, expected in FY25.

PERFORMANCE

» EFFECTIVENESS

IRST Block II operational flight test events demonstrated tactically relevant detection ranges against operationally relevant targets and the ability to translate these long-range target detections into stable system tracks to facilitate weapons employment. The Navy must continue to improve the F/A-18 E/F Super Hornet's operating software and address existing deficiencies to effectively integrate IRST into aircraft fire control solutions. Additional details will be provided in DOT&E's classified IOT&E report.

» SUITABILITY

IRST Block II demonstrated significant reliability problems during operational testing. Throughout the test period, IRST Block II suffered from hardware and software deficiencies, which required the aircrew to restart the pod multiple times. Troubleshooting and repair often exceeded the abilities of Navy maintenance crews and required assistance from Lockheed Martin. Many of these problems were discovered during integrated and operational test after the Navy completed a minimal developmental test program with the representative hardware. Additional details will be provided in DOT&E's classified IOT&E report.

» SURVIVABILITY

IRST Block II contributes to the survivability of the F/A-18E/F by providing target tracks in a contested and congested electromagnetic spectrum environments. Cyber survivability testing was conducted 1QFY24. Additional details will be provided in DOT&E's classified IOT&E report.

RECOMMENDATIONS

The Navy should:

1. Continue to address the known IRST Block II and Super Hornet operating software deficiencies as recommended in the FY23 Annual Report.
2. Continue to address the reliability deficiencies of IRST Block II.
3. Implement the recommendations in DOT&E's classified IRST Block II IOT&E report, after it is published in 2QFY25.

F/A-18E/F Super Hornet and EA-18G Growler

Left: F/A-18E Super Hornet | Right: EA-18G Growler

Both the F/A-18E/F Super Hornet and EA-18G Growler programs continue to experience development challenges in the latest system configuration set (SCS) updates. The Navy has continued to field SCS updates prior to completing OT&E, with the fielding of SCS H18 Release 2 in April 2024. The fielding decision was based entirely on integrated test (IT) events with no dedicated operational test (OT) events. In September 2024, DOT&E published an early fielding report (EFR) on SCS H18 Release 2. To date, the Navy has not accomplished dedicated OT for Release 2. DOT&E approved the SCS H18 Release 3 FOT&E plan in June 2024, and OT is currently being conducted. The Navy fielded H18 Release 3 in September 2024 prior to completion of OT.

SYSTEM DESCRIPTION

The F/A-18E/F Super Hornet is a twin-engine, supersonic, all-weather, carrier-capable, multirole combat aircraft performing a variety of roles, including air superiority, fighter escort, suppression of enemy air defenses, reconnaissance, forward air control, close and deep air support, day and night strike, and aerial refueling. The F/A-18E/F Super Hornet is the replacement for the F/A-18A through D and the F-14, and it complements the F-35C in a carrier environment. The F/A-18E/F Block III Super Hornet aircraft leverages ongoing production of the Kuwaiti Super Hornet; it is also available as a Block II aircraft retrofit. F/A-18E/F Block III Super Hornets include upgraded hardware, advanced cockpit displays, and improved networking capability.

The EA-18G Growler is a two-seat, electronic attack variant of the F/A-18E/F Super Hornet that can provide standoff, escort, and self-protection jamming using both noise and deception techniques against land/surface-based and airborne radar systems. The EA-18G Growler carries up to five AN/ALQ-99 tactical jammer system pods mounted under the wings and fuselage, which integrate with its internal AN/ALQ-218 electronic warfare system for detection and jamming. The EA-18G Growler also employs the AGM-88 High-Speed Anti-Radiation Missile/Advanced Anti-Radiation Guided Missile for suppression of enemy air defenses and the AIM-120 Advanced Medium-Range Air-to-Air Missile for self-protection. The Navy is currently testing the AN/ALQ-249 Next Generation Jammer Mid-Band (NGJ-MB) on the EA-18G Growler to eventually replace the AN/ALQ-99.

MISSION

Combatant commanders use the F/A-18E/F Super Hornet to conduct offensive and defensive counter-air combat missions and attack both ground-based and maritime targets with precision and non-precision weapons. The F/A-18E/F Super Hornet can also carry a pod that provides organic aerial refueling capability to a carrier strike group.

The EA-18G Growler can operate forward deployed from expeditionary land bases or as part of a carrier air wing. It is employed as an embedded airborne electronic attack platform, organic to the carrier strike group or integrated into the joint force. It can also be used in a tactical reconnaissance role.

PROGRAM

The F/A-18 Super Hornet and EA-18G Growler are Acquisition IC programs that share an acquisition strategy with SCS H18. Urgent fleet capability needs are driving the Navy's acquisition strategy for tactical aircraft SCS releases.

The Navy's acquisition strategy for SCS H18 is an incremental three-part test-and-release plan to support the urgent fleet needs that include the Long Range Anti-Ship Missile (LRASM)1.1 on the F/A-18E/F Super Hornet and NGJ-MB on the EA-18G Growler. In February 2023, the Navy completed IT events for SCS H18 Release 1, which did not produce sufficient operational data for a DOT&E assessment. However, the Navy required an early operational capability (EOC) and accepted the risk of fielding based on IT data alone. The Navy fielded SCS H18 Release 1 to support LRASM 1.1 capabilities. DOT&E received and approved an updated TEMP in June 2023. In August 2023, DOT&E published an EFR for SCS H18 Release 1 in response to the Navy's fielding decision.

In August 2023, the Navy conducted an operational test readiness review (OTRR) for SCS H18 Release 2, which is designed to enable NGJ-MB capability in the EA-18G Growler and capability enhancements in the F/A-18E/F. However, DOT&E did not approve the FOT&E due to significant unresolved software deficiencies. The Navy then combined a subset of SCS H18 Release 2 IT with H18 Release 3 testing with the goal of Release 2 supporting the NGJ-MB initial operational capability (IOC). Once the Navy was satisfied maintenance deficiencies with H18 Release 2 had been resolved, the Navy fielded Release 2 to the fleet in April 2024. Again, the Navy relied solely on IT events. In September 2024, DOT&E published an EFR on SCS H18 Release 2. To date, the Navy has not accomplished OT for the fielded version of Release 2.

DOT&E approved the SCS H18 Release 3 FOT&E plan in June 2024, and OT is currently being conducted. The Navy fielded H18 Release 3 in September 2024 prior to completion of OT.

The Navy is in the process of transitioning from the current "H"-series SCS development strategy to a more agile Continuous Integration, Delivery and Deployment (CID&D) strategy. The Navy intends to use the CID&D strategy to determine which capabilities should be prioritized and included in the planned annual releases. This strategy will also be used to facilitate early releases enacted to fulfill urgent needs in the fleet. Open Air Battle Shaping test instrumentation, which is essential for adequate mission-level evaluations, is built into SCS H18 and expected to expand with CID&D. The program office plans to deliver a CID&D TEMP to DOT&E in 2QFY25.

» MAJOR CONTRACTORS

- Boeing Defense, Space & Security – St. Louis, Missouri
- Raytheon, a subsidiary of RTX – Forest, Mississippi
- GE Aerospace, a subsidiary of General Electric – Evendale, Ohio

- Northrop Grumman Aeronautics Systems – Bethpage, New York
- Lockheed Martin Missiles and Fire Control – Orlando, Florida

TEST ADEQUACY

SCS H18 Release 1 and 2 OT with the F/A-18E/F Super Hornet and EA-18G Growler was observed by DOT&E, but was inadequate. The Navy is currently conducting OT on SCS H18 Release 3 and DOT&E is observing.

DOT&E received and approved an updated TEMP in June 2023, but the Navy had already fielded SCS H18 Release 1 without a DOT&E-approved TEMP and without conducting dedicated OT. The Navy relied on IT data collection, and while DOT&E approved the collection for potential OT consideration, OT data were not collected. The Navy identified Release 1 as an EOC to meet the combatant commander's intent.

The F/A-18E/F Super Hornet and EA-18G Growler programs conducted an OTRR in August 2023 for SCS H18 Release 2. The OTRR revealed severe system deficiencies that could impact OT adequacy, so DOT&E did not approve the programs to conduct FOT&E. The Navy completed several SCS H18 Release 2 IT events in August 2023 after DOT&E required the program to correct the severe system deficiencies and conduct a Delta-OTRR to show system maturity for FOT&E approval. However, the Navy did not conduct the Delta-OTRR and did not conduct SCS H18 Release 2 FOT&E during FY24. The Navy fielded H18 Release 2 to the fleet, but VX-9, the OT squadron for the F/A-18E/F and EA-18G programs, did not conduct OT of the final fielded version of H18 Release 2 (22.4.3) due to the compressed timeline for H18 Release 3 fielding. The Navy provided VAQ-133, an operational squadron, with H18 Release 2 (22.4.3) and designated the squadron as adjunct testers, but DOT&E has not yet received data from VAQ-133. Therefore, DOT&E did not assess the operational effectiveness, suitability, or survivability in the EFR written for the early fielding of SCS H18 Release 2 on the F/A-18E/F or EA-18G.

The Navy conducted IT of SCS H18 at Exercises SENTRY ALOHA in January 2024 and BLACK FLAG in April 2024. VX-9 began IT of the Release 3 builds of H18 for the EA-18G and F/A-18E/F platforms in February and March respectively, prior to conducting an OTRR. However, these tests were not accomplished under a DOT&E-approved test plan. DOT&E is currently analyzing the data to determine if it is adequate for OT purposes.

The F/A-18E/F Super Hornet and EA-18G Growler programs conducted an OTRR in May 2024 for SCS H18 Release 3. The OTRR revealed system deficiencies that could impact OT adequacy, but the SCS showed significant maturity over earlier SCS builds. DOT&E approved the H18 Release 3 FOT&E plan in June 2024. OT of SCS H18 Release 3 builds continued with participation in the annual fleet Rim of the Pacific Exercise (RIMPAC), which was identified in the DOT&E-approved test plans as being one of the primary test events for the final releases of SCS H18. However, the Navy fielded H18 Release 3 in September 2024, prior to completion of OT.

Based on DOT&E's recommendation in the FY23 Annual Report, the program office has made progress on addressing the test limitations and should continue to look for new opportunities for advanced red air, land-based radar threat simulators, and ship-based simulators for both the F/A-18E/F and EA-18G.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

The Navy did not have a DOT&E-approved SCS H18 Release 2 FOT&E plan and did not complete dedicated OT on the fielded version of H18 Release 2. As stated in the September 2024 EFR, DOT&E could not assess the effectiveness, suitability, or survivability of the F/A-18E/F and EA-18G aircraft with SCS H18 Release 2 due to a lack of OT data. The fielded version of SCS H18 Release 2 did undergo developmental testing, but it was not loaded by VX-9 due to a compressed timeline to complete FOT&E of H18 Release 3. The Navy conducted IT events for an earlier version of SCS H18 Release 2, but no significant data were generated by the IT events for analysis on the final version of SCS H18 Release 2 that was fielded to the fleet.

DOT&E will provide an assessment of SCS H18 Release 3 operational effectiveness, suitability, and survivability at the conclusion of FOT&E.

RECOMMENDATIONS

The Navy should:

1. Complete dedicated OT of SCS H18 Release 3 to assess operational effectiveness, suitability, and survivability prior to fielding subsequent versions.
2. Implement the recommendations provided in the SCS H18 Release 2 EFR of September 2024.
3. Continue to incorporate Open Air Battle Shaping instrumentation, high-fidelity active electronically scanned array threat radar emulators, and other new test assets (as they become available) into SCS OT&E to improve data collection, integrity, and thoroughness.
4. Submit a CID&D TEMP and test plan for DOT&E approval. Use the CID&D strategy to implement new capabilities and efficiently address deficiencies and untested capabilities that have been carried forward from SCS H18 and previous SCS versions.

LHA 6 Flight 1 Amphibious Assault Ship

In FY24, the Navy conducted no testing on LHA 6 Flight 1 Amphibious Assault Ships. The Navy expects to commence an FOT&E of LHA 6 Flight 1 in FY26. The LHA 6 Flight 1 TEMP, previously expected for delivery to DOT&E for approval in FY24, continues to be revised by the Navy and is now expected for approval in FY25.

SYSTEM DESCRIPTION

The LHA 6 class are large-deck amphibious assault ships intended to provide transportation and operational support for deployed Marine Corps forces, aircraft squadrons (including F-35B, AV-8B, MV-22, CH-53, AH-1, UH-1, and H-60 squadrons), and the Marine Air Ground Task Force. The class has two variants, referred to as Flights. The LHA 6 Flight 0, commencing with USS *America* (LHA 6), maximizes aviation capability (i.e., flight deck and hangar deck) and includes no well deck. The LHA 6 Flight 1, commencing with USS *Bougainville* (LHA 8), reduces aviation capability to support a well deck capable of deploying two Landing Craft Air Cushion (LCAC) hovercraft. LHA 6 Flight 1 is outfitted with Ship Self-Defense System (SSDS) Mk 2 Mod 4E, 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. LHA 6 Flight 1 will be outfitted with AN/SPY-6(V)2 as the air and missile defense radar.

MISSION

Joint force commanders will employ LHA 6-class ships as the primary command ship and aviation platform for an Amphibious Ready Group or Expeditionary Strike Group and associated Marine Expeditionary Unit/Marine Air-Ground Task Force. LHA 6 Flight 1 enables a mix of ground and aviation assets in support of Marine Corps warfighting concepts.

PROGRAM

The LHA 6 program is an Acquisition Category IC program. The Navy completed the LHA 6 Flight 0 IOT&E and LFT&E in FY17 and FOT&E in FY22. DOT&E published reports in April 2019 and February 2023 respectively. DOT&E removed LHA 6 Flight 0 from oversight in FY23. The Navy completed an operational assessment of the LHA 6 Flight 1 design in 2020. The LHA 6 Flight 1 TEMP, previously expected for delivery to DOT&E for approval in FY24, continues to be revised by the Navy and is now expected for approval in FY25. The LHA 6 Program Office expects to deliver USS *Bougainville* (LHA 8) in FY26 and subsequently conduct LHA 6 Flight 1 FOT&E and LFT&E.

In FY24, the Navy convened working groups to address recommendations in the FY23 Annual Report to investigate aviation space utilization options and supplemental crewing options that could support sustained operations with an F-35B-heavy Aviation Combat Element (ACE) embarked. These recommendations were based on observations from the LHA 6 Flight 0 FOT&E that was detailed in the FY22 Annual Report. The Navy and Marine Corps are currently working to define the formal requirements to inform discussions of Navy/Marine Corps aviation space allocation options. The working groups further concluded that additional information is necessary to determine specific manning stressors and directed the use of after-action reports from ship's operations regarding personnel and ongoing manpower studies to inform guidance on manpower requirements.

The Navy remains in the development of enterprise test strategies for SSDS Mk 2 Mod 4E and AN/SPY-6(V)2, which will coordinate ship self-defense evaluation of multiple ship classes, including LHA 6 Flight 1. The details of the enterprise approach are in the SSDS and Air and Missile Defense Radar (AMDR) / AN/SPY-6 articles in this Annual Report.

» MAJOR CONTRACTOR

- Ingalls Shipbuilding, a division of HII – Pascagoula, Mississippi

TEST ADEQUACY

As first reported in the FY21 Annual Report, DOT&E and the LHA 6 Program Office have yet to agree on an LHA Flight 1 LFT&E Strategy to evaluate the survivability of the LHA 6 Flight 1 against air-delivered or underwater kinetic threats. Specific DOT&E concerns are the lack of fire testing for embarked vehicle spaces and the lack of a Full Ship Shock Trial. DOT&E approval of the pending LHA Flight 1 TEMP is dependent of its inclusion of these test events and associated resources.

No testing was conducted in FY24. The Navy expects to begin FOT&E of LHA 6 Flight 1 in FY26.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

No data are available to assess LHA 6 Flight 1 operational effectiveness, suitability, and survivability. DOT&E expects to report on LHA 6 Flight 1 operational effectiveness, suitability, and survivability after completion of FOT&E that the Navy expects to commence in FY26.

RECOMMENDATIONS

The Navy should:

1. As recommended in the FY23 Annual Report, continue to investigate aviation space allocation options that support sustained operations with an F-35B-heavy ACE embarked.
2. As recommended in the FY23 Annual Report, continue to investigate supplemental crewing options for sustained LHA 6 Flight 0 operations with an F-35B-heavy ACE embarked.
3. As recommended in the last three DOT&E Annual Reports, deliver the LHA 6 Flight 1 LFT&E Strategy to DOT&E for approval in FY25. Identify resources in the updated TEMP for embarked vehicle fire testing and a Full Ship Shock Trial.

Littoral Combat Ship (LCS)

In FY24, the Navy conducted no operational test and deferred cyber survivability evaluation of the *Independence* variant of the Littoral Combat Ship (LCS) with the Mine Countermeasures (MCM) Mission Package (MP). The Secretary of the Navy expects to certify the replacement of the *Avenger*-class MCM ships and the MH-53E Sea Dragon helicopters in U.S. Central Command (USCENTCOM) with the *Independence* variant of the LCS with MCM MP and remaining Expeditionary MCM capabilities in FY25.

SYSTEM DESCRIPTION

The LCS is a small surface combatant designed for littoral operations and capable of executing open ocean missions. The LCS comprises two seaframe variants: the *Freedom* variant (odd-numbered) and the *Independence* variant (even-numbered). 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 Surface Warfare (SUW) and MCM MPs.

The SUW MP is scheduled to deploy only on the *Freedom* variant and derives its capability from the following components:

- Two Mk 46 30mm guns
- MH-60R helicopter
- Two 11-meter rigid-hull inflatable boats
- Surface-to-surface missile module with 24 Longbow Hellfire missiles

The MCM MP is scheduled to deploy only on the *Independence* variant and derives its capability from the following baseline components:

- AN/AES-1 Airborne Laser Mine Detection System (ALMDS) employed from an MH-60S helicopter
- AN/ASQ-235 Airborne Mine Neutralization System (AMNS) employed from an MH-60S helicopter
- MCM unmanned surface vehicle (USV) with AN/AQS-20C sonar (MCM USV and mine-hunt)
- Unmanned Influence Sweep System (UISS) that comprises the MCM USV with the mine sweep payload

The MCM MP will incorporate the following systems, pending continued system development:

- Barracuda Mine Neutralization System employed from MCM USV

In FY24, the following systems were removed from the MCM MP baseline:

- Knifefish Block I unmanned undersea vehicle
- AN/DVS-1 Coastal Battlefield Reconnaissance and Analysis Block I system

MISSION

The maritime component commander will employ LCS alone, or within a group of ships, to prepare the environment for joint forces access to littoral regions by conducting MCM or SUW operations, possibly under an air defense umbrella. Due to capabilities inherent to both seaframes, commanders can also employ LCS in a maritime presence role and support deterrence operations. Moreover, the Maritime Security Module of the SUW MP enables the *Freedom* variant to conduct Maritime Security Operations, including visit, board, search, and seizure (VBSS) of ships suspected of transporting contraband.

PROGRAM

The LCS seaframes and the combined MPs are each Acquisition Category IC programs. Additionally, several components within the MPs are themselves individual programs of record.

The Navy restructured the MCM USV program, subsuming the UISS program into one USV program with both mine hunt and sweep payloads. In FY24, one *Independence*-variant ship and one *Freedom*-variant ship were delivered. The Navy expects the remaining one *Independence*-variant and two *Freedom*-variant ships to deliver in FY25. In FY24, three MCM MPs and the final five SUW MPs were delivered with the remaining 21 MCM MPs expected between FY25 and FY33.

The LCS TEMP requires an update to address changes in the test program for the LCS MCM MP and for the Navy's divestment of the Anti-Submarine Warfare MP. The Navy intended to provide this update for DOT&E approval in FY23 but has delayed to FY25.

The Navy declared initial operational capability of the MCM MP and the MCM USV and mine-hunt payload (AN/AQS-20C sonar) and authorized full-rate production of the MCM USV and mine-hunt payload in FY23.

The Secretary of the Navy expects to certify that available LCS with MCM MP, combined with other remaining Expeditionary MCM capabilities, meets MCM operational requirements in the USCENTCOM area of responsibility and supports sunset of the *Avenger*-class MCM ships and the MH-53E Sea Dragon helicopters in this USCENTCOM area of responsibility, in FY25.

» MAJOR CONTRACTORS

- Lockheed Martin Corporation and Fincantieri Marinette Marine team – Marinette, Wisconsin

- Austal USA – Mobile, Alabama
- Northrop Grumman Corporation – Falls Church, Virginia

TEST ADEQUACY

In FY24, the Navy introduced no modifications to the *Freedom* variant that would change SUW MP performance and conducted no operational testing.

The Navy conducted no operational testing on the *Independence* variant with the MCM MP in FY24 and has planned no additional testing. DOT&E cannot determine operational effectiveness of the LCS MCM MP due to insufficient performance data on AMNS and ALMDS that the Navy elected to deliver in FY16 without conducting IOT&E. The Navy continues to work with DOT&E to provide fleet data from the employment of AMNS and ALMDS, but data are not yet sufficient to characterize their performance.

The Navy did not execute the planned FY24 cyber survivability evaluation of the *Independence* variant with MCM MP to include MCM USV and mine-hunt payload, due to unavailability of test assets; allocated funding for this test expired at the end of FY24. A cyber survivability evaluation and an operational performance evaluation of AMNS and ALMDS are required in order to complete the MCM MP IOT&E.

PERFORMANCE

» EFFECTIVENESS

Operational effectiveness of *Freedom* variant with the SUW MP was provided in the classified IOT&E report of July 2020. No modifications have been made that would change that assessment.

Insufficient data are available to determine operational effectiveness of the *Independence* variant with MCM MP due to uncertain performance in AMNS and ALMDS.

» SUITABILITY

Operational suitability of *Freedom* variant with the Increment 3 SUW MP was provided in the classified IOT&E report of July 2020. No modifications have been made that would change that assessment.

Insufficient data are available to determine operational suitability of the *Independence* variant with MCM MP, due to insufficient suitability data on AMNS and ALMDS. However, completed analysis suggests that:

- UISS remains not operationally suitable, as detailed in the UISS IOT&E report of June 2022.
- AMNS and ALMDS demonstrated low reliability prior to fleet release, as detailed in the classified LCS MCM MP Early Fielding Report of June 2016. Insufficient reliability data are available to re-assess.

» SURVIVABILITY

Cyber survivability of the *Freedom* variant with SUW MP was detailed in the classified June 2023 cyber addendum to the June 2020 IOT&E report. The Navy made no modifications to the *Freedom* variant with SUW MP that would change that assessment.

Insufficient data are available to determine cyber survivability of the *Independence* variant with MCM MP. The program office conducted two cyber developmental tests with NAVSEA Red Team and shared the resultant data with the operational test community, but data did not meet full requirements of operational evaluation for cyber survivability.

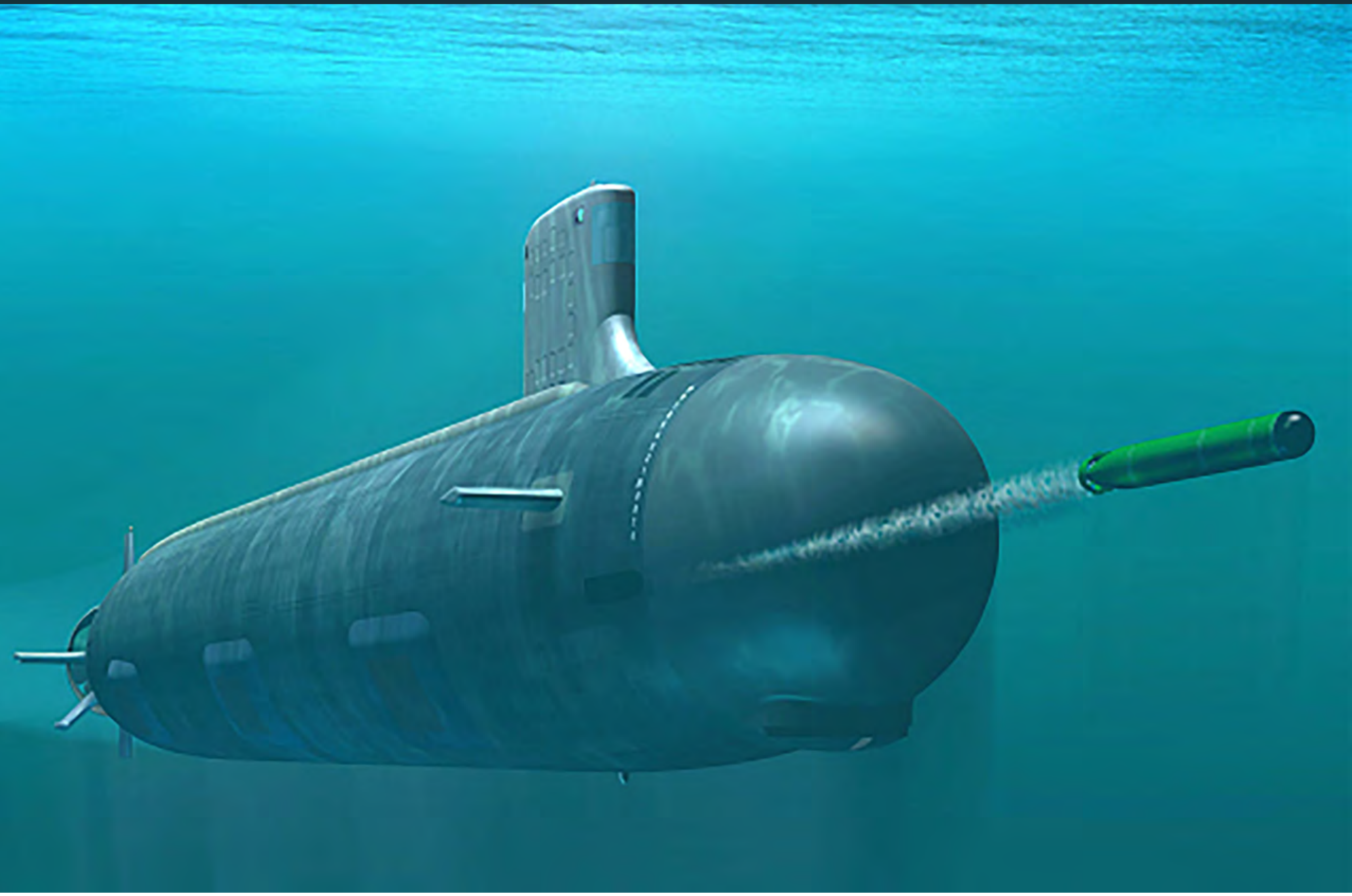
RECOMMENDATIONS

The Navy should:

1. Submit for DOT&E approval an update to the LCS TEMP that addresses changes in the test program for the LCS MCM MP.
2. Schedule and complete cybersecurity evaluation of the *Independence* variant with MCM MP in FY25.
3. As recommended in the FY23 Annual Report, fund and schedule operational test of ALMDS and AMNS in FY25 to sufficiently characterize their performance and determine operational effectiveness of the *Independence* variant with MCM MP.
4. As recommended in the FY23 Annual Report, improve

resilience of the *Freedom* variant with the SUW MP to cyber-attack by addressing recommendations in the classified June 2023 cyber addendum to the July 2020 IOT&E report.

Mk 48 Torpedo Modifications



In February 2024, DOT&E published a classified early fielding report (EFR) on the Mk 48 Heavyweight Torpedo with Shallow Water Urgent Build (SWUB) software to support a subsequent Navy fielding decision in the following month. In FY24, the Navy conducted two test events to evaluate Mk 48 torpedo performance within more representative scenarios to assess SWUB features. The Navy expects to complete FOT&E of the Mk 48 Mod 7 APB 6 torpedo in FY25.

SYSTEM DESCRIPTION

The Mk 48 is a submarine-launched heavyweight torpedo that directs itself toward a target submarine or surface ship based on an operator-developed targeting solution. The Mk 48 uses organic sensors to detect, classify, localize, and intercept its target.

The Mk 48 torpedo has hardware variants referred to as Mods. Each Mod represents a hardware improvement in capability, integrating upgraded sensors, guidance and control (G&C), and/or propulsion system. Two Mods are in use in the fleet with two additional Mods in development:

- Mod 6 integrated noise quieting in the propulsion section and commercial-off-the-shelf electronics in the G&C section. Advanced Common Torpedo (a follow-on improvement on Mod 6) integrated additional commercial-off-the-shelf electronics in the G&C section.
- Mod 7 Common Broadband Advanced Sonar System upgraded the sonar receiver.
- Mod 8 is in development and will consist of a new G&C section with an upgraded sonar array.
- Mod 9 is a five-year Middle Tier of Acquisition (MTA) rapid prototyping effort to develop several feature upgrades to include a new propulsion section.

Additionally, the Mk 48 torpedo undergoes regular software updates, referred to as Advanced Processor Builds (APB), to supplement the hardware Mods. APBs include modifications (e.g., tactics, classification algorithms, operator interface) intended to improve torpedo performance or simplify the operator interface. APBs can operate on various torpedo Mods with some variance in performance based on Mod hardware. Current APBs in use or in development are:

- APB 5 (found on Mod 7 torpedoes) – Modifications focused on detection and discrimination of target submarines and surface ships. It also provided an alternative tactic against surface ships.
- APB 5+ (found on Mod 7 torpedoes) – Modifications focused on simplifying the interface between the submarine's combat system and the torpedo. APB 5+ is limited to Mod 7 torpedo hardware and requires the employing submarine to have the AN/BYG-1 combat control system version APB-18/TI-19 or beyond.
- SWUB – Modifications were developed in FY23 and fielded in FY24 to address a classified urgent fleet need. The capability is an add-on and will be included as a baseline in future torpedo variants.
- APB 6 (developing for Mod 7 and Mod 8 torpedoes) – Modifications will improve torpedo tactics and sonar processing while introducing new classified capabilities via software. APB 6 is scheduled to attain initial operating capability in FY26 on Mod 7 and FY29 on Mod 8. Mod 7 APB 6 will introduce APB 6 capabilities that do not rely on the upgraded Mod 8 G&C.

MISSION

The Navy Submarine Force employs the Mk 48 torpedo to destroy threat submarines and surface ships in all ocean environments.

PROGRAM

The Navy fielded the earliest version of the Mk 48 heavyweight torpedo in 1972. Mk 48 Mod 7 and beyond are a shared development effort with the Royal Australian Navy. In FY24, the Navy completed the Acquisition Category III program for the Mk 48 with SWUB. In February 2024, DOT&E published a classified EFR on the Mk 48 torpedo with SWUB software. The Navy fielded the Mk 48 with SWUB the following month.

The Navy is completing developmental test of Mk 48 Mod 7 APB 6. The Navy expects to complete Mk 48 Mod 7 APB 6 FOT&E in FY25. The Navy initiated Mod 9 development in December 2023 as an MTA rapid prototyping effort with operational demonstration within five years.

The Navy expects to deliver the Mod 9 Master Test Strategy to DOT&E for approval in FY25. The Navy is also in development for Mod 8 APB 6 and intends a Milestone C decision in FY26 and FOT&E in FY28.

» MAJOR CONTRACTORS

- Lockheed Martin Sippican, Inc. – Marion, Massachusetts
- Lockheed Martin Corporation – Syracuse, New York
- Science Applications International Corporation, Inc. – Reston, Virginia

TEST ADEQUACY

In February 2024, DOT&E submitted a classified EFR on Mk 48 with SWUB. As detailed in the FY23 Annual Report, testing was adequate to evaluate a specific feature of the SWUB software. However, deviations from the DOT&E-approved test plan prevented an assessment of the end-to-end mission performance. The SWUB upgrade did not change cyber threat vectors or torpedo resilience to cyber-attack and cyber survivability was not evaluated for Mk 48 with SWUB.

The Navy conducted 18 exercise firings of the Mk 48 torpedo, in FY24 to evaluate SWUB features within end-to-end mission scenarios. The Navy's Operational Test and Evaluation Force developed a data collection plan and DOT&E observed these events for potential use of collected data in operational assessment. Testing in FY25 is required to assess operational effectiveness and suitability of Mk 48 Mod 7 APB 6.

The adequacy of future Mk 48 torpedo testing depends on representative threats and threat capability surrogates. In August 2020, the Navy began developing the Towed Array Threat Emulator (TATE) to improve the threat representation of the current surrogate for a mobile countermeasure, the Submarine Launched Countermeasure Emulator (SLACE). In July 2023, the Navy began developing the Modular Threat Countermeasure Emulator (MOTCE) to improve the threat representation for static countermeasures. The Navy expects SLACE with TATE, and MOTCE will be available for use in Mk 48 operational tests commencing in FY28.

The Navy uses a hardware in-the-loop simulator, the Environment Centric Weapons Analysis Facility (ECWAF), to test torpedoes in a simulated undersea environment. The use of ECWAF is integral in minimizing the number of actual at sea launches required to assess torpedo performance. The deferral of test events within some test environments in the Mod 7 APB 5 IOT&E reduced the live data available to validate the ECWAF for use in Mod 8 APB 6 IOT&E. Prior to Mod 8 APB 6 IOT&E, the Navy will need to collect data from fleet events conducted in these environments to validate and accredit the ECWAF for its full use. The full use of the ECWAF reduces live tests required to evaluate Mod 8 APB 6 to approximately half of those required for the Mod 7 APB 5 test design.

PERFORMANCE

» EFFECTIVENESS

Mk 48 with SWUB demonstrated a specific SWUB feature which operates as designed, but the end-to-end mission performance for SWUB intended use could not be determined. Details are in the classified EFR published in February 2024. Analysis of FY24 tests of the Mk 48 torpedo to evaluate SWUB features remain in progress. DOT&E will report Mk 48 operational effectiveness, including SWUB features, after completion of FOT&E that the Navy expects to occur in FY25.

» SUITABILITY

The Mk 48 Mod 7 remains operationally suitable. Torpedoes employed in FY23 to evaluate SWUB features on Mk 48 continued to meet operational availability and reliability needs. DOT&E will report Mk 48 Mod 7 APB 6 operational suitability, to include SWUB assessments, after completion of FOT&E that the Navy expects to occur in FY25.

» SURVIVABILITY

The SWUB software update was not designed to change the cyber resilience of the MK 48 torpedo, so the Navy did not conduct a cyber survivability assessment. MK 48 torpedoes with the SWUB software update remain not survivable to cyber-attack. Details are in the classified April 2022 APB 5 IOT&E report.

RECOMMENDATIONS

The Navy should:

1. Address all recommendations in the classified April 2022 APB 5 IOT&E report, the August 2023 APB 5+ FOT&E report, and the February 2024 SWUB EFR.
2. Obtain performance data from test environments deferred in APB 5 IOT&E to support validation of the ECWAF and its use in Mod 8 APB 6 IOT&E, as recommended in the FY22 and FY23 Annual Reports.
3. Complete development and validation of surface ship models and reverberation models in the ECWAF and validate their use for Mod 8 APB 6 IOT&E, as recommended in the FY23 Annual Report.
4. Complete development of the TATE and MOTCE prior to FY28. Include SLACE with TATE, and MOTCE in testing for Mod 8 APB 6 IOT&E.

MQ-25 Stingray Carrier Based Unmanned Aerial System (CBUAS)

Since achieving Milestone B (MS B) in August 2018, a series of technical delays led the MQ-25 Program Office to submit a request for fiscal reprogramming in FY23, and Congress granted that request in 2QFY24. The Navy will submit an updated MS B TEMP as well as a MS C TEMP to DOT&E for approval in FY25.

SYSTEM DESCRIPTION

The MQ-25 Stingray Carrier-Based Unmanned Aerial System (CBUAS) is composed of the MQ-25A Stingray air vehicle (Group 5 unmanned aircraft system (UAS)) and the Unmanned Carrier Aviation Mission Control System (UMCS) MD-5 Ground Control Station (GCS). The UMCS is the system-of-systems required for MQ-25 air vehicle and payload command and control. The MD-5 GCS, developed by the U.S. Government, is composed of Lockheed Martin's Skunk Works® Multi Domain Combat System (MDCX™), which is the Air Vehicle Pilot operating consoles and associated computing systems, and U.S. Government-developed communications, networking, and other ancillary equipment. The MQ-25 is intended to enhance carrier air wing (CVW) warfighting capabilities as a dedicated carrier-based tanker with a secondary maritime intelligence, surveillance, and reconnaissance (ISR) role. MQ-25 will assume the organic tanking mission currently performed by the F/A-18E/F. The MQ-25 is intended to integrate manned and unmanned operations while maturing complex sea-based command, control, communication, computers, and intelligence UAS technologies to support future UAS development to pace emerging threats.

MISSION

Commanders will utilize the MQ-25 to provide tanking and ISR capabilities to the carrier strike group, extend CVW strike range and alleviate the persistent, sea-based ISR gap, while introducing and integrating organic unmanned aviation into the CVW.

PROGRAM

The MQ-25 CBUAS is composed of the MQ-25A Stingray air vehicle, an Acquisition Category IB program; the MD-5 UMCS, an Acquisition Category II program; and additional systems, capabilities, and facilities needed to enable operations. The MQ-25 will be the first operational, carrier-based, fixed-wing, and catapult-launched UAS.

In the DOT&E-approved MQ-25 MS B TEMP, the MS C decision was to occur in FY23 and be informed by an operational assessment (OA) based on testing up to and including initial sea trials. In December 2022, based on production delays, the Navy issued an updated Acquisition Decision Memorandum which revised the MS C criteria to use information from an early operational assessment (EOA) that would be based on data collected between June 2019 and December 2021 that utilized a Boeing-owned, -operated, and -funded MQ-25A Stingray prototype.

The prototype test program was a 30-month, risk-reduction effort with ground and flight events executed at Mid-America Airport in Mascoutah, Illinois; ground events at Naval Air Station Norfolk, Virginia; and an underway (non-flight) deck-handling demonstration onboard USS *George H. W. Bush* (CVN 77) in December 2021, which concluded the program. While the prototype demonstrated in-flight refueling capability and was taxied under its own power on the flight deck, there are significant differences between the prototype and the MQ-25A Engineering Development Model design. These differences include internal structures, fuel system design, communications, and network architecture, and for later test articles, obsolescence updates for some internal hardware that need to be incorporated before production model delivery. Moreover, the prototype was flown with a Boeing ground station, not the Lockheed Martin-produced UMCS ground station planned for use with fleet aircraft. At the time of testing, the Navy did not intend the prototype test program to inform an EOA, and DOT&E did not observe the testing. Developmental risk reduction activities are in progress at both Boeing-owned and U.S. Government-owned software and hardware integration labs.

Due to an extension of the engineering and manufacturing development phase, as well as delays with MQ-25A Stingray production of test air vehicles, MS C did not occur in FY23. The MQ-25 program office is currently in the process of completing and submitting an updated MS B TEMP to DOT&E for approval, which is expected to arrive in FY25.

» MAJOR CONTRACTORS

- Boeing Defense, Space & Security – St. Louis, Missouri (MQ-25A Stingray)
- Lockheed Martin Corporation – Marietta, Georgia (Multi-Domain Combat System)

TEST ADEQUACY

DOT&E has not approved any operational test plans for MQ-25. Once the MS B TEMP update is approved, the Navy should submit to DOT&E for approval a test plan which includes an adequate OA. An adequate OA should be conducted using operationally representative air vehicles and include the MQ-25's primary operational environment: carrier-based flight operations. As a result, this OA should use non-prototype air vehicles and incorporate all test events up to and including initial sea trials.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Insufficient data are currently available to evaluate the MQ-25 operational effectiveness, suitability, and survivability.

RECOMMENDATION

The Navy should:

1. As recommended in the FY23 Annual Report, submit an update to the MS B TEMP to DOT&E for approval.

MQ-4C Triton

The MQ-4C Triton program has not entered IOT&E. Immature systems that prevented IOT&E in FY23 continue to preclude operationally representative testing for the primary missions. Even so, the Navy fielded multiple new MQ-4C configurations in FY24 without operational testing. In January and December 2024, DOT&E published Early Fielding Reports (EFR) for MQ-4C Triton Integrated Functional Capability (IFC) 4.1.2.4, IFC 4.1.2.6, IFC 4.2, and IFC 4.2.1.

SYSTEM DESCRIPTION

The MQ-4C Triton is a high-altitude, long-endurance, intelligence, surveillance, and reconnaissance (ISR) unmanned aircraft intended to support global naval and joint operations by collecting, processing, and distributing geospatial intelligence (GEOINT), including imagery and track data, and signals intelligence (SIGINT) data to tactical and information operations centers.

MISSION

Commanders will employ the MQ-4C to provide persistent, broad-area ISR 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, along with the P-8A Poseidon, of the Navy's maritime ISR transition plan to retire the EP-3E Aries II. Section 112 of the FY11 National Defense Authorization Act prohibits the Navy from retiring or preparing to retire the EP-3E until it fields one or more platforms that provide an equivalent or superior capability in the aggregate.

The program is following an incremental development approach after restructuring in 2021. The first increment is designed for the Navy to deliver SIGINT capabilities sufficient to support the MQ-4C's portion of the maritime ISR transition plan. DOT&E approved Revision E of the TEMP in January 2023. The Navy declared initial operational capability with the IFC 4.1.2.3 configuration in July 2023. In addition, the Navy's Operational Test and Evaluation Force (OPTEVFOR) published a classified interim report in July 2023. The Navy approved an updated acquisition strategy in August 2023. As previously reported, DOT&E published a classified EFR in August 2023. The Navy subsequently fielded the IFC 4.1.2.4, IFC 4.1.2.6, IFC 4.2, and IFC 4.2.1 configurations. DOT&E published an unclassified EFR in January 2024, addressing only test adequacy, and another classified EFR in December 2024 following the Navy's fielding decision.

» MAJOR CONTRACTOR

- Northrop Grumman Corporation Aeronautics Sector – Rancho Bernardo, California

TEST ADEQUACY

The Navy has not yet started IOT&E. As stated in the FY23 Annual Report, the Navy intended to enter IOT&E in January 2023. DOT&E did not approve the IOT&E plan because SIGINT system deficiencies prevented operationally realistic testing. DOT&E did approve conduct of the GEOINT and cyber survivability portions of the test plan for integrated testing. The Navy has since fielded multiple new IFC configurations. The MQ-4C integrated test team conducted three dedicated SIGINT flights in April and May 2024 with a system in the IFC 4.2 configuration to assess the performance of the SIGINT systems. These events demonstrated that the SIGINT deficiencies still prevent operationally realistic testing.

The Navy has not conducted any operational testing of the effectiveness or suitability of the fielded IFC 4.1.2.4, IFC 4.1.2.6, IFC 4.2, or IFC 4.2.1 configurations.

OPTEVFOR conducted cyber survivability testing of the MQ-4C in October 2023 and March 2024 as integrated testing that will be potentially usable for IOT&E. OPTEVFOR conducted, and DOT&E observed, the testing in accordance with the approved portion of the test plan.

OPTEVFOR conducted integrated testing of the Joint Signal Processor (JSP) capability in June 2024 that will be potentially usable for IOT&E. The JSP capability was not included in the original IOT&E plan. After integration of the JSP capability, OPTEVFOR submitted an IOT&E plan change covering that capability. DOT&E approved the test plan change as integrated testing in May 2024. OPTEVFOR conducted the testing in accordance with the change. DOT&E was unable to observe this test.

As previously reported, the Navy has not yet demonstrated a reliable method to collect MQ-4C SIGINT data and has not yet fully implemented their tasking, collection, processing, exploitation, and dissemination plan for MQ-4C mission data.

PERFORMANCE

» EFFECTIVENESS

As stated in the FY23 Annual Report, GEOINT performance of the IFC 4.1.2.3 configuration was qualitatively comparable to the IFC 3 configuration the Navy fielded as an early operational capability. Details are provided in the August 2023 classified EFR. Any effects of the changes in IFC 4.1.2.4, IFC 4.1.2.6, IFC 4.2, and IFC 4.2.1 on the operational effectiveness of the MQ-4C in the GEOINT mission are not known.

The operational effectiveness of the MQ-4C for its primary SIGINT missions remains unknown. An initial assessment of the operational effectiveness of the JSP capability and an update on SIGINT systems are provided in the December 2024 classified EFR.

» SUITABILITY

As stated in the FY23 Annual Report, the reliability, availability, and maintainability of the IFC 4.1.2.3 configuration are not likely to sustain the planned operational tempo. The only data that could be collected for suitability assessment was during JSP testing. An update of the operational suitability of the MQ-4C in the IFC 4.2 configuration is provided in the December 2024 classified EFR.

» SURVIVABILITY

An initial assessment of the survivability of the MQ-4C in contested cyberspace is provided in the December 2024 classified EFR.

RECOMMENDATIONS

As recommended in early fielding reports and previous Annual Reports, the Navy should:

1. Develop and demonstrate a method to extract SIGINT mission data from the MQ-4C system.
2. Complete the integrated test program and correct major deficiencies prior to proceeding into IOT&E.
3. Complete IOT&E to evaluate the operational effectiveness, suitability, and survivability of the system.
4. Complete development and implementation of the tasking, collection, processing, exploitation, and dissemination plan for MQ-4C mission data.

MQ-8C Fire Scout

In March 2024, the Navy's Operational Test and Evaluation Force (OPTEVFOR) ended test of the MQ-8C Surface Warfare (SUW) Increment prior to completing all test requirements in the DOT&E-approved test plan. In August 2024, DOT&E published a classified FOT&E report that identified the MQ-8C SUW Increment as not operationally effective or suitable. Although some mission areas were unresolved due to limited data, DOT&E requires no additional testing due to the Navy's divestiture of the system in the Presidential Budget 2025.

SYSTEM DESCRIPTION

The MQ-8C is a helicopter-based tactical unmanned aerial system designed to support intelligence, surveillance, and reconnaissance as well as SUW payloads. The air vehicle (AV) is a modified Bell 407 airframe embarking on and supporting the littoral combat ship. The basic AV is equipped with the Battle - Ready Infrared Targeting Equipment Star Block II multi-sensor imaging system equipped with Electro-Optic/Infrared (EO/IR) cameras and laser range finding and target designation.

The MQ-8C SUW Increment integrates the AN/ZPY-8 multi-mode active electronically scanned array (AESA) radar into the aircraft. Additionally, it adds the Minotaur Mission Management System for track correlation. The AESA radar has maritime search, inverse synthetic aperture radar, and synthetic aperture radar imagery modes.

MISSION

Embarked on littoral combat ships, the MQ-8C SUW Increment is intended to provide open ocean search and maritime target detection capability operating over-the-horizon for contact and track detection to support battlespace awareness. The system is also designed to support target cuing for the employment of shipboard weapon systems as well as remote target designation for precision-guided munitions fired by MH-60R/S helicopters.

PROGRAM

The MQ-8C Fire Scout is an Acquisition Category IC program that received Milestone C approval in FY17. The Navy completed procurement of 38 baseline aircraft in FY19. To support Navy testing, DOT&E approved an MQ-8C SUW Increment operational test plan in April 2021 that provided flexibility for integrated testing through the completion of final SUW system development. DOT&E approved an update to the MQ-8C TEMP in February 2022 that detailed the test strategy for the baseline aircraft upgrade to the MQ-8C SUW Increment.

The Navy initiated the divestment process in FY24 with completion of planned divestiture in FY26.

» MAJOR CONTRACTOR

- Northrop Grumman Systems Corporation – San Diego, California

TEST ADEQUACY

In FY24, DOT&E determined developmental testing conducted between April 2021 and August 2023, primarily testing at the Navy's Atlantic Test Range facility, Maryland, met objectives of the DOT&E-approved operational test plan and represented integrated test for MQ-8C SUW assessment. DOT&E observed portions of these developmental test events. The test events were primarily land-based testing. Testing provided maritime search radar performance data, including the use of inverse synthetic aperture radar mode, against Navy surface targets and non-Navy targets of opportunity, or watercraft that transited the test area, in the Chesapeake Bay, Maryland. Testing also included overland surveillance using synthetic aperture radar mode. OPTEVFOR conducted no dedicated operational test events with the MQ-8C SUW Increment embarked on littoral combat ships during underway operations. OPTEVFOR conducted limited at-sea testing of the SUW Increment aircraft from a littoral combat ship in FY22 and FY23.

In March 2024, OPTEVFOR ended test of the MQ-8C SUW Increment prior to completing all test requirements of the DOT&E-approved test plan. OPTEVFOR considered the data collected to be sufficient to determine operational effectiveness and suitability. DOT&E concluded that the collected data were not adequate for a complete assessment of the system; some aspects of operational effectiveness and operational suitability cannot be determined. However, DOT&E did not require additional test due to the Navy's divestiture of the system in the Presidential Budget 2025. In August 2024, DOT&E published a classified FOT&E report with a limited assessment of operational effectiveness and suitability of the MQ-8C SUW Increment.

PERFORMANCE

» EFFECTIVENESS

The MQ-8C SUW Increment is not operationally effective, with some mission areas unresolved. Details are in the classified FOT&E report.

» SUITABILITY

The MQ-8C SUW Increment is not operationally suitable. However, software upgrade 12.2 of the AV likely improved reliability compared to software 12.1. Details are in the classified FOT&E report.

» SURVIVABILITY

Cyber survivability testing was not evaluated during the MQ-8C SUW Increment FOT&E. The baseline MQ-8C aircraft, including the SUW Increment, remains not cyber survivable as reported in DOT&E's IOT&E report of September 2019.

RECOMMENDATIONS

If the Navy plans to use the baseline MQ-8C aircraft, or its mission capability systems including the SUW Increment in the future, it should:

1. Address the recommendations identified in the classified FOT&E report of August 2024.
2. Update the cyber resilience of the baseline MQ-8C aircraft and its mission capability systems to address the issues identified in the classified IOT&E report of September 2019 and for increased cyber challenges since 2019. Conduct a comprehensive cyber survivability assessment of the system before fleet employment.

Next Generation Jammer Mid-Band (NGJ-MB)

In FY24, the Navy made substantial progress with the Next Generation Jammer Mid-Band (NGJ-MB) system, culminating in the completion of integrated testing (IT) in July 2024. Despite this progress, DOT&E could not draw definitive conclusions about the system's operational effectiveness or suitability based on the IT results. The data reveal that while progress has been made, significant technical challenges remain, particularly in the area of reliability, which currently hinders the system's ability to fully support operational missions. The NGJ-MB Program Office has actively worked to resolve these reliability issues both before and during IOT&E, which commenced in July 2024. The Navy deployed the system with Electronic Attack Squadron (VAQ-133) in July 2024, prior to the completion of IOT&E. In November 2024, DOT&E published a classified early fielding report (EFR).

SYSTEM DESCRIPTION

The NGJ-MB is an airborne electromagnetic attack system, consisting of two pods, mounted under the EA-18G wings, containing Active Electronically Scanned Arrays (AESA) that radiate over a range of frequencies. The NGJ-MB is the first of three proposed programs for the overall Next Generation Jammer upgrade that is intended to eventually replace the legacy AN/ALQ-99 Tactical Jammer System in the EA-18G. The NGJ-MB will add increased jamming capability at higher power and longer ranges than the AN/ALQ-99 Tactical Jammer System, as well as the ability to rapidly update hardware and software to counter rapidly evolving threat capabilities.

MISSION

Combatant commanders will employ NGJ-equipped EA-18Gs as an embedded component of Carrier Air Wings and joint forces to deny, degrade, disrupt, or deceive the adversary's use of the electromagnetic spectrum while protecting friendly forces. The NGJ-MB is typically employed as a component of a Carrier Air Wing, embarked on an aircraft carrier in support of operations in a Carrier Strike Group.

PROGRAM

The NGJ-MB is an Acquisition Category IC program. In May 2021, the Secretary of the Navy approved the NGJ-MB program to move past Milestone C, thereby authorizing procurement of the low-rate initial production pods. The Navy conducted an updated operational test readiness review in May 2024 to re-evaluate the progress made since the Navy's first operational test readiness review in April 2023. DOT&E determined that the NGJ-MB's progress toward test readiness, along with an update to the NGJ-MB IOT&E plan, warranted the system's entry into operational testing. DOT&E approved the IOT&E test plan in July 2024.

The Navy deployed the NGJ-MB with Electronic Attack Squadron (VAQ-133) in July 2024, prior to completing IOT&E. The deployed pods were loaded with an earlier software version (P5.2) than what is being tested in IOT&E. Further testing on the fielded software version is scheduled. The Navy seeks to complete IOT&E in 1QFY25 to support an FY25 full-rate production decision.

» MAJOR CONTRACTORS

- Raytheon, a subsidiary of RTX – El Segundo, California
- The Boeing Company – St. Louis, Missouri
- Northrop Grumman Mission Systems – Linthicum, Maryland

TEST ADEQUACY

In March 2024, the Navy completed NGJ-MB IT with participation in Exercise Red Flag 2024. This testing was observed by DOT&E, but it was not conducted in accordance with a DOT&E-approved test plan. During IT, the NGJ-MB was loaded with earlier software versions than the P5.3 series loaded on the pods for the ongoing IOT&E period. Following a 4QFY23 meeting with the Navy's Operational Test and Evaluation Force (OPTEVFOR) and Air Test and Evaluation (VX-9), the operational test squadron for the NGJ-MB and DOT&E agreed that some of the data collected during IT, using the earlier software build, could be used for operational test consideration upon further validation of subsequent software versions, and demonstration of an organized software development plan. DOT&E published a classified EFR in November 2024, containing data through the beginning of July 2024 when the Navy fielded NGJ-MB with software version P5.2 prior to the completion of IOT&E.

The Navy participated in Exercise Rim of the Pacific (RIMPAC) 2024 with NGJ-MB, conducting War at Sea scenarios. The Navy also conducted a capstone test event in 1QFY25 with NGJ-MB at the Electronic Combat Range in China Lake, California, to verify the performance of later system software versions. Both events were observed by DOT&E and conducted in accordance with the DOT&E-approved IOT&E test plan.

The Navy intends to use modeling and simulation to supplement its evaluation of the NGJ-MB's operational effectiveness, to compliment electromagnetic warfare test and training on open-air ranges and support adequate testing. After the test data from the accredited modeling and simulation has been received, DOT&E will be able to use the results from the modeling and simulation in June and July 2024 and Design Reference Mission (DRM) analyses in August 2024 to support an assessment of NGJ-MB performance for IOT&E. Model validation and accreditation are expected to be completed in 2QFY25.

Technical challenges were significant during the course of all testing in FY24. Specifically, reliability has been a clear challenge during the course of the program development, to the point of affecting suitability and the ability to assess the performance of the system overall. Early reliability issues were predominantly hardware related, but after further development and implementation of fixes, the remaining issues appear to be mostly software centric. Although data are still insufficient to fully assess the reliability of the system, data trends have been markedly improving, suggesting the potential for a strong positive reversal in the future.

PERFORMANCE

» EFFECTIVENESS

Insufficient test data are available from the later versions of NGJ-MB and EA-18G software to determine NGJ-MB operational effectiveness, suitability, and survivability. DOT&E published a classified EFR in November 2024. IOT&E will complete in 1QFY25, and DOT&E will publish an IOT&E report in 3QFY25.

» SUITABLITY

The NGJ-MB Program Office worked to mitigate observed reliability challenges, both before and during IOT&E. Initial suitability results are provided in the DOT&E September 2024 classified EFR. DOT&E will provide a full evaluation of operational suitability, to include reliability, availability, pilot and maintainer workload, usability, and training, in an IOT&E report after testing ends in 1QFY25.

» SURVIVABILITY

Program stakeholders assessed results from developmental cyber survivability testing using NGJ-MB software version P5.1.3 and are addressing any system vulnerabilities. DOT&E approved the developmental cyber testing with additional supply chain analysis as adequate to evaluate the system during IOT&E. DOT&E will assess the cyber survivability of the system in their classified IOT&E report, following completion of IOT&E in 1QFY25. The survivability determination will rely on the results of a previous cyber tabletop, multiple cooperative vulnerability identification events, and an adversarial developmental T&E cybersecurity event.

RECOMMENDATIONS

The Navy should:

1. Complete IOT&E, performing the most rigorous testing possible on the open-air ranges, in accordance with the DOT&E-approved test plan.
2. Continue to develop and support advanced test and training infrastructure for electromagnetic warfare.
3. Continue to refine the software development plan; threat and technique libraries; and tactics, techniques, and procedures for the employment of NGJ-MB.

Offensive Anti-Surface Warfare (OASuW) Increment 1

In FY24, the Offensive Anti-Surface Warfare (OASuW) Increment 1 program continued the development of missile hardware and software to increase targeting capabilities and employment range over the previously fielded AGM-158C Long Range Anti-Ship Missile (LRASM 1.0). The Navy conducted modeling and simulation (M&S) events and an LRASM 1.1 integrated developmental/operational weapon employment test event. The Navy performed LRASM 1.1 integrated flight test events in accordance with the DOT&E-approved Master Test Strategy (MTS). DOT&E concurred with the Navy's plan to collect operational test (OT) data during integrated test (IT), subject to final trial validation, with the understanding that the Navy would deliver the complete IOT&E plan before further OT data were collected. A DOT&E-approved IOT&E plan is expected in 1QFY25. Following IT, the Navy fielded LRASM 1.1 in November 2023 prior to dedicated OT beginning in July 2024. DOT&E published a classified early fielding report in April 2023. The Navy is currently developing the next missile upgrade, LRASM C-3, which brings an upgraded threat target library, greater employment range, and beyond line-of-sight communication capability.

SYSTEM DESCRIPTION

The OASuW Increment 1 is the first weapon of an incremental approach to produce an OASuW capability in response to an urgent U.S. Pacific Fleet operational need generated in 2008. AGM-158C LRASM, the weapon system for the OASuW Increment 1, is a long-range, conventional, air-to-surface, precision-standoff weapon intended for launch from the Navy's F/A-18E/F and the Air Force's B-1B aircraft. Once launched, LRASM guides to an initial point using a GPS guidance system and employs onboard sensors to locate, identify, and provide terminal guidance to the target.

To date, there are three LRASM variants that comprise the OASuW Increment 1 program, designated LRASM 1.0, LRASM 1.1, and LRASM C-3. In FY22, the Navy began development of LRASM C-3, which added extended range capability. The LRASM C-3 upgrade remains focused on surface warfare capabilities and includes a greater employment range, beyond line-of-sight communication capability, and threat target library improvements. The Navy continues to work through the details required to plan and execute test events to meet the LRASM C-3 early operational capability (EOC) in 4QFY26.

MISSION

Combatant commanders will use units equipped with LRASM to destroy adversary ships from standoff ranges.

PROGRAM

OASuW Increment 1 is an Acquisition Category IC program. It began as an accelerated acquisition program to procure a limited number of air-launched missiles in response to a U.S. Pacific Fleet urgent operational need generated in 2008. The program leveraged the near-term Defense Advanced Research Projects Agency (DARPA)'s LRASM initiative as the weapon system for OASuW Increment 1. DOT&E approved the LRASM 1.1 MTS in January 2020, in lieu of a TEMP. In 2QFY23, the Navy announced the intention to field LRASM 1.1, following FY22 IT events but before conducting the IOT&E. DOT&E published a classified early fielding report in April 2023, and the Navy fielded LRASM 1.1 in November 2023. DOT&E will publish a classified LRASM 1.1 combined IOT&E and LFT&E report at the completion of OT flights, M&S, and cyber survivability testing in FY25 to inform continual fielding.

The LRASM C-3 program was delayed by expanded program scope and does not plan to conduct integrated developmental/operational weapon employment testing until 1QFY26, with EOC planned for 4QFY26. The Navy continued drafting the LRASM C-3 MTS in FY24.

OASuW Increment 2 is intended to deliver anti-surface warfare capabilities to counter future threats. The DoD continues to plan for the development of OASuW Increment 2 via full and open competition, with EOC anticipated in FY29 and initial operational capability anticipated in FY31. The Navy funded LRASM C-3 to bridge the gap in capability against predicted threats until an OASuW Increment 2 program of record is established. The C-3 upgrade is intended to incorporate missile hardware and software improvements to address component obsolescence and increase missile range and targeting capabilities.

» MAJOR CONTRACTOR

- Lockheed Martin Missiles and Fire Control – Orlando, Florida

TEST ADEQUACY

The start of LRASM 1.1 dedicated OT activity was delayed due to hardware production delays. However, the Navy proceeded with IT events in accordance with the DOT&E-approved MTS. The IOT&E plan was not ready for DOT&E approval before collection of IOT&E data began in July 2024. An IOT&E test plan for DOT&E approval is expected in 1QFY25.

IOT&E data collection began in July 2024 and will continue into early FY25 after DOT&E approval of the IOT&E plan. IOT&E is composed of weapon employment test events, including one with a live warhead, M&S-based test events, and cyber survivability test events. Weapon employment test events have occurred under benign environmental and threat conditions thus far; M&S events simulated more realistic conditions not easily replicated in live-range environments. Future open-air test events should include increased threat realism to the extent practicable to provide better validation data for the M&S tools. DOT&E will publish a classified combined IOT&E and LFT&E report in FY25 after operational flight, cyber survivability, and M&S tests are complete.

In March 2024, the Navy completed one IT event and engaged a moving maritime target with a salvo of four LRASM 1.1 free-flight evaluation missiles employed from F/A-18F aircraft. Three of the four missiles had undergone suitability testing on an aircraft carrier in FY23. In July 2024, the Navy conducted an OT event with an LRASM 1.1 All-Up Round employed from an F/A-18F aircraft against a maritime target. In FY24, the Navy continued development of the M&S environment and completed two M&S IT events.

The Navy continued to develop the LRASM C-3 MTS and OT plan in FY24. The Navy completed the missile concept of operations and system requirements during FY23, focusing on anti-surface warfare employment range and updating the missile target threat library compared to LRASM 1.1. The Navy should continue to work with DOT&E to develop and execute an adequate OT plan to support EOC in 4QFY26.

PERFORMANCE

» EFFECTIVENESS

Insufficient data are available for an assessment of the operational effectiveness of LRASM 1.1. However, FY24 test results show that LRASM 1.1 can successfully impact the target under the benign conditions used during the integrated flight test. Operational effectiveness will be assessed in the FY25 combined IOT&E and LFT&E report, once testing and data analysis are complete.

» LETHALITY

Testing accomplished in July 2024 focused on evaluating the lethality of LRASM 1.1, but the required data were not collected due to test instrumentation issues. DOT&E will assess lethality in the FY25 combined IOT&E and LFT&E report, once testing and data analysis are complete.

» SUITABILITY

Insufficient data are available for an assessment of the operational suitability of LRASM 1.1. DOT&E will provide an assessment of operational suitability in the FY25 combined IOT&E and LFT&E report, once testing and analysis are complete.

» SURVIVABILITY

Cyber survivability testing is scheduled for FY25. DOT&E will assess operational survivability in the FY25 combined IOT&E and LFT&E report, once testing and analysis are complete.

RECOMMENDATIONS

As recommended in the FY23 Annual Report, the Navy should:

1. Complete development, verification, validation, and accreditation of the M&S environment to facilitate the evaluation of LRASM 1.1.
2. Complete development of the LRASM C-3 MTS and OT plan and submit both for DOT&E approval.

Additionally, the Navy should:

1. Submit for DOT&E approval an LRASM 1.1 IOT&E and LFT&E plan that includes operationally representative open-air scenarios and environments.
2. Complete LRASM 1.1 IOT&E to support continual fielding.
3. Include an end-to-end LRASM C-3 lethality test event to collect lethality data the Navy failed to acquire from the LRASM 1.1 event in July 2024.

Over-The-Horizon Weapon System (OTH-WS)

In July 2024, the Navy conducted an IOT&E flight test of the Over-The-Horizon Weapon System (OTH-WS) as part of a biennial fleet exercise, Rim of the Pacific 2024. No lethality tests were conducted in FY24. In June 2024, the Navy reported that the program is unfunded to conduct the remaining IOT&E flight and LFT&E tests, including six arena tests, five sled tests, and modeling and simulation (M&S) required to determine missile lethality and survivability within a contested environment.

SYSTEM DESCRIPTION

The OTH-WS is a standalone system providing surface-to-surface missile capability that the Navy intends to defeat maritime targets inside and beyond the firing unit's radar horizon. The Navy employs the OTH-WS on the *Independence*-class littoral combat ship with plans to employ it from the *Arleigh Burke*-class guided missile destroyer and the *Constellation*-class guided missile frigate. The OTH-WS requires minimal integration with the host platform and consists of an operator interface console, the Naval Strike Missile (NSM), and a missile launching system. The OTH-WS receives targeting data via tactical communications from combatant platforms or airborne sensors and requires no firing unit support after launch.

MISSION

The joint force commander/strike group commander employs OTH-WS-equipped platforms to conduct offensive over-the-horizon and within-the-horizon engagements against maritime targets. The U.S. Marine Corps intends to employ NSMs from the Joint Light Tactical Vehicle mobile launch platform as a component of a Navy/Marine Expeditionary Ship Interdiction System (NMESIS).

PROGRAM

OTH-WS is an Acquisition Category II, Non-Developmental Item program. The integrator of the OTH-WS onto Navy platforms is Raytheon Missile and Defense (now known as Raytheon). The Navy is conducting OT&E and LFT&E in accordance with a test plan approved by DOT&E in March 2021 and a TEMP approved in May 2023; however, operational tests and LFT&E events were delayed due to funding shortfalls and test asset reallocation to support the Marine Corps NMESIS project.

» MAJOR CONTRACTORS

- Raytheon, a subsidiary of RTX – Tucson, Arizona
- Kongsberg Defence and Aerospace – Kongsberg, Norway

TEST ADEQUACY

In July 2024, the Navy conducted one of two remaining IOT&E flight tests during a fleet exercise, Rim of the Pacific 2024, in accordance with the DOT&E-approved test plan and with DOT&E observation. The final flight test was completed in September 2024 in Andøya, Norway; DOT&E signed a Reciprocal Use of Test Facilities with Norway in April 2024. Contributing to delays in completion of IOT&E of OTH-WS was the reallocation of test resources for flight tests in FY22 to support the Marine Corps NMESIS project.

No lethality tests were conducted in FY24. Six of seven requisite arena tests and five of six requisite sled tests to characterize the OTH-WS warhead lethality remain unscheduled due to lack of funding. Determination of missile lethality is required by DOT&E to complete our assessment. In June 2024, the Navy reported that the program remains unfunded to conduct the remaining LFT&E tests to assess missile lethality and survivability within a contested environment.

DOT&E evaluation of the July 2024 flight test, previous year flight tests, and the flight integration tests of the NSM with a Joint Light Tactical Vehicle-based mobile launch platform discussed in the FY23 Annual Report, remain in progress, but are not adequate to determine operational effectiveness and suitability due to IOT&E being incomplete.

As reported in the FY23 Annual Report, cyber survivability testing was adequate to assess the resilience of the OTH-WS to cyber-attack when employed on a Littoral Combat Ship.

PERFORMANCE

» EFFECTIVENESS AND LETHALITY

Insufficient data are available to determine lethality and operational effectiveness of the OTH-WS. The three live fire tests in FY21 demonstrated that the OTH-WS has potential to provide the Navy with an over-the-horizon capability to defeat surface ships. However, the Navy has not fully characterized this capability. Remaining arena tests, sled tests, and lethality M&S are needed to characterize the lethality of OTH-WS against threat-representative targets. Moreover, the Navy completed verification and validation of their lethality assessment simulation but has yet to accredit it. DOT&E will report OTH-WS operational effectiveness, including lethality, after the completion of remaining operational and lethality test events.

» SUITABILITY

Insufficient data are available to determine operational suitability of the OTH-WS due to remaining IOT&E events. DOT&E will report OTH-WS operational suitability after the completion of remaining operational test events.

» SURVIVABILITY

Assessment from the Navy's cyber survivability evaluation in May 2022 is classified. DOT&E will report on the cyber survivability of the OTH-WS after the completion of IOT&E.

RECOMMENDATION

The Navy should:

1. Fund and schedule the arena tests, sled tests, and M&S runs for adequate evaluation of OTH-WS.

Ship Self-Defense System (SSDS) Mk 2 Integrated Combat Systems

Clockwise from top left: SSDS Mk 2 Mod 3 on LHD 8; Mod 6 on CVN 78; Mod 5 on LSD 51; Mod 2 on LPD 20; Mod 4 on LHA 6; and Mod 1 on CVN 68

Between February and March 2024, the Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted cyber survivability testing of Mod 6 of the Ship Self-Defense System (SSDS) Mk 2 Baseline 10 aboard USS *Gerald R. Ford* (CVN 78). OPTEVFOR expects to complete cyber survivability evaluation and continue operational test of Mod 6 with at-sea tests for cyber survivability and a live fire demonstration against anti-ship cruise missile (ASCM) targets aboard CVN 78 in FY25. The Navy did not conduct the remaining operational tests for Mod 5 of SSDS Mk 2 Baseline 10 in FY24. The Navy continued development of SSDS Mk 2 Baseline 12 in FY24 and expects to commence operational test in FY27.

SYSTEM DESCRIPTION

SSDS Mk 2 is the command and control system aboard amphibious ships and aircraft carriers. It comprises a local area network with processors that host tactical programs, and interfaces to external systems. SSDS Mk 2 integrates the following systems: horizon search radars (i.e., SPQ-9B and SPY-3), volume search radars (i.e., SPS-48, SPS-49, SPY-4, and SPY-6), MK 9 tracker illuminator system for Evolved Sea Sparrow Missile (ESSM), SLQ-32 electronic warfare system, Cooperative Engagement Capability (CEC) sensor fusion and netting system, ESSM and Rolling Airframe Missile (RAM) launchers, and Close-In Weapon System 20mm Gatling gun. SSDS includes operator workstations that display real-time tactical information.

SSDS Mk 2 has six variants referred to as mods. Each mod represents the integration of a unique set of sensors and self-defense weapon systems for a specific ship class.

1. Mod 1 on *Nimitz*-class aircraft carriers (CVN 68 class)
2. Mod 2 on *San Antonio*-class amphibious transport dock ships (LPD 17 class)
3. Mod 3 on *Wasp*-class landing helicopter dock ships (LHD 1 class)
4. Mod 4 on *America*-class landing helicopter assault ships (LHA 6 class)
5. Mod 5 on *Whidbey Island*-class and *Harpers Ferry*-class dock landing ships (LSD 41 and LSD 49 classes)
6. Mod 6 on *Ford*-class aircraft carriers (CVN 78 class)

SSDS Mk 2 capability improvements are delivered via software and hardware baselines within each mod. Individual ships in a class may have different SSDS software and hardware baselines, but they have the same SSDS mod. Most SSDS-based ships have baselines up to and including SSDS Mk 2 Baseline 10. The Navy is developing SSDS Mk 2 Baseline 12, which includes major changes to engagement doctrine and weapon scheduling algorithms intended to improve ship survivability.

MISSION

Navy commanders use SSDS Mk 2 for timely engagement of ASCM threats, aircraft, and unmanned aerial vehicles to defend their ships. Moreover, SSDS Mk 2 contributes to the commander's tactical picture during air, surface, amphibious, and undersea warfare missions by combining participating units' sensor data into a real-time composite target track picture of the battlespace.

PROGRAM

SSDS Mk 1 achieved Milestone C in 1998. In 2005, the Navy transitioned to SSDS Mk 2. SSDS Mk 2 is an Acquisition Category IC program. The Navy completed testing of the Mods 2, 3, and 4 of SSDS Mk 2 prior to May 2018, when DOT&E approved Revision C of the SSDS Mk 2 TEMP. That revision included operational tests of Mod 1 of SSDS Mk 2 (an untested capability demonstrating force-level interoperability), Mod 5 of SSDS Mk 2 Baseline 10 on LSD 41 and LSD 49 classes, and Mod 6 of SSDS Mk 2 Baseline 10 on CVN 78.

The Navy continues to develop the Air Warfare Ship Self-Defense Enterprise TEMP 1910, which also serves as the SSDS Mk 2 Baseline 12 TEMP for all mods, except Mod 5, which the Navy currently does not have identified for upgrade to Baseline 12. The Navy plans to start operational testing of SSDS Mk 2 Baseline 12 in FY27 using the Navy's Self-Defense Test Ship.

» MAJOR CONTRACTORS

- Lockheed Martin Corporation – Bethesda, Maryland
- Raytheon, a subsidiary of RTX – Arlington, Virginia

TEST ADEQUACY

Between February and March 2024, OPTEVFOR conducted cyber survivability testing of Mod 6 of SSDS Mk 2 Baseline 10 aboard USS *Gerald R. Ford* (CVN 78), in accordance with a DOT&E-approved test plan and with DOT&E observation. The test occurred with CVN 78 pierside and was informed by results from the land-based test site evaluation detailed in the FY23 Annual Report. OPTEVFOR intends to complete cyber survivability testing of Mod 6 of SSDS Mk 2 Baseline 10 from the CVN 78 when it is underway in FY25.

The Navy conducted no additional operational test of SSDS Mk 2 Baseline 10 in FY24. The demonstration of force-level interoperability that had been planned in conjunction with Mod 1 of SSDS Mk 2 testing will instead be conducted with Mod 6 of SSDS Mk 2 Baseline 12, per the drafted TEMP 1910. DOT&E concurs that the intent of this test can be met with Mod 6. Remaining operational test requirements for SSDS Mk 2 Baseline 10 include:

- Mod 5 – Eight of nine test events outlined in the 2018 SSDS TEMP have yet to be conducted. The Navy has not scheduled this testing.
- Mod 6 – DOT&E agreed to a reduction of live fire test events aboard CVN 78 against ASCM targets, due to changes in employment of the ship's defense missiles that – combined with test restrictions – prevent collecting some originally intended data. The Navy expects to complete the remaining shipboard test events in FY25. Adequate evaluation of the Mod 6 capability requires runs from the CVN 78 Probability of Raid Annihilation modeling and simulation (M&S) test bed. The Navy requires live fire test events from CVN 78 in FY25 to complete verification, validation, and accreditation (VV&A) of the test bed. Furthermore, 10 live fire test events in the DDG 1000 *Zumwalt*-class IOT&E Strategy that were intended to support VV&A of the AN/SPY-3 radar performance modeled in the CVN 78 test bed cannot be used due to modifications made to the DDG 1000 AN/SPY-3 radar system that no longer make it representative for Mod 6 performance evaluation. The loss of these data may prevent a complete determination of the operational effectiveness of the Mod 6 self-defense capability against ASCMs.

In December 2023 and March 2024, the Navy conducted two land-based developmental test (LBDT) events of SSDS Mk 2 Baseline 12 in the Mod 6 and Mod 4 configurations at the Surface Combat Systems Center in Wallops Island, Virginia. The Navy intends to conduct sea-based developmental test of SSDS Mk 2 Baseline 12 in the Mod 2 configuration on USS *Richard M. McCool Jr.* (LPD 29) in early FY25 and commence operational testing of the SSDS Mk 2 Baseline 12 in FY27.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

No data were collected in FY24 that would change previously provided assessment of operational effectiveness and suitability for Mods 1 and 5 of SSDS Mk 2 Baseline 10.

Insufficient data are available to determine the operational effectiveness of Mod 6 of SSDS Mk 2 Baseline 10 against ASCMs, or change preliminary assessments detailed in the classified USS *Gerald R. Ford* (CVN 78) reports of April 2022 and April 2023. DOT&E will report operational effectiveness and suitability of Mod 6 of SSDS Mk 2 Baseline 10 after completion of IOT&E that the Navy expects to occur in FY26.

SSDS Mk 2 Baseline 12 remains in development, so no assessment of operational effectiveness and suitability can be made.

» SURVIVABILITY

No data were collected in FY24 that would change previously provided assessment of survivability for Mods 1 and 5 of SSDS Mk 2 Baseline 10.

Insufficient data are available to assess cyber survivability of Mod 6 of SSDS Mk 2 Baseline 10 on CVN 78. DOT&E will address Mod 6 of SSDS Mk 2 Baseline 10 cyber survivability in a CVN 78 report, after completion of at-sea evaluation that the Navy expects to occur in FY25.

SSDS Mk 2 Baseline 12 remains in development, so no assessment of cyber survivability can be made.

RECOMMENDATIONS

As recommended in the FY23 Annual Report, the Navy should:

1. Address all recommendations for Mod 6 of SSDS Mk 2 Baseline 10 performance

in the classified USS *Gerald R. Ford* (CVN 78) reports of April 2022 and April 2023.

2. Complete Mod 5 of SSDS Mk 2 Baseline 10 testing to characterize ship self-defense performance of LSD 49 ship class.

Additionally, the Navy should:

3. Complete remaining anti-air warfare testing aboard CVN 78 to support demonstration of capability of Mod 6 of SSDS Mk 2 Baseline 10 against surrogate threat ASCMs.
4. Complete development and VV&A of the CVN 78 Probability of Raid Annihilation M&S suite in FY25, to support assessment of Mod 6 of the SSDS Mk 2 Baseline 10.
5. Complete development of and submit to DOT&E for approval in FY25, the Air Warfare Ship Self-Defense Enterprise TEMP 1910 for operational testing of SSDS Mk 3 Baseline 12 including a force-level interoperability test for Mod 6.
6. Complete an at-sea cyber survivability evaluation onboard CVN 78 in FY25 to assess Mod 6 of SSDS Mk 2 Baseline 10 resilience to cyber-attack.
7. Validate with operational testing the correction of Mods 1 and 3 of SSDS Mk 2 Baseline 10 integration issues discussed in the FY22 Annual Report.

Ship to Shore Connector (SSC)

In FY24, the Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted no OT&E or LFT&E events on the Ship to Shore Connector (SSC) due to continued program effort to improve vessel reliability and availability. The Navy deferred the IOT&E and remaining work on the SSC survivability assessment from FY24 to FY25.

SYSTEM DESCRIPTION

The SSC is a fully amphibious air cushion vehicle similar to the currently in-service Landing Craft, Air Cushion (LCAC). Compared to the LCAC, the SSC is intended to have increased payload, availability, and the ability to operate in a greater range of environmental conditions.

MISSION

Navy commanders will use the SSC to provide ship-to-shore transport of forces conducting a Ship-To-Objective Maneuver. The SSC system is expected to bridge the gap of brigade-sized maneuver and operations capability after the retirement of the LCAC at the end of its service life.

PROGRAM

The SSC is an Acquisition Category IC major capability acquisition program. The Navy approved Milestone C in July 2015. The SSC Program Office took delivery of the first test and training craft in February 2020. DOT&E approved the SSC program TEMP in November 2021 and the IOT&E test plan in November 2022.

In FY24, the program office continued efforts to correct the vessel reliability and availability issues that had prevented commencing IOT&E in December 2022, and that are detailed in the FY23 Annual Report. Although the Navy had expected to commence IOT&E in FY24, these efforts have further delayed IOT&E start to FY25. Moreover, the Navy now expects to complete analysis of SSC survivability in the presence of threat mines using mine susceptibility modeling and simulation in FY25.

» MAJOR CONTRACTOR

- Textron Systems – New Orleans, Louisiana

TEST ADEQUACY

In FY24, OPTEVFOR conducted no OT&E or LFT&E events on the SSC due to continued program effort to improve vessel reliability and availability. Cyber survivability testing and LFT&E previously conducted between 2018 – 2023 will be reviewed against vessel modifications to determine if any test data are invalidated by the modifications and require additional test.

In FY24, the program office prioritized their efforts on the correction of vessel reliability and availability issues and thus delayed verification, validation, and accreditation of SSC vulnerability assessment models, as well as the final survivability assessment report, to FY25. The final survivability assessment report will detail SSC mine susceptibility and final predictions for the probability of kill given hit to the SSC by threat weapons.

PERFORMANCE

» EFFECTIVENESS

No data are available to determine operational effectiveness of the SSC. DOT&E will report operational effectiveness after completion of IOT&E that the Navy expects to occur in FY25.

» SUITABILITY

SSC reliability did not support conducting the planned operational test in FY23 or FY24. Insufficient test data are available to determine operational suitability of SSC or confirm reliability improvement from SSC vessel modifications made since FY23. DOT&E will report operational suitability after completion of IOT&E that the Navy expects to occur in FY25.

» SURVIVABILITY

DOT&E will report the cyber survivability of SSC, and SSC platform survivability to threat weapons, after completion of IOT&E that the Navy expects to occur in FY25.

RECOMMENDATIONS

The Navy should:

1. Verify SSC reliability supports operational test prior to commencing IOT&E. Correction of reliability issues should be confirmed with representative SSC operations as recommended in the FY23 Annual Report.

2. Complete verification, validation, and accreditation of SSC vulnerability assessment models in early FY25 to support timely completion of the final survivability assessment report as recommended in the FY23 Annual Report.

Standard Missile 2 (SM-2) Block IIIC and Block IIICU

In March 2024, DOT&E delivered an early fielding report (EFR) for the Standard Missile 2 (SM-2) Block IIIC that detailed demonstrated operational capability of the delivered rapid prototype. Subsequently, the Navy fielded the SM-2 Block IIIC in 4QFY24. The Navy plans IOT&E of the follow-on variant, SM-2 Block IIICU, in FY31.

SYSTEM DESCRIPTION

The SM-2 Block IIIC and Block IIICU are medium-range, surface-to-air missiles with active radio frequency seekers. Both missiles are modifications to legacy SM-2 Block III/IIIA/IIIB missiles. The most significant modification is replacement of the legacy semi-active missile seeker with a dual-mode semi-active and active missile seeker based on SM-6 Block I technology. The SM-2 Block IIIC and Block IIICU have a new dorsal fin design and a thrust vectoring jet tab assembly that control trajectory as the missile egresses the launcher.

The Navy's Guidance Section Electronics Unit (GS EU) replacement program is making hardware changes to the SM-6 Block IA Guidance Section and Target Detection Device to address obsolescence issues. The upgraded GS EU will be qualified on the SM-6 Block IA missile as the SM-6 Block IAU. Integration of the upgraded GS EU on the SM-2 Block IIIC results in the SM-2 Block IIICU.

MISSION

The joint force commander will use SM-2 Block IIIC and Block IIICU missiles from *Arleigh Burke*-class and *Constellation*-class ships to provide medium-range air defense, both self-defense and area air defense, against anti-ship cruise missiles and tactical aircraft. The joint force commander will use SM-2 Block IIIC and Block IIICU missiles in Naval Integrated Fire Control – Counter Air engagements from ships with this capability.

PROGRAM

The SM-2 Block IIIC was developed as a Middle Tier of Acquisition program for rapid prototyping. The Navy fielded the SM-2 Block IIIC in 4QFY24. This decision was informed by DOT&E's classified EFR submitted March 2024.

The Navy plans acquisition program baseline approval for the SM-2 Block IIICU as an Acquisition Category II program on the major capability acquisition pathway, post Milestone B, in FY25. DOT&E approved the SM-2 Block IIICU Milestone B TEMP in January 2024. SM-2 Block IIICU IOT&E is planned to commence in FY31. There are no changes to the legacy warhead or fusing method used on the SM-2 Block IIIC and Block IIICU missile. However, the packaging of the warhead within a modified airframe should be assessed by the Navy with analysis provided to DOT&E.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX – Tucson, Arizona

TEST ADEQUACY

In March 2024, the Navy's Operational Test Force accredited modeling and simulation for operational assessment of the SM-2 Block IIIC, specifically for general missile performance characterizations and identifying operational risks. The results of the missile performance study, the cyber risk assessment reported in the FY23 Annual Report, and the live fire test events reported in the FY22 Annual Report informed DOT&E's EFR. Testing supported operational demonstration of SM-2 Block IIIC but not determination of operational effectiveness, operational suitability, or cyber survivability.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Operational effectiveness, suitability, and survivability observations are provided in the classified EFR.

RECOMMENDATION

The Navy should:

1. Assess the effect of missile airframe modifications on SM-2 Block IIICU lethality and provide associated analysis to DOT&E as recommended in the EFR and the FY23 Annual Report.

Standard Missile-6 (SM-6) Family of Missiles

In March 2024, a Standard Missile-6 (SM-6) Block IA variant was used in the Missile Defense Agency's Flight Test Aegis Weapon System-32 (FTM-32) event. FTM-32 demonstrated capability to detect, track, engage, and intercept a Medium Range Ballistic Missile (MRBM) target. Details are in the Missile Defense System (MDS) article in this Annual Report and the classified DOT&E MDS Annual Assessment, planned for February 2025. No additional testing of the SM-6 occurred in FY24.

SYSTEM DESCRIPTION

SM-6 is a missile that can defeat a range of targets, including air, surface, and land targets. The SM-6 seeker and terminal guidance electronics derive from technology developed in the Advanced Medium-Range Air-to-Air Missile program, discussed in a separate article in this Annual Report. SM-6 receives midcourse flight control from the Aegis Weapon System (AWS) via the ship's radar.

Current SM-6 variants include Block I and Block IA to deliver over-the-horizon anti-air warfare, anti-surface warfare, strike, and ballistic missile defense capabilities. The Navy is developing the SM-6 Block IB variant – a modification of the Block IA missile – to extend its engagement range.

MISSION

The joint force commander/strike group commander employs naval units equipped with the SM-6 to conduct defensive and offensive operations. Missions include: (1) fleet air defense against fixed and rotary-winged aircraft and anti-ship missiles operating at altitudes ranging from very high to sea-skimming, (2) extended range, over-the-horizon anti-surface capability, (3) overland air-defense as a component of the integrated fire control concept, and (4) sea-based capability against short- and medium-range ballistic missiles in their terminal phase of flight.

PROGRAM

SM-6 is an Acquisition Category (ACAT) IC program. SM-6 Block I and Block IA are beyond Milestone C. The Navy transitioned Block IB from a Middle Tier of Acquisition program to the SM-6 ACAT IC program in November 2021. The Navy provided a Block IB Milestone B TEMP to DOT&E for approval in FY23 but retracted it later that year due to the Navy reexamining the acquisition pathway and variant end state. The Navy is developing an update to the Guidance Section Electronics Unit to mitigate obsolescence issues and intends to incorporate the update into the missile as part of the SM-6 Block IA upgrade, or Block IAU. No new capabilities are planned.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX – Tucson, Arizona

TEST ADEQUACY

The Navy did not conduct SM-6 operational test nor submit operational test plans for DOT&E approval. However, the Navy included DOT&E and the Navy's Operational Test Force during test planning and test observation in the SM-6 Missile Defense Agency's FTM-32 event in March 2024. Additional information can be found in the MDS article in this Annual Report and the classified DOT&E MDS Annual Assessment, planned for February 2025. FTM-32 demonstrated capability of SM-6 to detect, track, engage, and intercept a MRBM target in the terminal phase of flight but was not intended to determine the operational effectiveness, lethality, suitability, or survivability of the SM-6.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

Use of the SM-6 during the FTM-32 event does not affect DOT&E's prior assessments of SM-6 variants. Evaluation of SM-6 Block IB operational effectiveness, lethality, suitability, and survivability will be reported upon completion of operational and live fire testing.

RECOMMENDATIONS

The Navy should:

1. Address the recommendations from the FY22 Annual Report.
2. Submit a Block IB test strategy to DOT&E for approval.

Surface Electronic Warfare Improvement Program (SEWIP) Block 2

Between February and March 2024, the Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted cyber survivability evaluation of the AN/SLQ-32B(V)6 variant of Surface Electronic Warfare Improvement Program (SEWIP) Block 2 on USS *Gerald R. Ford* (CVN 78). OPTEVFOR conducted no operational testing of effectiveness and suitability of any variant of SEWIP Block 2 in FY24 and now expects to complete FOT&E in FY25. The completion of FOT&E has been delayed three years due to limited ship and test resource availability.

SYSTEM DESCRIPTION

SEWIP Block 2 is an electromagnetic warfare system that detects, identifies, and tracks threat anti-ship missiles and targeting radars. SEWIP Block 2 incorporates a new antenna system, enhanced processing capabilities, and the SEWIP Block 1B3 High Gain High Sensitivity antenna and associated hardware to improve battlefield situational awareness. Some variants of SEWIP Block 2 incorporate additional software, known as the Soft Kill Coordination Subsystem, to improve combat system integration with non-kinetic effects, such as decoys, to defeat aerial threats.

MISSION

Navy commanders use SEWIP Block 2 to perform anti-ship missile defense (ASMD), counter-targeting, and counter-surveillance, as do earlier versions of the AN/SLQ-32 electronic warfare system. SEWIP Block 2 further upgrades the electromagnetic support capabilities and integrates more closely with the combat system to improve ASMD against emerging threats.

PROGRAM

SEWIP Block 2 is an Acquisition Category II program that achieved Milestone C in January 2013. SEWIP Block 2 completed IOT&E in FY16 and the Navy approved full-rate production in September 2016. SEWIP Block 2 has three variants, each of which have distinct hardware and software suites:

- AN/SLQ-32(V)6 on *Arleigh Burke*-class destroyers with the Aegis Combat System.
- AN/SLQ-32A(V)6 on *Zumwalt*-class destroyers.
- AN/SLQ-32B(V)6 on USS *Gerald R. Ford* (CVN 78).

SEWIP Block 2's FOT&E addresses the following:

- System upgrades since IOT&E.
- Integration of each SEWIP Block 2 variant with its corresponding combat system: the Aegis Combat System on the *Arleigh Burke*-class, the Total Ship Computing Environment (TSCE) combat system on the *Zumwalt*-class, and the Ship Self-Defense Combat System (SSDS) on the *Gerald R. Ford*-class.
- Combat system integration and decoy integration capabilities of the Soft Kill Coordination Subsystem for the variant fielded on *Arleigh Burke*-class destroyers with the Aegis Combat System.

DOT&E has approved the following test plans:

- AN/SLQ-32(V)6 operational test plan in October 2024.
- AN/SLQ-32A(V)6 operational test plan in July 2023.
- DDG 1000 cyber survivability test plan that included test of AN/SLQ-32A(V)6 in November 2022.
- CVN 78 cyber survivability test plan that included test of AN/SLQ-32B(V)6 in February 2024.

The Navy expects to deliver the cyber survivability test plan in early FY25 for Aegis Advanced Capability Build 16 Baseline 9.C2.3 that will include cyber survivability of AN/SLQ-32(V)6. DOT&E will submit a classified FOT&E report, after SEWIP Block 2 FOT&E, which the Navy expects to complete in FY25.

» MAJOR CONTRACTOR

- Lockheed Martin Corporation – Syracuse, New York

TEST ADEQUACY

Between February and March 2024, OPTEVFOR conducted cyber survivability testing of AN/SLQ-32B(V)6 aboard USS *Gerald R. Ford* (CVN 78), in accordance with a DOT&E-approved test plan and with DOT&E observation. The test occurred with CVN 78 pierside and was informed by the land-based test site evaluation detailed in the FY23 Annual Report. The shipboard testing was adequate to evaluate the cyber survivability of AN/SLQ-32B(V)6.

OPTEVFOR will use results from the AN/SLQ-32B(V)6 cyber survivability testing, cyber survivability testing of AN/SLQ-32A(V)6 detailed in the FY23 Annual Report, and AN/SLQ-32(V)6 system scans during *Arleigh Burke*-class destroyer platform testing in FY25, to complete cyber survivability evaluation of SEWIP Block 2. As documented in the FY21 Annual Report, the cyber survivability test of AN/SLQ-32(V)6 was expected to be conducted in 1QFY23, but it has been repeatedly delayed due to *Arleigh Burke*-class destroyer availability.

The Navy conducted no operational test to determine effectiveness and suitability of any of the SEWIP Block 2 variants in FY24 due to limited ship and test resource availability. The Navy now plans to complete the remaining test events for AN/SLQ-32(V)6 and AN/SLQ-32A(V)6, and end FOT&E of SEWIP Block 2, in FY25. OPTEVFOR completed operational testing of AN/SLQ-32B(V)6 in FY21. Adequate evaluation of SEWIP

Block 2 depends on data from AN/SLQ-32(V)6 (*Arleigh Burke*-class destroyers) and AN/SLQ-32A(V)6 (*Zumwalt*-class destroyers) test events in a comprehensive and complex electromagnetic spectrum environment.

SEWIP Block 2 FOT&E has included additional threat stimulators from those available in IOT&E. However, several stressing threats that the system could encounter remain unavailable for test. The Navy has yet to fund required programming of these threats within threat emulators for test.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Insufficient data are available to determine operational effectiveness and suitability of SEWIP Block 2 due to outstanding FOT&E test events. DOT&E will deliver a classified report on SEWIP Block 2 operational effectiveness and suitability after testing that the Navy expects to complete in FY25.

» SURVIVABILITY

Insufficient data are available to determine cyber survivability of SEWIP Block 2 due to outstanding testing on AN/SLQ-32(V)6. DOT&E will deliver a classified report for SEWIP Block 2 cyber survivability after testing that the Navy expects to complete in FY25.

RECOMMENDATIONS

The Navy should:

1. As recommended since the FY21 Annual Report, fund the programming of more stressing threats within threat stimulators and incorporate them into remaining SEWIP Block 2 test events as they become available.
2. Schedule and complete remaining tests for operational effectiveness, suitability, and cyber survivability of AN/SLQ-32(V)6 in FY25.
3. Schedule and complete remaining tests for operational effectiveness and suitability of AN/SLQ-32A(V)6 in FY25.

T-AO 205 *John Lewis*-Class Fleet Replenishment Oiler

Between April and November 2024, the Navy's Operational Test and Evaluation Force (OPTEVFOR) continued IOT&E aboard USNS *Harvey Milk* (T-AO 206). The *John Lewis* (T-AO 205)-class has successfully demonstrated capability to deliver fuel and cargo, including vertical replenishment with multiple aircraft types, for supported ship classes tested to date. The Navy plans to provide all required reports for assessment of platform survivability in FY25. The Navy expects to complete T-AO 205 IOT&E in early FY25.

SYSTEM DESCRIPTION

The T-AO 205 *John Lewis*-class of fleet replenishment oilers will replace the 15 ships in the T-AO 187 *Henry J. Kaiser*-class currently in the fleet today. T-AO 205 has port and starboard refueling stations, an astern fuel delivery station, connected cargo transfer stations, and a vertical replenishment station from the flight deck.

The T-AO 205-class has an advanced degaussing system, the Nixie torpedo countermeasure system, and mounts for security team machine guns. The ship has the space and weight reservations for defensive weapons system installation. The T-AO 205-class is designed to commercial standards for a crew of 95 civilian mariners and accommodations for an additional 34 personnel.

MISSION

Combatant commanders will use T-AO 205-class ships to replenish ships within carrier strike groups and expeditionary strike groups during peacetime and combat operations. T-AO 205-class ships will serve as the primary logistics platform, linking Navy ships and embarked aircraft with logistics nodes ashore. The T-AO 205-class ships deliver fuel, food, supplies, and spare parts.

PROGRAM

The T-AO 205-class replenishment oiler is an Acquisition Category IB program that achieved Milestone B/C in September 2017. The Assistant Secretary of the Navy for Research, Development, and Acquisition increased the low-rate initial production (LRIP) to 12 ships in June 2022. The Navy plans a total buy of 20 T-AO 205-class ships.

General Dynamics, National Steel and Shipbuilding Company (NASSCO) delivered T-AO 205 in July 2022, T-AO 206 in July 2023, and T-AO 207 in May 2024. Three ships (T-AO 208 through T-AO 210) are under construction.

DOT&E approved the TEMP Revision 1 in September 2021 and IOT&E test plan in October 2022.

» MAJOR CONTRACTOR

- General Dynamics NASSCO – San Diego, California

TEST ADEQUACY

The Navy evaluated cyber survivability of T-AO 205 in FY23. Testing to assess T-AO 205's cyber survivability posture and the crew's ability to conduct their mission in a cyber-contested environment was conducted in accordance with the DOT&E-approved test plan and observed by DOT&E. Between April 2024 and September 2024, OPTEVFOR conducted IOT&E aboard USNS *Harvey Milk* (T-AO 206) in accordance with the DOT&E-approved test plan and with DOT&E observation. This testing continued IOT&E detailed in the FY23 Annual Report. The Navy expects to complete IOT&E in FY25. Testing could not demonstrate transfer to all ship classes within the IOT&E test design due to their unavailability during test execution, as well as limited T-AO 206 crew manning that could not support one test. Some remaining test events may move to FOT&E after sufficient data are available to determine overall operational effectiveness and suitability.

In September 2024, the Navy provided a verification and validation report for the modeling and simulation (M&S) tool used to predict the vulnerability of the ship to threat weapons. As part of the accreditation of the M&S used in assessing ship survivability, the Navy identified that modeling limitations prevent a representative prediction of damage from underwater weapons. The Navy plans to provide a Total Ship Survivability Trial (TSST) Report in FY25. TSST is a shipboard trial which simulated the damage from weapon events to evaluate the ability of the ship to implement effective damage control and maintain mission capability. TSST was conducted aboard USNS *John Lewis* in July of 2023.

The Navy plans to issue the Final Survivability Assessment Report (FSAR) for T-AO 205 in FY25. The FSAR is a compilation report that details the findings from all T-AO 205 LFT&E tests and analysis over the course of the program, including TSST and predictions from M&S. As identified above, the M&S tool could not be fully accredited for its use in LFT&E analysis.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Insufficient data are available to determine operational effectiveness and suitability of the TAO-205-class. T-AO 205-class has successfully demonstrated the capability to deliver fuel and cargo, including vertical replenishment with multiple aircraft types, to a subset of Navy ship classes within the IOT&E test design. Ship manning has not yet been sufficient to evaluate the most stressing operations for the T-AO 205-class. DOT&E will report operational effectiveness and suitability after completion of IOT&E that the Navy expects to occur in FY25.

» SURVIVABILITY

Analysis of platform survivability is ongoing. The M&S limitations are expected to constrain determination of ship survivability against underwater weapons. However, the findings of the FSAR and associated testing are expected to still support determination of LFT&E critical issues for the T-AO 205-class, including recommendations for potential design improvements for ship survivability against threat weapons. DOT&E will report platform and cyber survivability within a classified IOT&E report after completion of IOT&E that the Navy expects to occur in FY25.

RECOMMENDATION

The Navy should:

1. Complete the remaining IOT&E as soon as feasible in FY25.

Tomahawk Weapon System (TWS)

In FY24, the Navy completed an operational assessment of Tomahawk Weapon System (TWS) upgrades to the Theater Mission Planning Center (TMPC) and the Tactical Tomahawk Weapon Control System (TTWCS). DOT&E anticipates submitting an FOT&E report in 2QFY25. Maritime Strike Tomahawk (MST), a subprogram of TWS, conducted no operational tests or LFT&E in FY24. The Navy conducted some Joint Multi-Effects Warhead System (JMEWS) testing in FY24.

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 major components of the system include the all-up round (AUR) missile, the TTWCS, and the TMPC.

- AUR: Block IV and Block V AURs are conventional Tomahawk missiles with surface and submarine vertical launch capabilities and ground launch capabilities with the U.S. Marine Corps and U.S. Army.
- TTWCS: Provides operator interface to employ the Tomahawk missile.
- TMPC: A shore-based or sea-based mission planning center that provides maritime component commanders the capability to plan, modify and distribute TWS missions.

The MST, currently in development, intends to integrate a maritime seeker into a Block V AUR, designated variant Va. The JMEWS integrates a new multi-stage, insensitive munitions-compliant, warhead into a Block V AUR, designated variant Vb.

MISSION

The joint force commander employs naval units equipped with the TWS for long-range, precision strikes against land targets. MST upgrades are designed to enable the joint force commander to employ the TWS in anti-surface warfare.

PROGRAM

The TWS is an Acquisition Category (ACAT) IC program. The Block V variant completed operational testing in 2021 and is detailed in the classified TWS FOT&E report of October 2021. DOT&E approved Revision I of the TWS TEMP 251-4 in May 2023 to evaluate hardware and software modifications to the TTWCS (TTWCS v5.6.1) and the TMPC (TMPC 6.0.2/7.0.X).

- TTWCS v5.6.1 upgrades support future AUR changes and GPS Military Code (M-code) capability, as well as SSN *Virginia*-class Payload Module implementation.
- TMPC 6.0.0/7.0.x supports AUR land attack capability changes.

The Navy transitioned the MST from the rapid deployment capability acquisition pathway to a subprogram of the TWS program in April 2023. The resultant Block Va variant effort will add a surface warfare capability to the legacy TWS Block V. Contributing to this decision to transition pathways were delays in system development and production, and congressional marks in FY21 and FY22. The Navy has evaluated warhead fuzing and target impact in accordance with the DOT&E-approved LFT&E Strategy but has yet to evaluate warhead lethality against threat-representative ships. The Navy has yet to develop program requirements for MST or provide a TEMP update to DOT&E for approval that includes evaluation of MST.

DOT&E approved the JMEWS LFT&E Strategy in January 2021. The JMEWS, an ACAT III program, is scheduled for Milestone C decision in 1QFY26. Operational testing of JMEWS employed from TTWCS 7.0 and TMPC 8.0 is planned for FY27.

» MAJOR CONTRACTORS

- Raytheon, a subsidiary of RTX – Tucson, Arizona (AUR)
- Lockheed Martin Rotary and Mission Systems – King of Prussia, Pennsylvania (TTWCS)
- Peraton, Inc. – Santa Clara, California (TMPC)
- Tapestry Solutions – St. Louis, Missouri (TMPC)
- BAE Systems – San Diego, California (TMPC)

TEST ADEQUACY

In September 2023 and June 2024, the Navy completed operational test and cyber survivability evaluation of the TTWCS and TMPC upgrades, respectively, in accordance with the DOT&E-approved test plan and with DOT&E observation. The operational assessment consisted of simulated strike group scenario events in laboratory and shipboard environments, a maintenance demonstration, simulated flight tests, and one live flight test of a Block V missile launched from a surface ship. Test data are adequate for regression evaluation of the legacy system capabilities and cyber survivability. DOT&E expects to submit a FOT&E Report in 2QFY25.

In March 2024, the Navy conducted a target sled test using the Supersonic Naval Ordnance Research Track (SNORT) at Naval Air Warfare Center Weapons Division China Lake, in accordance with the DOT&E-approved LFT&E Strategy and with DOT&E observation. Additionally, the Navy has incorporated previously collected LFT&E test data into weaponeering and lethality assessment models for continued assessment of JMEWS lethality against target requirements. The Navy plans a target sled test in FY25 in continuance of the JMEWS LFT&E Strategy to aide in determining lethality of the Block Vb AUR. The Navy expects to commence ground launch flight tests against threat representative targets in FY26 after completion of the JMEWS developmental test program and warhead qualification to support a Milestone C decision.

The Navy conducted no operational tests of MST in FY24.

PERFORMANCE

» EFFECTIVENESS

Analysis of operational test data of the TTWCS and TMPC upgrades is ongoing. DOT&E expects to provide an FOT&E report in 2QFY25. Insufficient data are available to provide assessment on the operational effectiveness of JMEWS or MST.

» SUITABILITY

Analysis of operational suitability data of the TTWCS and TMPC upgrades is ongoing. DOT&E expects to provide an FOT&E report in 2QFY25. Insufficient data are available to provide assessment on the operational suitability of JMEWS or MST.

» LETHALITY

TTWCS and TMPC upgrades do not change AUR lethality. LFT&E data suggest that MST fuzing performs as designed but additional data are required to determine MST lethality against threat-representative ships. Additional data are also required to determine JMEWS lethality.

» SURVIVABILITY

The cyber survivability assessment of the TTWCS and TMPC upgrades is classified. DOT&E expects to provide an FOT&E report in 2QFY25. No data are yet available to determine cyber survivability of MST or JMEWS.

RECOMMENDATIONS

The Navy should:

1. Approve TWS program requirements for MST and provide a TEMP to DOT&E for approval that details its test strategy for operational effectiveness, suitability, lethality, and survivability.
2. Fund and schedule LFT&E of MST to determine lethality against threat-representative ships.
3. Fund follow-on JMEWS T&E efforts to further characterize JMEWS performance and improve weaponeering tools.

VH-92A® Patriot® Presidential Helicopter

In FY24, the Navy received the final delivery of 23 total aircraft procured under the VH-92A program. The Navy conducted a verification of correction of deficiencies (VCD) operational test that focused on Mission Communications System (MCS) improvements. VH-92A® and Patriot® are registered trademarks 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-92A medium lift helicopter. VH-92A replaces the legacy fleet of VH-3D and VH-60N aircraft flown by Marine Helicopter Squadron One (HMX-1) to perform the Presidential Transport mission. The VH-92A is transportable via a single Air Force C-17 cargo aircraft to worldwide locations. The aircraft is equipped with the MCS, which provides simultaneous line-of-sight and beyond line-of-sight, non-secure and secure, voice and data communications to the passengers, to perform senior leader duties. MCS performance is critical to mission success.

MISSION

HMX-1 uses the VH-92A aircraft to conduct administrative lift and contingency operation missions for pre-planned and unscheduled transport of the President of the United States, cabinet members, heads-of-state, and other parties, as directed by the White House Military Office (WHMO). HMX-1 will operate the VH-92A from the White House South Lawn, commercial airports, military airfields, Navy ships, and austere sites throughout the world.

PROGRAM

VH-92A is an Acquisition Category IC program. The Navy procured 23 aircraft: 21 operational aircraft and 2 dedicated engineering development model test aircraft. The U.S. Marine Corps declared initial operational capability for the VH-92A in December 2021, and the VH-92A is now supporting the WHMO Transition Plan assigned tasking. The WHMO Transition Plan stipulates an event-driven, multi-phased approach to replace legacy helicopters with the VH-92As. The final production VH-92A aircraft were delivered in FY24. DOT&E published an FOT&E report in January 2023, based upon FOT&E completed in 4QFY22, that assessed effectiveness, suitability, and cyber survivability, and verified the correction of deficiencies identified during IOT&E conducted in FY21. In FY24, the Navy conducted a VCD operational test that focused on MCS improvements. The program's roadmap has funded modernization planned through FY29. The Navy intends an additional FOT&E to test these future capability improvements, beginning in FY25. The current TEMP, approved by DOT&E in 2015, will require a revision that includes the schedule and resources for this FOT&E.

» MAJOR CONTRACTOR

- Sikorsky Aircraft Corporation, a subsidiary of Lockheed Martin Corporation – Stratford, Connecticut

TEST ADEQUACY

In 2QFY24, HMX-1 conducted a VCD operational test, at the request of the VH-92A Program Office, under the auspices of the Navy's Operational Test and Evaluation Force. The objective of this test was to determine whether an updated MCS software version fixed MCS deficiencies identified during FOT&E in FY22. This MCS software was qualitatively evaluated for operational functionality on two VH-92As through four functionality flights. Although DOT&E provided input to the test plan, this VCD was not part of a formal FOT&E period, nor did it address effectiveness or suitability, therefore DOT&E did not approve the test plan, nor observe testing. DOT&E will not provide an independent assessment of the performance of this MCS version due to the relatively minor capability improvements from the MCS version tested in FOT&E.

PERFORMANCE

» EFFECTIVENESS

VH-92A is operationally effective for all operations based upon IOT&E conducted in FY21 and FOT&E conducted in FY22. DOT&E's assessment of the VH-92A's effectiveness is detailed in the September 2021 IOT&E report and January 2023 FOT&E report. The VCD operational test conducted in FY24 found that 30 open deficiencies had been adequately corrected, 1 has been mitigated through changes to the standard operating procedures, and 1 is no longer applicable due to a WHMO policy change regarding the system design.

» SUITABILITY

VH-92A is operationally suitable for all operations based upon IOT&E conducted in FY21 and FOT&E conducted in FY22. In the January 2023 FOT&E report, DOT&E assessed that VH-92A is a maintenance-intensive aircraft, with maintenance inspections accounting for the majority of maintenance hours. Fleet data indicates the Navy is making progress in this area.

» SURVIVABILITY

DOT&E's assessment of the VH-92A's cyber survivability is detailed in the classified annexes of the

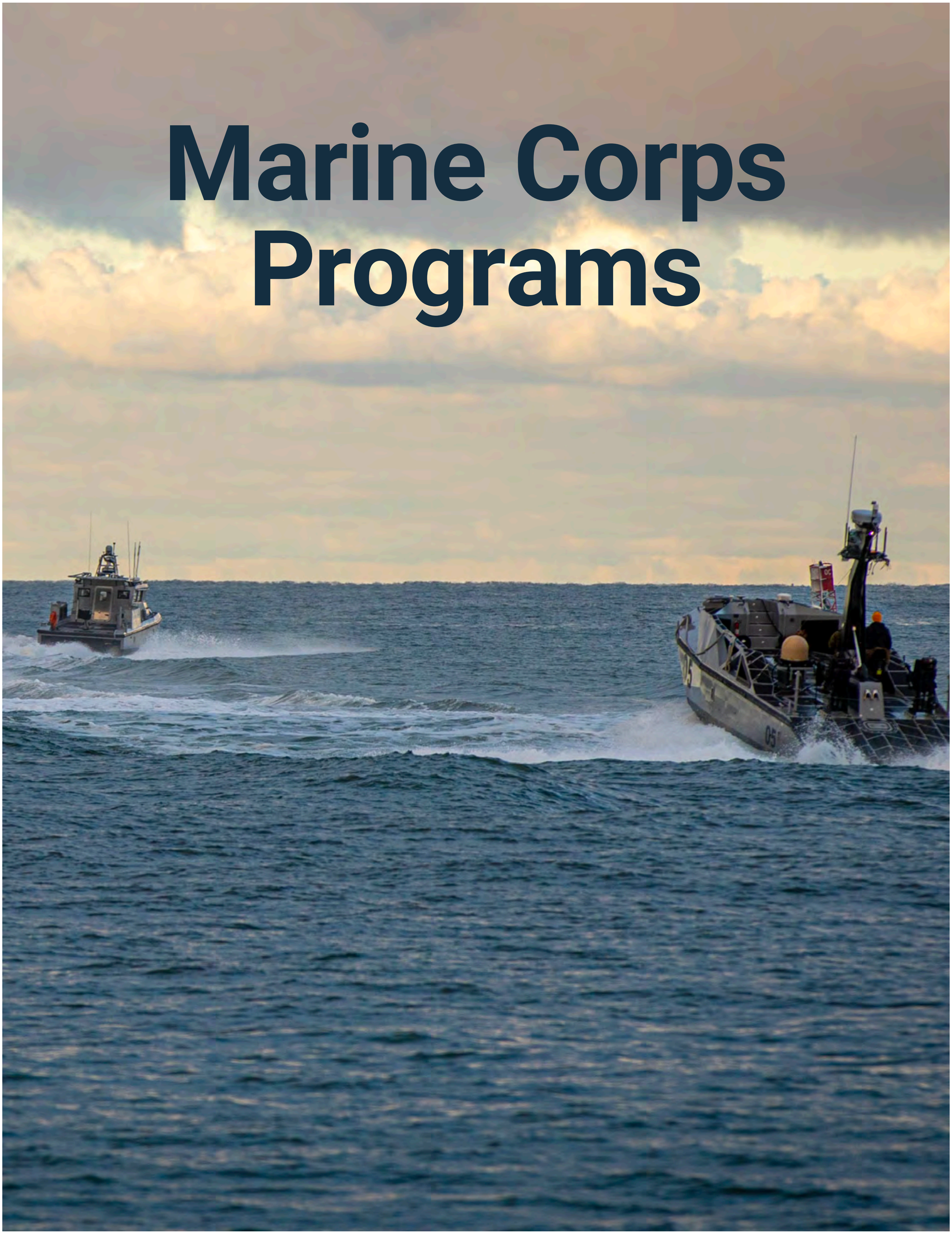
September 2021 IOT&E report and January 2023 FOT&E report.

RECOMMENDATIONS

The Navy should:

1. Continue to address recommendations in the IOT&E report from September 2021, and the FOT&E report from January 2023, as recommended in the FY22 and FY23 Annual Reports.
2. Submit an updated TEMP to DOT&E for approval in FY25 to support future capability upgrades.
3. Conduct FOT&E to assess new capabilities in operationally representative environments.

Marine Corps Programs



This page intentionally left blank.

Long Range Unmanned Surface Vessel (LRUSV)

In May 2024, DOT&E published a classified report on an Early Operational Assessment (EOA) of the Long Range Unmanned Surface Vessel (LRUSV). The Marine Corps terminated the LRUSV Middle Tier of Acquisition program subsequent to the EOA and intends to transition the LRUSV to the major capability acquisition pathway in FY27.

SYSTEM DESCRIPTION

The LRUSV prototype is an unmanned platform capable of traveling semi-autonomously to and from a designated patrol area, where it can then loiter indefinitely (dependent on fuel state) and launch loitering munitions (LMs) and other payloads to strike maritime targets. The LRUSV rapid prototyping program consisted of the following five major sub-systems:

- Unmanned Surface Vessel (USV): powered vessel that can maneuver autonomously, or as directed by a pilot, with capability to launch LMs or small unmanned surface vessels (sUSVs).
- LM System: organic precision fires-mounted loitering munition system with a munition control interface to launch an all-up round against designated maritime targets.

- sUSV: a small USV that can be carried on the rear deck of the LRUSV to provide extended reach to deliver kinetic and non-kinetic effects.
- Command, Control, Communications, and Computers System: integrates the functions of the other required subsystems, enabling USV autonomy and deployment of LMs or sUSVs.
- Contact Vessel: a manned version of the USV that provides sustainment.

MISSION

The Marine Corps and joint force commanders will employ the LRUSV to enhance maritime reconnaissance in support of sea denial and sea control operations. LRUSV supports implementation of the Littoral Operations in a Contested Environment concept, the Expeditionary Advanced Base Operations concept, and emerging doctrine defined by the Marine Corp's Force Design 2030.

PROGRAM

The LRUSV was established as a Middle Tier of Acquisition rapid prototyping program, designated by the Marine Corps in May 2021. The Marine Corps approved the LRUSV Master Test Strategy in November 2021, prior to the program being put on DOT&E oversight. In July 2023, the Marine Corps directed a capability requirement change to refine direction for the next phase of acquisition of the LRUSV. The Marine Corps intends future development of the LRUSV to focus on multi-domain sensor collections in support of the Maritime Reconnaissance Company. In September 2023, the Marine Corps directed the termination of the LRUSV Middle Tier of Acquisition program. The Marine Corps intends to transition the LRUSV to the major capability acquisition pathway at Milestone B in 2QFY27. DOT&E removed the LRUSV program from oversight in March 2024 and expects to return it to oversight upon restoration of the program in FY27.

» MAJOR CONTRACTORS

- Metal Shark – Jeanerette, Louisiana (LRUSV)
- HII – Newport News, Virginia (autonomy systems)

TEST ADEQUACY

In FY23, the Marine Corps conducted an EOA with five prototype LRUSVs, as detailed in the FY23 Annual Report. The EOA was not intended to determine operational effectiveness, suitability, and survivability. The EOA was conducted, and adequate, to provide observation of the LRUSV prototype for future development or acquisition pathway transition. Testing was conducted in accordance with a Marine Corps Operational Test and Evaluation Activity-approved test plan. DOT&E reviewed the test plan, subsequently agreed with it, and observed the test events.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

The EOA provided an operational demonstration of capability of the LRUSV prototype to direct itself to a designated patrol area and fire munitions against simulated maritime targets. The EOA also demonstrated LRUSV capability to autonomously maneuver safely in various navigational scenarios when encountering another surface vessel during transit operations.

Additional effectiveness and suitability observations were provided in the May 2024 classified EOA report.

» SURVIVABILITY

No data were collected during the EOA to determine cyber survivability of the LRUSV prototype.

RECOMMENDATION

The Marine Corps should:

1. Address all DOT&E recommendations provided in the May 2024 classified EOA report.

DEPARTMENT OF THE AIR FORCE PROGRAMS

This page intentionally left blank.

Air Force Programs

This page intentionally left blank.

Advanced Battle Management System (ABMS)

Throughout FY24, the Air Force conducted quarterly minimum viable capability releases (MVCRs) of Cloud-Based Command and Control (CBC2), a component of the Advanced Battle Management System (ABMS). In FY24, the Air Force scheduled a CBC2 operational assessment (OA) as part of an MVCR event, however the Air Force Operational Test and Evaluation Center (AFOTEC) postponed the OA due to software immaturity. CBC2 is the only ABMS component to schedule operational testing (OT) to date and is the focus of this report.

SYSTEM DESCRIPTION

The ABMS portfolio of systems and capabilities is designed to create a next-generation command and control (C2) system that will allow Air Force and Space Force systems to share data that will enable faster C2 decision making. The portfolio is composed of multiple programs and lines of effort including:

- CBC2 (the focus of this report),

- Digital Infrastructure (DI),
- Distributed Battle Management Node (DBMN), and
- Aerial Networking.

Together, these contribute to the Department of the Air Force (DAF) BATTLE NETWORK, which is the DAF contribution to Combined Joint All-Domain Command and Control warfighting concepts.

CBC2 was developed in partnership with the Royal Canadian Air Force to modernize battle management and C2 functions by replacing the Battle Control System-Fixed at U.S. and Canadian Air Defense Sectors with modern cloud-based applications to create a single fused C2 air picture with automated decision aids.

MISSION

DoD military commanders use ABMS to share data and information and receive a real-time, complete picture of the battlespace so that they can quickly make informed decisions, direct action, and monitor execution of operations. The CBC2 component of ABMS will provide an air defense C2 platform that supports homeland defense/homeland security missions, as well as disaster relief and national special security events by maintaining air sovereignty and executing C2 for air defense.

PROGRAM

Each ABMS component program is a separate acquisition program. CBC2, the only program to schedule OT in FY24, is a software acquisition pathway effort. DOT&E approved the CBC2 TES in August 2024. DOT&E also approved the CBC2 OA test plan in August 2024.

The other ABMS component programs are Middle Tier of Acquisition rapid prototyping pathway efforts. Several TESs for ABMS component programs, other than CBC2, are under development.

» MAJOR CONTRACTOR

- Science Applications International Corporation, Inc. – Rosslyn, Virginia (CBC2)

TEST ADEQUACY

DOT&E approved the CBC2 TES with two conditions. First, the Air Force needs to submit the verification, validation, and accreditation (VV&A) plans for the modeling and simulation (M&S) tools required for OT. Second, the Air Force needs to provide an updated cyber test strategy that includes a schedule of events and operational cyber testing that follows the developmental cyber test program.

The Air Force has conducted quarterly CBC2 MVCRs since June 2023. Although the first five MVCRs were developmental test and evaluation (DT&E) events, the Air Force made significant efforts to ensure early OT involvement in CBC2. AFOTEC Detachment 2 observed all MVCRs and was a key stakeholder in all CBC2 DT&E events and processes.

AFOTEC Detachment 2 was scheduled to perform an OA during the sixth MVCR. The OA was postponed due to software immaturity.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E will provide an assessment of CBC2's potential to be operationally effective, suitable, and cyber survivable in the classified CBC2 OA report that is anticipated in FY26.

RECOMMENDATIONS

The Air Force should:

1. Continue to develop TESs for the remaining ABMS components.
2. Submit the VV&A plans for the M&S tools required for OT to DOT&E for approval and AFOTEC for accreditation.
3. Update the CBC2 cyber test strategy and submit to DOT&E for approval. The revised cyber strategy should include a schedule of events for cyber OT that provides time for, and builds upon, a cyber DT&E program.

AGM-183A Air-Launched Rapid Response Weapon (ARRW)

In FY24, the Air Force's AGM-183A Air-Launched Rapid Response Weapon (ARRW) program completed development of the ARRW prototype design and executed two flight tests, including an operational demonstration (Ops Demo). Testing to properly assess lethality of the weapon system was executed successfully. Data analysis from flight tests conducted during FY24 continues.

SYSTEM DESCRIPTION

ARRW is a conventional, air-launched, 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.

MISSION

The Air Force will employ units equipped with ARRW to provide an offensive, high-speed strike capability to destroy high-value, time-sensitive, land-based targets in anti-access/area-denial environments. Launched from bomber aircraft, ARRW provides standoff capability to prosecute targets in a timely fashion.

PROGRAM

ARRW uses the rapid prototyping Middle Tier of Acquisition pathway leveraging technology and lessons learned from the Defense Advanced Research Projects Agency (DARPA)'s Tactical Boost Glide program. The program completed its Critical Design Review in February 2020. In FY21 – 22, the Air Force conducted a series of booster test flights (BTFs), followed by a series of all-up round (AUR) (including live warhead) test flights (ATFs) in FY22 — 24. In August 2023, DOT&E approved the ARRW Integrated Master Test Plan, and in February 2024 DOT&E approved the ARRW Ops Demo Plan. The Ops Demo was completed in March 2024. The Air Force is assessing the ATF results to inform the way ahead for the technologies developed in the ARRW program. DOT&E intends to publish an Ops Demo report in FY25.

» MAJOR CONTRACTOR

- Lockheed Martin Missiles and Fire Control – Orlando, Florida

TEST ADEQUACY

In FY24, the Air Force conducted two ATFs to further validate ARRW's performance in the free flight state from release through terminal maneuver as well as terminal effects. Both flight tests were adequate to demonstrate operational effectiveness and suitability, conducted in accordance with the DOT&E-approved Ops Demo Plan, and observed by DOT&E. The AURs used during the flight tests were produced on certified pilot production lines to demonstrate AUR producibility.

In October 2023, the Air Force conducted the ATF that included a land impact (the previous ATFs in FY23 targeted broad ocean areas). In March 2024, the Air Force conducted an Ops Demo of the ARRW system, which included a land impact, to assess operational capabilities and limitations of the system.

By combining the BTF and ATF data, the Air Force collected sufficient data to demonstrate system capability in a permissive environment, but not enough information to confidently assess operational effectiveness, lethality, suitability, and survivability. From the BTF and ATF test launches, the Air Force collected data on the ARRW integration with a B-52H by releasing ARRWs from all B-52H weapon stations and across the required release conditions. The Air Force collected data on safe separation and safe deconfliction of the ARRW from a B-52H. The ATF series also provided data to demonstrate ARRW performance through all phases of flight, to include boost and ascent, booster-glide vehicle separation, and warhead function.

The Ops Demo, the capstone event of the ATF series, tested the proper function of the ARRW through all phases of flight, with all aspects of employment executed by operational personnel. The Air Force used operational aircrews to complete mission planning, operational maintenance personnel to handle and maintain the ARRW, and operational aircraft armament personnel to upload and download the ARRW to/from a B-52H during the test. To support the Ops Demo, the Air Force provided training to the maintenance personnel and executed a maintenance demonstration.

The Air Force is in the final stages of conducting analysis of test data that captured missile and glider flight characteristics as well as warhead performance and comparing the observed results to modeling and simulation (M&S) results. Lethality of the ARRW system will be evaluated based on the test data and various M&S tools developed to support ARRW system capability.

The Air Force used engagement-level and mission-level M&S to assess ARRW survivability in anti-access/area-denial environments.

No operational cyber assessment was completed. If program elements undergo further development, a cyber assessment must be executed in future developmental iterations.

PERFORMANCE

» EFFECTIVENESS

Preliminary results indicate that the ARRW weapon system demonstrated sufficient mission capability in a permissive environment. From the combined data set, the Air Force demonstrated the ARRW would be able to satisfy the required launch platform release conditions, downrange and cross-range requirements, and the time to place effects on target requirements that are needed to support the strike mission. Due to the limited number of ATF assets (i.e., AUR vehicles), however, there are insufficient data to determine weapon accuracy with statistical confidence from current operational testing. Moreover, the Ops Demo indicated that operational personnel could plan a mission and execute a strike on surrogate targets.

DOT&E expects to publish an Ops Demo report in FY25 after the remaining data are received from the Air Force.

» LETHALITY

Both ATFs in FY24 included the use of land targets to gain knowledge of ARRW lethality effects and support lethality M&S development. In both tests, the Air Force collected data on the dispersion and penetration of ARRW's fragmenting warhead. These data informed and helped to increase confidence in the lethality M&S tools. Analysis of the effects of fragment impacts on the targets' functionality is still pending. Formal accreditation of the lethality M&S supporting ARRW has not been conducted and is not anticipated, somewhat limiting the confidence of M&S to properly predict ARRW system lethality against a wide range of targets.

DOT&E expects to publish an Ops Demo report in FY25 after the remaining data are received from the Air Force.

» SUITABILITY

The limited number of flight hours and test assets (i.e., booster and AUR vehicles) preclude an assessment of all operational suitability metrics for the ARRW system. Specifically, there are insufficient data to assess the operational availability or the operational reliability in the captive-carry and free-flight configurations, with statistical confidence. However, the limited test data that the Air Force collected during ARRW test events indicate that the ARRW system is likely on track to meet all suitability requirements.

Preliminary results of survey responses from the Ops Demo indicate that personnel rated the ARRW training as adequate after completing additional qualification training to handle the ARRW munition. Preliminary results also indicate ARRW is supportable. After training, maintenance personnel were able to store and transport the ARRW, while aircraft armament personnel were able to upload and download the ARRW to a B-52H. Personnel rated the ARRW documentation (i.e., technical orders) as accurate and clear. No interoperability or compatibility issues were noted, although timeline limitations prevented some interoperability and compatibility testing.

DOT&E expects to publish an Ops Demo report in FY25 after the remaining data are received from the Air Force.

» SURVIVABILITY

The Air Force conducted engagement-level and mission-level simulations to assess ARRW survivability in a contested environment. The survivability assessment estimates the probability that a single ARRW will complete its mission, given the capabilities of various early warning radars, surface-to-air missile systems, and anti-aircraft-artillery batteries to detect and engage ARRW in various scenarios. Simulations indicate that ARRW will meet its survivability requirements.

DOT&E expects to publish an Ops Demo report in FY25 after the remaining data are received from the Air Force.

RECOMMENDATION

As recommended in the FY23 Annual Report, the Air Force should:

1. Verify, validate, and accredit all M&S tools intended for use to enable an adequate assessment of ARRW performance.

AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM)

DOT&E published a classified AIM-120D System Improvement Program (SIP)-3F FOT&E report in January 2024. The Advanced Medium-Range Air-to-Air Missile (AMRAAM) AIM-120D3 SIP-3F finished integrated testing in May 2023 and fielded in March 2024. Additional reliability testing of AIM-120D3 hardware is ongoing. Planning is underway for SIP-4 and SIP-3 Tape 2 operational testing, which are both planned to begin in 4QFY25.

SYSTEM DESCRIPTION

The AMRAAM is a radar-guided, air-to-air missile, with capabilities in both the beyond-visual-range and within-visual-range arenas. F-35A/B/C, F-22A, EA-18G, F/A-18C/D/E/F, F-16C/D, and F-15C/D/E/EX aircraft can all employ AMRAAM, including multiple-target engagements with multiple missiles simultaneously.

The AIM-120D3 is the newest variant in the AMRAAM family of missiles and incorporates a form-fit-function hardware refresh to replace obsolete components and re-hosts the SIP-3 operational flight software as SIP-3F. Multiple follow-on SIPs are planned to provide AIM-120D3 updates to enhance missile performance and resolve deficiencies.

Additional software updates to the legacy AIM-120D variant (now called AIM-120D0) are planned under the "SIP-3 Tape X" designation. These updates will enhance performance and resolve deficiencies for legacy AIM-120D0 hardware.

MISSION

The Air Force, Navy, and several foreign militaries employ various versions of the AIM-120 AMRAAM to conduct air-to-air combat missions. All U.S. fighter aircraft use the AMRAAM as their primary beyond-visual-range, air-to-air weapon.

PROGRAM

AIM-120D upgrades are Air Force-led projects under the Acquisition Category IC AMRAAM program. DOT&E published a classified AIM-120D SIP-3F FOT&E test report in January 2024, and SIP-3F fielded in March of 2024. The Services are now in the process of test planning for the next set of AIM-120D operational tests: SIP-4 for AIM-120D3 and SIP-3 Tape 2 for AIM-120D0 variants. The Air Force expects to submit a TEMP update in 1QFY25. Operational testing is scheduled to begin in 4QFY25 for SIP-4 and SIP-3 Tape 2.

The Air Force Operational Test and Evaluation Center is the Operational Test Agency for SIP-4 FOT&E, while the 53rd Wing is the Operational Test Organization for SIP-3 Tape 2 operational testing.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX – Tucson, Arizona

TEST ADEQUACY

In May 2023, the Air Force and Navy completed SIP-3F integrated testing in accordance with the DOT&E approved test plan. DOT&E personnel observed the testing. Discoveries during testing led to multiple missile software and firmware changes. As a result of these changes, some of the early tests were not representative of the final production version of the missile. In the SIP-3F report, DOT&E recommended further testing of the AIM-120D3 to characterize the reliability of the new hardware, which is ongoing.

The availability of threat surrogates for test remains a challenge when assessing missile effectiveness and lethality. Upcoming operational testing may include limited or no full-scale targets due to test asset availability limitations. Additionally, surrogates for many other modern threats do not currently exist. These test asset limitations put greater importance on modeling and simulation (M&S) to adequately characterize the performance of the AIM-120D. However, verification, validation, and accreditation of M&S is also negatively affected, due to the lack of relevant flight test data from testing against representative targets. The Services should fund, develop, and produce modern aerial targets, such as fourth- and fifth-generation fighter aircraft, large bomber and mobility aircraft, helicopters, and others, as discussed in the Test and Evaluation Resources section of this Annual Report.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Details on SIP-3F operational effectiveness and suitability are available in the classified DOT&E test report published in January 2024. The report includes three classified recommendations to improve operational effectiveness and suitability.

» LETHALITY

SIP-3F is lethal, based on previous test results from SIP-3. Details are available in the classified DOT&E SIP-3 test report of November 2022.

» SURVIVABILITY

SIP-3F cyber survivability is based on previous test results from SIP-3. Details are available in the classified DOT&E SIP-3 test report of November 2022.

RECOMMENDATIONS

The Air Force should:

1. Continue additional testing of the new AIM-120D3 hardware to better characterize

the reliability of the new configuration.

2. Fund, develop, and produce modern aerial targets, such as fourth- and fifth-generation fighter aircraft, large bomber and mobility aircraft, helicopters, and others, as discussed in the Test and Evaluation Resources section of this Annual Report. This shortfall is beyond the scope of the AMRAAM program and must be addressed at the Department of the Navy and Department of the Air Force levels.
3. Submit TEMP updates for both SIP-4 and SIP-3 Tape 2 to support the testing scheduled to begin in 4QFY25.

Air Operations Center – Weapon System (AOC-WS)

In October 2023, the Air Force conducted a cooperative vulnerability and penetration assessment (CVPA) of the Air Operations Center – Weapons System (AOC-WS) Increment 10.1, followed by an adversarial assessment (AA) in February 2024. DOT&E published a classified report on the cyber assessment findings in September 2024. The Air Force did not conduct cyber assessments on the AOC-WS Block 20 instantiation. The Air Force continues to develop and deploy AOC-WS Block 20 software but does not intend to conduct operational testing until the capabilities are sufficiently mature. There is still no DOT&E-approved test strategy for the Block 20 instantiation or AOC-WS as a whole.

SYSTEM DESCRIPTION

The AOC-WS is a system of systems that incorporates numerous third party, commercial off-the-shelf, and Agile-developed software applications. The AOC-WS consists of two instantiations:

- The AOC-WS Increment 10.1 (AN/USQ-163 Falconer) is the currently fielded backbone system for the AOC.
- AOC-WS Block 20 consists of software-based upgrades that are delivered incrementally to enhance warfighter capability. The upgrades include the Kessel Run All-Domain Operations Suite (KRADOS) and AppTX. KRADOS is intended to serve as the backbone of the AOC, connecting applications through common data streams and supported by a hybrid cloud infrastructure, with the goal of enabling warfighters to move faster and commanders to be more efficient with their manpower. AppTX is intended to migrate existing applications to the hybrid cloud environment to complement KRADOS.

The Air Force continues to provide upgrades to sustain and improve the fielded AOC-WS Increment 10.1, while also developing and fielding software capabilities through the AOC-WS Block 20. As the Air Force develops more Block 20 capabilities, the AOC-WS will transition from the fielded Increment 10.1 to a hybrid configuration of the two instantiations. Ultimately, the Air Force intends to modernize AOC-WS Increment 10.1 capabilities with Block 20 as the delivered software capabilities mature.

MISSION

The AOC-WS provides the Commander, Air Force Forces, or the Joint/Combined Forces Air Component Commander, the capability to exercise command and control of joint (or combined) air forces. This includes planning, directing and assessing air, space, and cyberspace operations; air defense; airspace control; and coordination of space and mission support operations not resident within the theater of operations.

PROGRAM

The AOC-WS Increment 10.1 transitioned from Acquisition Category (ACAT) I to an ACAT III program when it entered sustainment in FY12. Block 20 began as a Defense Innovation Unit Experimental Pathfinder effort in 2017 and transitioned to six Middle Tier of Acquisition programs in FY19. In October 2021, the Assistant Secretary of the Air Force for Acquisition, Technology and Logistics designated both AOC-WS Increment 10.1 and Block 20 as software acquisition pathway programs, merged them, and authorized them to enter the execution phase of development. To comply with DoD Instruction 5000.87, the programs require a DOT&E-approved test strategy prior to entry into the execution phase of development. AOC-WS Increment 10.1 has a DOT&E-approved overarching test plan, but there is still no DOT&E-approved test and evaluation master plan or test strategy that covers Block 20, or the AOC-WS as a whole.

The Air Force continues to revise the draft test strategy for the merged AOC-WS Increment 10.1 and Block 20 program, and has partially addressed DOT&E critical comments, including concerns about the roles, responsibilities, and authorities for the two independent Air Force operational test organizations that will both be testing AOC-WS. The program office continues to deliver incremental capability updates and maintenance software revisions to AOC-WS Increment 10.1 via periodic Agile Release Events (AREs). The Air Force delivered and fielded AREs 23-08 and 24-03 in FY24, based on results from integrated developmental and operational testing at the Ryan Center, Joint Base Langley-Eustis, Virginia.

Block 20 capabilities are developed and fielded at numerous sites, following Agile software development and continuous integration and deployment principles. Block 20 continues to undergo iterative development, but no dedicated OT&E has yet been conducted on any Block 20 instance.

DOT&E has determined that annual, independent, dedicated OT&E of AOC-WS Increment 10.1, and frequent observation of Block 20 efforts by the operational test agency (OTA), are required to assess the evolving hybrid system and Block 20's progress toward system maturity. A single annual test at an operational site that has both AOC-WS Increment 10.1 and Block 20 could satisfy these requirements. However, the Air Force assesses that AOC-WS Increment 10.1 is the only configuration currently ready for operational testing, so Block 20 will begin operational test once the capabilities are sufficiently mature to execute the AOC mission across the entire spectrum of conflict.

DOT&E published a classified report on the cyber assessment findings of AOC-WS Increment 10.1 in September 2024. In FY25, the Air Force plans to conduct a mission-based cyber risk assessment, and a test design and measures review event supporting eventual Block 20 OT&E.

» MAJOR CONTRACTORS

- RTX – Dulles, Virginia
- Science Applications International Corporation, Inc. – Reston, Virginia

TEST ADEQUACY

The Air Force is conducting planned AOC-WS Increment 10.1 system upgrades via AREs, in accordance with the DOT&E-approved overarching test plan. DOT&E monitors the releases, observes the testing, and reports on more significant capability releases. In FY24, the Air Force conducted integrated tests on ARE 23-08, ARE 24-03, and ARE 24-09 in accordance with DOT&E-approved test plans, and DOT&E observed testing of all three upgrades. The integrated test of ARE 23-08 required additional testing of both functionality and deployability, which began in October 2023 and was completed January 2024. ARE 24-03 testing occurred in March and April 2024. ARE 24-09 testing is scheduled to begin in September 2024, with completion in FY25.

The Air Force did not conduct a Block 20 software supply chain test in FY24.

Following DOT&E approval of the test plans, the Air Force conducted a CVPA and an AA at a geographic AOC in October 2023 and February 2024, respectively. The CVPA and AA were adequate to support a cyber survivability evaluation of the AOC-WS Increment 10.1; however, the Air Force needs to collect additional data to characterize the survivability of AOC-WS Block 20 and the hybrid weapon system. DOT&E published a classified report in September 2024 on the CVPA and AA findings. Annual CVPAs and AAs are needed to adequately characterize the mission risk of the evolving AOC-WS. The Air Force intends to conduct a CVPA at another geographic AOC in FY25.

The Air Force did not conduct operational testing of Block 20 in FY24. The OTA observed two program office-led usability assessments of Block 20 at an operational AOC site, and its subsequent use during a major combatant command exercise. However, none of these events qualify as operational tests, nor were they intended to provide adequate data to draw OT&E conclusions. Block 20 capabilities continue to be deployed incrementally through an Agile release capabilities model. Capabilities are released to the field, then feedback is obtained from the users, and the capability is refined to fit warfighter needs. DOT&E has determined that frequent observations by the OTA may suffice to monitor progress toward meeting Air Combat Command's annual Capability Needs Statements, replacing AOC-WS Increment 10.1, and assessing the evolving risk that is being imposed on the warfighters. DOT&E does not expect to issue reports based on these observations unless they identify exceptional findings.

PERFORMANCE

» EFFECTIVENESS

The Air Force found that AOC-WS Increment 10.1 AREs 23-08 and 24-03 are operationally effective. The Air Force collected operational progress report observations on operational effectiveness on Block 20, but the data were insufficient for DOT&E to evaluate and comment on its effectiveness.

» SUITABILITY

The Air Force found that AOC-WS Increment 10.1 ARE 23-08 is operationally suitable with limitations; ARE 23-08 regression testing, conducted at a second test location, generated recommendations to improve suitability. The Air Force found that ARE 24-03 is operationally suitable. Since there has been no operational suitability testing of Block 20, there are insufficient data for DOT&E to comment on its suitability.

» SURVIVABILITY

DOT&E's assessment of AOC-WS Increment 10.1 cyber survivability can be found in DOT&E's September 2024 classified test report on cyber assessment findings.

Although Block 20 capabilities, software, and hardware were present at the CVPA and AA test site, operational constraints and system administration decisions precluded testing them. DOT&E still does not have sufficient data on the cyber survivability of the AOC-WS Block 20 instantiation or of the hybrid AOC-WS configuration. Moreover, the Air Force has not provided sufficient data on critical portions of the software supply chain and the unclassified development environments to enable adequate OT&E planning.

RECOMMENDATIONS

The Air Force should:

1. Address all recommendations in the September 2024 classified test report on cyber assessment findings.
2. As recommended in the FY22 and FY23 Annual Reports, provide an updated Block 20 acquisition strategy with product roadmaps that identify when capabilities under development are expected to be sufficiently mature for operational testing. Sufficient lead time is necessary for test planning and to comply with DoD policy for software acquisition pathway programs.
3. Complete the revision of the consolidated test strategy covering AOC-WS Increment 10.1 and Block 20 that will provide for adequate, periodic evaluations of operational effectiveness, operational suitability, and cyber survivability.
4. As recommended in the FY22 and FY23 Annual Reports, conduct a cyber survivability assessment of the Block 20 software supply chain, to include the unclassified development environment and distribution environments, and to adequately inform subsequent OT&E.
5. Complete an annual CVPA and an AA at a fielded AOC, which has both AOC-WS Increment 10.1 and Block 20 capabilities present, to characterize the cyber vulnerabilities of the hybrid weapon system.
6. As recommended in the FY22 and FY23 Annual Reports, implement a solution to meet the long-standing requirement to collect and report stability, reliability, availability, and maintainability data for the AOC-WS.

B-52 Radar Modernization Program (RMP)

Modification of B-52 Radar Modernization Program (RMP) test aircraft and development of initial system flight software began in FY23. Developmental and integrated flight testing are planned to begin in FY26. DOT&E will evaluate integrated test data for potential to reduce FY28 IOT&E requirements. Full-rate production (FRP) will follow completion of system development. Exact dates are uncertain due to technical and schedule risks.

SYSTEM DESCRIPTION

The B-52 RMP will replace the legacy APQ-166 radar with the modified AN/APQ-188 Bomber Modernized Radar System, which is a variant of the radar currently used on the F/A-18 and F-15E/EX. Replacement of the aging legacy radar is intended to increase system reliability and reduce sustainment costs. The Bomber Modernized Radar System will also provide new high-resolution ground mapping capabilities to improve target location accuracy and capabilities to track moving surface and air targets.

MISSION

Theater commanders will use units equipped with the RMP-modified B-52 to conduct long-range, all-weather conventional and nuclear strike operations that employ a wide range of munitions against ground and maritime targets in low-to-medium adversary threat environments. B-52 theater mission tasks include strategic attack, time-sensitive targeting, air interdiction, close air support, suppression/destruction of enemy air defenses, maritime mining, and nuclear deterrence.

PROGRAM

The B-52 RMP is an Acquisition Category IB Major Defense Acquisition Program. DOT&E approved the B-52 RMP TEMP in April 2021. In June 2021, the Air Force completed the Milestone B (MS B) decision and awarded a five-year engineering and manufacturing development contract to Boeing. A two-part MS C decision is planned in 2Q and 4QFY26 to modify 28 low-rate initial production aircraft. An FRP decision for the remaining 46 aircraft will follow IOT&E execution in FY28. Exact dates are uncertain due to technical and schedule risks.

The program completed Critical Design Review in February 2022. The Air Force continues to refine the system radome design to address aircraft integration issues. Depending on final radome design, radar performance may be impacted. The program office should fully characterize performance with the final radome design to inform operational employment tactics. Modification of test aircraft and development of initial system flight software began in FY23. Delays related to integration challenges have shifted the planned start of developmental and integrated flight testing to FY26, leading to IOT&E in FY28.

The program office has identified necessary system design changes to manage system integration. These changes should be implemented and evaluated to inform operational employment tactics.

Installation of the Tactical Data Link communication system upgrade is necessary to complete RMP operational test requirements. The program office has dedicated sufficient modification kits to ensure timely support to test aircraft for these requirements.

The Air Force successfully leveraged DOT&E-sponsored funding to modernize B-52 test data collection and processing infrastructure. New B-52 data acquisition technologies have been successfully paired with a government-owned knowledge management system to implement cutting-edge data collection, management, and processing capabilities. Application of big data analytics has improved the quality, depth, and speed of post-mission data processing for current B-52 upgrade programs and hypersonic weapons testing. The program office is exploring expansion of the system to other government and vendor sites to support distributed test operations.

DOT&E approved the B-52 Cybersecurity TES in September 2023. This strategy defines a comprehensive, integrated cybersecurity test approach across all planned modernization programs, including the Commercial Engine Replacement Program, RMP, and multiple communication system upgrade programs. DOT&E requires an RMP-specific updated strategy prior to the first MS C decision point, which is scheduled for 2QFY26.

» MAJOR CONTRACTORS

- The Boeing Company – Oklahoma City, Oklahoma
- Raytheon, a subsidiary of RTX – Arlington, Virginia

TEST ADEQUACY

DOT&E approved the B-52 RMP TEMP in April 2021. The TEMP defines an adequate operational test strategy and necessary resources for integrated testing and IOT&E. The B-52 Cybersecurity TES defines an adequate cybersecurity test approach across all B-52 modernization programs, but it will require an RMP-specific update prior to the first MS C decision point.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Modification of two test aircraft and development of initial system flight software began in FY23. Developmental and integrated flight testing are scheduled to begin in FY26. DOT&E will evaluate integrated test data for potential to reduce IOT&E requirements. DOT&E will assess operational effectiveness, suitability, and survivability following IOT&E in FY28.

RECOMMENDATIONS

The Air Force should:

1. Evaluate and implement system design changes necessary to manage system integration, as recommended in the FY23 Annual Report.
2. Evaluate system changes to characterize radar operations based on the final radome design.
3. Develop and submit, for DOT&E approval, an RMP-specific, updated Cybersecurity TES prior to the first MS C decision point.

B-52J Commercial Engine Replacement Program (CERP)

In December 2023, at Air Force Acquisition Executive direction, the B-52J Commercial Engine Replacement Program (CERP) transitioned from the Middle Tier of Acquisition (MTA) rapid prototyping pathway to the major capability acquisition pathway, following delivery of Virtual System Prototype digital models in FY23. The Milestone B (MS B) decision is scheduled for FY25.

SYSTEM DESCRIPTION

The B-52J CERP is the final phase of a multi-year, multi-program modernization effort. B-52J CERP replaces legacy TF33 engines with Rolls Royce F130 commercial derivative engines to increase system reliability and reduce sustainment costs. This upgrade will also increase fuel efficiency and electrical power generation capacity and provide modern digital engine controls and displays.

MISSION

Theater Commanders will use units equipped with the B-52J CERP to conduct long-range, all-weather, conventional and nuclear strike operations that employ a wide range of munitions against ground and maritime targets in low-to-medium adversary threat environments. B-52 theater mission tasks will include strategic attack, time-sensitive targeting, air interdiction, close air support, suppression/destruction of enemy air defenses, maritime mining, and nuclear deterrence.

PROGRAM

The B-52J CERP completed initial MTA rapid prototyping efforts with delivery of Virtual System Prototype digital models in FY23. These models support initial system performance analysis, production planning, system support analysis, and early training activities. Digital models developed during the MTA phase will require extensive ground and flight test validation to enable their use as primary program data sources.

At Air Force Acquisition Executive direction, the program transitioned to the major capability acquisition pathway in December 2023, with a planned MS B decision in FY25, which was delayed from FY24 due to changes required in nacelle design and auxiliary engine systems. The proposed acquisition strategy extends system development until FY33 to better integrate these design changes with preceding modernization upgrades, to include the radar modernization and communication system upgrades, along with ongoing aircraft sustainment programs. The proposed program schedule includes system-level Critical Design Review in FY25, followed by modification of two test aircraft. Developmental and integrated flight testing would begin in FY29, leading to IOT&E in FY32. The proposed production program would award low-rate initial production (LRIP) contracts to procure engines and modify 69 percent (51 of 74) of B-52 fleet aircraft prior to the completion of IOT&E in FY32. A full-rate production decision for the remaining 23 aircraft is planned for FY33. IOT&E will be conducted with two fully modernized B-52J CERP LRIP aircraft.

Integration of new engines on a legacy aircraft is a major design change. B-52J CERP integration will require extensive flight tests to evaluate safety and performance in the areas of aircraft structures, wing flutter, propulsion system compatibility, aerodynamic performance, and aircraft flying qualities in critical phases of flight. Changes in aircraft performance and flight characteristics require recertification of air refueling compatibility with all supporting tanker aircraft and recertification of all employed weapons. Based on results from previous flight test programs, the risk of deficiency discovery in one or more of these areas is high. The proposed Air Force acquisition strategy implements a highly concurrent flight test and production program, with LRIP contracts awarded for 69 percent of fleet aircraft prior to IOT&E. A contract for the first LRIP lot for five aircraft would be awarded prior to the start of the flight test program. Three additional LRIP contracts, covering 46 more aircraft, would be awarded prior to completion of the developmental flight test program and IOT&E. Previous aircraft development programs with highly concurrent flight test and production schedules of this kind have frequently incurred significant cost increases and schedule delays driven by deficiency discoveries. To minimize concurrency risks, section 4231 of title 10, U.S. Code limits LRIP quantities to the minimum necessary to provide production representative articles for operational test, to establish an initial production base for the system, and to permit an orderly increase in the production rate. Air Force rationale for establishing 69 percent of fleet aircraft as the minimum LRIP quantity necessary for these limited purposes is based on a 2017 business case analysis. That analysis projected significant cost savings from procurement of a commercial engine replacement in fewer and larger lots with installation schedules aligned with existing B-52 periodic depot maintenance schedules.

DOT&E is coordinating with the Air Force to develop the B-52J CERP MS B TEMP, which should be submitted for DOT&E approval in 1QFY25. DOT&E approved the B-52 Cybersecurity TES in September 2023. The Cybersecurity TES defines a comprehensive cybersecurity test approach across all planned modernization programs, including CERP, radar modernization, multiple communication system upgrades, and system sustainment programs. DOT&E requires an updated Cybersecurity TES prior to the program MS C decision, which is currently planned for 1QFY29.

» MAJOR CONTRACTORS

- The Boeing Company – Oklahoma City, Oklahoma
- Rolls-Royce North America – Indianapolis, Indiana

TEST ADEQUACY

DOT&E is coordinating with the Air Force to develop the B-52J CERP MS B TEMP. It will define an adequate operational test strategy for the modernized B-52J CERP aircraft configuration. The B-52 Cybersecurity TES defines an adequate cybersecurity test approach across all B-52 modernization programs, but it will require a CERP-specific update prior to the MS C decision point.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

The B-52J CERP is still in the system design phase. Developmental and integrated flight testing is proposed to begin in FY29. DOT&E will evaluate integrated test data for potential to reduce IOT&E requirements. DOT&E will assess operational effectiveness, suitability, and survivability following IOT&E in FY32.

RECOMMENDATIONS

The Air Force should:

1. Continue to develop verification and validation plans for digital models developed during the MTA phase to enable future use as primary engineering decision tools, as recommended in the FY23 Annual Report.
2. Mitigate concurrent flight test and production risks by establishing clear, data-driven exit criteria based on flight test results for each of the four LRIP contract award decision points, as recommended in the FY23 Annual Report.
3. Develop and submit for DOT&E approval, a CERP-specific updated strategy prior to the MS C decision point.

Defense Enterprise Accounting and Management System (DEAMS)

The Defense Enterprise Accounting and Management System (DEAMS) Program Management Office (PMO) continues to refine its implementation of the Scaled Agile Framework (SAFe) to improve the delivery of accounting management software, but the operational test strategy in the previously approved TEMP is out of date. DEAMS's operational effectiveness, suitability, and survivability have not been fully assessed since FY16, and DEAMS remains not survivable. The DEAMS PMO has improved its integrated test environment, and the Air Force should perform verification, validation, and accreditation (VV&A) of that environment to determine its level of operational representativeness. The results should be used to develop a more operationally representative test strategy to guide agile development and fielding of new capabilities and software fixes.

SYSTEM DESCRIPTION

DEAMS is a defense business system that uses commercial off-the-shelf enterprise resource planning software to provide accounting and financial management services.

The DEAMS PMO is following an agile acquisition strategy that adds capabilities and users incrementally. DEAMS serves a user base of up to 16,600 end-users at approximately 170 locations worldwide.

MISSION

DEAMS is intended to deliver accurate, reliable, timely, and auditable financial management information compliant with governing laws, regulations, and policies. DEAMS performs the following core accounting functions:

- Financial System Management
- General Ledger Management
- Funds Management
- Payment Management
- Receivable Management
- Cost Management
- Reporting

Air Force financial managers and tenant organizations use DEAMS to do the following across the U.S. Air Force, the U.S. Space Force, and their supported combatant and field commands:

- Compile and share accurate, up-to-the-minute financial management data and information.
- Satisfy congressional and DoD requirements for auditing of funds, standardizing of financial ledgers, timely reporting, and reduction of costly rework.

PROGRAM

DEAMS is a Business Acquisition Category I program of record. In FY18, DOT&E approved a TEMP for DEAMS Increment 1, which defined a non-agile test strategy. The approved TEMP does not detail any operational test events beyond FY18. DEAMS was designated as an Agile Software Development Pilot Program in the FY19 National Defense Authorization Act. In FY20, the DEAMS PMO adopted SAFe to facilitate agile software development. As of the end of FY24, the DEAMS PMO has not completed a TEMP update. During FY24, DEAMS continued the approach started in FY20 of completing four agile program increments of approximately 12 weeks each, which resulted in deployment of incremental updates to previously fielded capabilities.

» MAJOR CONTRACTOR

- CACI International, Inc. – Dayton, Ohio

TEST ADEQUACY

The DEAMS PMO developed a more operationally representative integrated test environment to support shortened development and deployment cycles and is executing a cloud migration strategy. The DEAMS PMO intends to deploy new capabilities to new user sets starting with major acquisition commands in FY25. The Air Force needs to conduct a risk assessment in accordance with DOT&E guidance to determine the scope of the FOT&E for these limited deployments planned to start in FY25. As reported in recent DOT&E Annual Reports, the following problems, resulting from SAFe software development implementation, still must be addressed:

- The approved DEAMS TEMP is out of date and does not detail an agile development test strategy. An update to the DEAMS TEMP is required to address future FOT&E of new capabilities being agilely fielded and/or new user deployments.
- The operational representativeness of the DEAMS integrated test environment is unknown because the Air Force has not yet conducted a VV&A of the environment.
- An Agile Operational Master Test Plan (AOMTP) is needed with sufficient detail to conduct adequate operational tests of the upcoming DEAMS capability deployments.

PERFORMANCE

» EFFECTIVENESS

The FY22 Annual Report noted some areas reducing the operational effectiveness of DEAMS identified during previous operational testing. The DEAMS PMO is using agile development methods to improve the following:

- Timeliness of displayed information to users has improved due to fixes in data replication performance.
- Faster resolution of critical software deficiencies, prioritization of the backlog of software deficiencies, and enhancements by the implementation of SAFe.

» SUITABILITY

DEAMS remains not operationally suitable based upon previous operational tests. In FY20, DOT&E recommended that site-specific workflows be developed to improve the usability of DEAMS. The DEAMS TEMP update and AOMTP should implement an agile test strategy that will evaluate site-specific operational needs for existing users and future user deployments.

» SURVIVABILITY

DEAMS remains not survivable based upon previous operational tests. In the FY20 Annual Report, DOT&E recommended that the DEAMS PMO address cyber vulnerabilities that present a high risk to DEAMS missions.

RECOMMENDATIONS

The Air Force should:

1. Conduct a cooperative vulnerability and penetration assessment and an adversarial assessment to measure the program's progress towards cyber survivability, as discussed in the FY22 and FY23 Annual Reports.
2. Perform a VV&A of the operational representativeness and realism of the DEAMS integrated test environment prior to planned capability deployments starting in FY25, as discussed in the FY22 and FY23 Annual Reports.
3. Submit an AOMTP and an updated TEMP to DOT&E for approval to support the planned capability deployments to new and existing users starting in FY25, as discussed in the FY22 and FY23 Annual Reports.

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

The Air Force Operational Test and Evaluation Center (AFOTEC) conducted an IOT&E of the Deliberate and Crisis Action Planning and Execution Segments (DCAPES) Increment 2B from February to September 2024 to assess its operational effectiveness, suitability, and cyber survivability. Due to AFOTEC deviating from the approved test plan for the IOT&E, additional data may need to be collected to support an adequate evaluation of DCAPES.

SYSTEM DESCRIPTION

DCAPES is used to create, manage, and project weapon systems, logistics, and personnel documentation, enabling the Air Force to deliver air, space, and cyberspace capabilities to combatant commanders worldwide. DCAPES stores planning and execution information for Air Force functional users in the four main operations planning disciplines: operations, logistics, manpower, and personnel.

MISSION

Air Force mission support personnel use DCAPES for deliberate and crisis action planning by providing users the capability to: (1) receive and analyze operational requirements;

(2) develop, compare, and prioritize alternative courses of action; and (3) prepare documents that support guidance for employment of the force.

DCAPES helps planners:

- Access and transact with joint planning and execution data
- Produce and maintain Air Force inputs to combatant commander's time-phased force and deployment data
- Create and maintain pre-defined packages of manpower and equipment for use in planning and execution
- Create and maintain postured force elements for joint planners
- Exchange data with other command and control systems
- Manage sourcing, scheduling, and deployment of Air Force military and civilian personnel
- Maintain strength accountability of deployed forces
- Perform feasibility and capability analysis in support of logistics, manpower, and personnel needs
- Develop planning and execution documents

PROGRAM

DCAPES Increment 2B is an ACAT IAC program with a full deployment decision (FDD) planned for 1QFY25. Upon completion of the FDD, the program management office plans to transition to the software acquisition pathway.

DCAPES is in the process of developing a new TEMP to support the new acquisition approach.

» MAJOR CONTRACTORS

- CGI Federal, Inc. – Fairfax, Virginia
- Obsidian Global, LLC – Washington, District of Columbia

TEST ADEQUACY

AFOTEC conducted the DCAPES IOT&E from February to September 2024 to assess operational effectiveness, suitability, and cyber survivability. This IOT&E is intended to inform the FDD. As AFOTEC did not conduct the IOT&E in accordance with the test plan as approved by DOT&E, DOT&E is working with AFOTEC to determine whether AFOTEC collected adequate data.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

As discussed above, DOT&E is working with AFOTEC to determine whether AFOTEC collected adequate data.

RECOMMENDATIONS

The Air Force should:

1. Work with DOT&E to ensure adequate data were obtained to permit a full evaluation of DCAPES' operational effectiveness, suitability, and cyber survivability.
2. Submit an updated TEMP to DOT&E for approval to support the planned transition to the software acquisition pathway.

F-15 Eagle Passive Active Warning Survivability System (EPAWSS)

In January 2024, the Air Force completed IOT&E for the AN/ALQ-250(V)1 F-15 Eagle Passive Active Warning Survivability System (EPAWSS). In July 2024, DOT&E published a classified IOT&E report, which concluded that EPAWSS is operationally effective, operationally suitable, and cyber survivable in the environment in which it was tested, but performance is unknown in modern combat environments, where test capability is lacking. Test resource shortfalls common to all electromagnetic warfare assessments constrained the Air Force's ability to assess EPAWSS electromagnetic attack (EA) performance. The Air Force should continue to assess and improve EPAWSS effectiveness and suitability as part of F-15EX FOT&E, currently planned to begin in FY25.

SYSTEM DESCRIPTION

The AN/ALQ-250(V)1 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 within highly contested environments. The EPAWSS radar warning function scans the radio frequency environment and provides the aircrew with identification and location information of potential threat signals. When necessary, the system can respond with countermeasures (i.e., jamming or expendables) to defeat a threat radar or missile. EPAWSS integrates with the F-15 AN/APG-82(V)1 radar and Advanced Display Core Processor II mission computer. EPAWSS replaces three 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.

MISSION

The Air Force employs the F-15E Strike Eagle as a dual-role fighter, designed to perform air-to-air and air-to-ground missions. The Air Force plans to initially employ the F-15EX in an air superiority role. It will be flown by active duty and Air National Guard units to perform both offensive and defensive air-to-air missions. EPAWSS provides the primary defensive suite to protect the F-15E and F-15EX during the conduct of these missions.

PROGRAM

F-15 EPAWSS is an Acquisition Category IC program that tailored Milestone C into two decision points (DPs) to take long-lead hardware procurement off the critical path and ensure delivery of the capability as soon as possible. The Air Force Service Acquisition Executive approved the Milestone C DP 1 (i.e., production decision) in December 2020, authorizing the procurement of low-rate initial production hardware. DP 2 (i.e., installation decision) was approved in June 2022, which authorized the start of fleet aircraft modifications. The first operational F-15E modification began in May 2023.

In June 2022, DOT&E approved the EPAWSS TEMP. DOT&E approved the IOT&E flight test plan in March 2023, the ground test plan in July 2023, and the cyber-survivability test plan in November 2023. DOT&E observed the Air Force conducting IOT&E between July 2023 and January 2024. DOT&E published the classified IOT&E report in July 2024 to support the Air Force's full-rate production decision briefing in September 2024.

The Air Force intends to retrofit 99 F-15Es and equip all F-15EXs with EPAWSS as the aircraft are produced, with fielding due to start in FY24.

» MAJOR CONTRACTORS

- Boeing Defense, Space & Security – St. Louis, Missouri
- BAE Systems, Inc. – Nashua, New Hampshire

TEST ADEQUACY

During FY24, the Air Force completed the EPAWSS IOT&E. The Air Force conducted the test in accordance with the DOT&E-approved TEMP, ground, flight, and cyber survivability test plans, with two DOT&E-approved waivers. DOT&E observed all operational testing.

In December 2023, the Air Force conducted operational ground testing of EPAWSS to collect data on the system's radar warning. A ground test conducted at the Integrated Demonstrations and Applications Laboratory (IDAL), Wright-Patterson AFB, Ohio, provided data for the evaluation of the radar warning performance in an operationally representative scenario. During IDAL testing, the Air Force's 36th Electronic Warfare Squadron programmed an operationally representative Mission Data File (MDF) that was evaluated in the operationally representative background radio frequency environment. Moreover, the Air Force conducted EA effectiveness testing during July 2023 at the Electronic Combat Simulation and Evaluation Laboratory, Point Mugu, Naval Base Ventura County, California, and collected data for the evaluation against two closed-loop threat simulators.

From August 2023 to January 2024, the Air Force flew open-air flight test missions at the Eglin Gulf Test and Training Range, Florida, and the Nevada Test and Training Range, Nevada. DOT&E used data from flight testing to evaluate EPAWSS geolocation performance and overall mission success. However, the data were not adequate for assessing EA effectiveness because of shortfalls in open-air threat representation and failure to collect comparison data of effectiveness without EPAWSS. As part of offensive and defensive counter-air missions, various fourth- and fifth-generation Air Force and Navy aircraft acted as threat surrogates against the EPAWSS-equipped F-15s.

The Air Force assessed EPAWSS suitability through developmental and operational test events starting from the release of EPAWSS Flight Bundle 9.0 in January 2023. The Air Force collected data and assessed maintainability during a maintenance demonstration conducted in January 2024 with 366th Fighter Wing maintainers. Evaluators administered surveys and interviews after flight test missions and the maintenance demonstration to collect data from aircrew and maintainers for human-systems interaction assessments. The Air Force could not collect data on EPAWSS operational availability because logistics and supply chains were not operationally representative.

To evaluate the cyber survivability of EPAWSS, the Air Force conducted a cooperative vulnerability and penetration assessment (CVPA) and an adversarial assessment (AA). The Air Force's 48th Cyberspace Test Squadron conducted the CVPA and provided technical feedback during the AA. The CVPA was conducted in a hangar on a ground-powered F-15E with EPAWSS installed. The lack of observed cyber effects during the CVPA resulted in the AA being converted to an interview with operational aircrew and maintainers.

PERFORMANCE

» EFFECTIVENESS

EPAWSS is operationally effective under the conditions the open-air test ranges could produce during IOT&E. There are limitations to testing at DoD's open-air test ranges due to infrastructure deficiencies, such that the test environment was not operationally representative of a modern threat environment. In addition, demonstrated system performance of the radar warning, geolocation, and EA capabilities highlighted areas that require improvement. Test limitations constrained characterizing EA performance during flight testing. The limited EA effectiveness data showed system performance inconsistencies between ground and flight test events, but overall results from both types of tests indicate that EPAWSS EA is potentially effective.

» SUITABILITY

EPAWSS is operationally suitable and met most of its reliability and maintainability requirements during IOT&E. Although the performance of the built-in test (BIT) system has improved since the end of developmental testing, BIT false alarms still occurred in IOT&E sorties. Assessments of the suitability impacts of BIT false alarms and the performance of the Fully Automated Debrief System are available in the classified DOT&E test report published in July 2024. The report also includes classified recommendations to improve suitability. The MDF generator software used to assemble threat parameters into an MDF is hard to use and too slow to meet updated Air Force requirements. The 36th Electronic Warfare Squadron submitted 20 documented program deficiencies for the current version of the MDF generator.

» SURVIVABILITY

EPAWSS is survivable against cyber threats emulated during the IOT&E. The cyber test team was unable to generate significant adverse cyber effects on the installed EPAWSS system.

RECOMMENDATIONS

The Air Force should:

1. Continue to improve EPAWSS as described in the classified IOT&E report, and test it as part of F-15EX FOT&E.

These tests should include a comprehensive evaluation of EPAWSS EA effectiveness against modern threat simulators, along with collection of reference effectiveness data, without EPAWSS, for comparison.

2. Ensure that EPAWSS BIT and the Fully Automated Debrief System provide accurate and actionable information to aircrews and maintainers during F-15EX FOT&E.
3. Correct deficiencies with the MDF generator to provide more effective and efficient programming.

F-15EX Eagle II

The F-15EX Eagle II was approved for full-rate production (FRP) in June 2024. The Air Force is developing a plan for FOT&E based on DOT&E recommendations in the November 2023 combined IOT&E and LFT&E report. The Air Force completed cyber survivability testing on a Lot 1B aircraft and is developing a plan to assess a Lot 2 aircraft. The cyber survivability evaluation will continue with Lot 2 aircraft due to planned changes in the fielding configuration and will be included in the FOT&E. DOT&E is currently analyzing the results of the survivability studies and will submit an annex to the November 2023 combined IOT&E and LFT&E report in 2QFY25.

SYSTEM DESCRIPTION

The F-15EX is a two-seat, twin-engine, multi-role fighter aircraft. It is a derivative of the Qatari F-15QA, which is a derivative of the Air Force F-15E Strike Eagle. The F-15EX inherits modern advances such as "fly-by-wire" flight controls, dual Digital Helmet Mounted Cueing Systems, a large touchscreen display, and additional improvements, such as the AN/ALQ-250(V)1 Eagle Passive Active Warning Survivability System for electronic warfare, which is being reported on in a separate annual report article.

MISSION

Although the aircraft is multi-role capable, the Air Force intends to use the F-15EX initially in an air superiority role, then expand to a multi-role mission. Units equipped with the F-15EX will provide offensive counterair, cruise-missile defense, and defensive counter-air capabilities, including escort of high-value airborne assets. The F-15EX can employ a full complement of air-to-air weapons and has four additional air-to-air weapons stations compared to the F-15E. The F-15EX has a limited capability to employ precision-guided, air-to-surface munitions, in addition to its primary air superiority mission.

PROGRAM

The F-15EX is an Acquisition Category IB program that transitioned from a rapid fielding Middle Tier of Acquisition program to a major capability acquisition program in September 2022. The Air Force intends to procure 98 F-15EX aircraft, training systems, and support equipment over 6 procurement lots. As part of the transition process, DOT&E approved the OT&E section of the Program Strategy Document in October 2022. DOT&E published the F-15EX combined IOT&E and LFT&E report with classified annex in November 2023 to support the program's FRP decision in June 2024. The live fire data collection and analysis was incomplete in the LFT&E portion of the November 2023 report. After the data collection and analysis are complete, DOT&E plans to submit an additional annex to the combined IOT&E and LFT&E report in 2QFY25.

» MAJOR CONTRACTORS

- Boeing Defense, Space & Security – St. Louis, Missouri
- RTX, Agile Radar Solutions – El Segundo, California
- General Electric – Cincinnati, Ohio

TEST ADEQUACY

During IOT&E, the threat level was adequate for the current F-15EX mission set. However, the mission-level testing did not include some advanced, longer-range threat weapons becoming operational at the time of F-15EX fielding. Subsequent FOT&E testing will be required to assess the system against higher threat levels in more complex mission scenarios. The Air Force successfully used Open Air Battle Shaping (OABS) instrumentation during the F-15EX IOT&E. However, due to limitations in open air range infrastructure, the Air Force is exploring incorporating the F-15EX into the Joint Simulation Environment (JSE) to enable testing and training that cannot currently be conducted on DoD's major test and training ranges.

In FY24, the Air Force completed remaining data collection for the alternative LFT&E strategy that DOT&E approved in January 2021. These studies were approved by DOT&E and include susceptibility and vulnerability analyses, while accounting for the F-15EX's performance, configuration, tactics, techniques, procedures, and countermeasures.

In June 2024, the Air Force Operational Test Center conducted – and DOT&E observed – a cooperative vulnerability and penetration assessment (CVPA) at Eglin AFB, Florida, which generated some of the data needed to characterize the performance of the F-15EX while under cyber-attack. A subset of the new systems in the Lot 1B F-15EX was investigated during the event. The program office held a Mission-Based Risk Assessment Process – Cyber (MRAP-C) in May 2024. The results from that MRAP-C will aid in the planning of a cybersecurity vulnerability identification for a Lot 2 aircraft, to be conducted in FY25. Additional cooperative and adversarial cyber testing is necessary before DOT&E can evaluate the platform. In FY25, the Air Force will submit for DOT&E approval an FOT&E test plan that will include cyber testing.

PERFORMANCE

» EFFECTIVENESS

DOT&E published the combined IOT&E and LFT&E report with classified annex in November 2023 to support the June 2024 FRP decision. Against the level of threat tested, the F-15EX is operationally effective in all its air superiority roles, including defensive and offensive counter-air against surrogate fifth-generation adversary aircraft, as well as basic air-to-ground capability against the tested threats. The F-15EX was able to detect and track all threats at advantageous ranges, use onboard and off-board systems to identify them, and deliver weapons while surviving. No further operational testing is planned until the test fleet is modified to the Lot 2 configuration. The Air Force Operational Test and Evaluation Center's Detachment 6 is currently drafting the test plan for DOT&E approval to support FOT&E in FY25 – 26 on F-15EX aircraft that are representative of Lot 2 or later configurations.

» SUITABILITY

DOT&E's final assessment of F-15EX suitability was in the F-15EX combined IOT&E and LFT&E report, which was published in November 2023 to support the June 2024 FRP decision. The F-15EX met all its reliability, availability, and maintainability requirements and achieved nearly all objectives although maintenance technical orders were still immature. Survey data assessing human-systems interactions show the pilots had positive opinions of F-15EX cockpit usability. While training for both pilots and maintainers on the new systems is currently lacking, the Air Force plans to have all training available in time for initial operational capability. At the time of the combined IOT&E and LFT&E report, the F-15EX Program Office had only completed Pre-Published and Preliminary Technical Order (TO) delivery for the Lot 1 aircraft TOs. The program has since completed delivery of all TOs for the Lot 1 fielding configuration and has completed certification and verification of 70 percent of them with a planned certification and verification completion date of November 2024. The TOs, for the Lot 2 configuration that is planned for the FOT&E, are expected to be completed in 3QFY25.

» SURVIVABILITY

In FY24, the Air Force completed all survivability studies in the DOT&E-approved Alternative LFT&E Strategy. DOT&E is currently analyzing the results of the survivability studies and will submit an additional annex to the November 2023 combined IOT&E and LFT&E report in 2QFY25.

As noted in the FY23 Annual Report and program strategy document that supports the FRP decision, DOT&E cannot evaluate the cyber posture of the F-15EX without additional cooperative and adversarial testing, to include a Lot 2 or later production aircraft. The Air Force will incorporate results from the CVPA and MRAP-C into the FOT&E test plan and submit it to DOT&E for approval.

RECOMMENDATIONS

The F-15EX Program Office should:

1. Ensure the F-15EX test fleet is production representative by modifying test aircraft to include any configuration or equipment changes that occur in future production lots, as recommended in the FY22 Annual Report.
2. Submit a TEMP that outlines test events and allocates resources for the period between the FY24 FRP decision and the fielding of Lot 6, as recommended in the FY23 Annual Report.
3. Continue to incorporate OABS and high-fidelity threat radar emulators into the F-15EX FOT&E, as recommended in the FY23 Annual Report.
4. Procure an F-15EX platform model for use in JSE. To ensure concurrence with fleet aircraft, the JSE model should be based on actual Operational

Flight Program and accurate weapons capabilities.

5. Incorporate results from the CVPA and MRAP-C into the FOT&E test plan and submit it to DOT&E for approval.

F-16 Radar Modernization Program (RMP)

The F-16 Radar Modernization Program (RMP) completed IOT&E in 4QFY23. In January 2024, DOT&E published a classified IOT&E report that informed a full-rate production decision in September 2024.

SYSTEM DESCRIPTION

The APG-83 SABR is a multifunction, active electronically scanned array (AESA) radar intended to replace the F-16's legacy APG-68 radar. It provides F-16 pilots with increased air-to-air and air-to-ground situational awareness, advanced electromagnetic protection, high-resolution synthetic aperture radar mapping, fire control, and enhanced datalink support to air-to-air missiles.

MISSION

F-16 pilots use the APG-83, along with onboard weapons, to complete the full kill chain against air, ground, and surface targets, from beyond visual range and in all weather conditions. The APG-83 is a significant improvement over the legacy system, allowing for targeting and engagement from farther ranges with enhanced accuracy and improved combat identification.

PROGRAM

The APG-83 F-16 RMP is an Acquisition Category II program. DOT&E approved the TEMP in November 2023.

The F-16 RMP acquisition used a three-phase approach. In response to a U.S. Northern Command joint emergent operational need statement requirement for homeland defense, the Air National Guard (ANG) completed Phases 1 and 2 in FY21 and FY22, respectively. In these phases, which were not under DOT&E oversight, the ANG acquired a total of 72 radars.

Phase 3, which is under DOT&E oversight, develops full APG-83 capability for 450 active duty and ANG F-16s. Following completion of Phase 3 IOT&E, DOT&E published an IOT&E report in January 2024. The Air Force made a full-rate production decision in September 2024.

» MAJOR CONTRACTOR

- Northrop Grumman Mission Systems – Linthicum, Maryland

TEST ADEQUACY

The F-16 RMP IOT&E was adequate to evaluate the operational effectiveness and suitability of the APG-83 currently being delivered to F-16s. The test was executed by the 53 Test and Evaluation Group in accordance with the DOT&E-approved TEMP and test plan. DOT&E personnel observed F-16 RMP IOT&E. The lack of instrumented test aircraft and poor data collection led to limited air-to-air data. Inconsistent program funding and unexpected engineering challenges delayed other upgrades to the overall F-16 system, most notably the conversion from MIL-STD-1553 data buses to Ethernet. These delays prevent full realization of APG-83 capability. Should the Air Force fund these upgrades in the future, the Service will need to assess all remaining untested radar capabilities in an FOT&E.

The program completed three cyber survivability test events as part of developmental testing: two cooperative vulnerability investigations and one adversarial cyber developmental test. In accordance with the approved TEMP, DOT&E observed the events and concurred with using the results for integrated testing purposes. DOT&E published the cyber survivability results in the classified IOT&E report.

PERFORMANCE

» EFFECTIVENESS

The APG-83 is operationally effective as employed on the F-16. The APG-83 is a significant improvement over the APG-68. The APG-83 has not yet demonstrated that it can meet all requirements due to limitations of the F-16's aging mission computers, obsolete data system, and insufficient network architecture. Upgrades to these systems have been delayed or have failed to meet mission requirements.

» SUITABILITY

The APG-83 is operationally suitable as employed on the F-16. The APG-83 showed improvements in overall reliability, maintainability, and availability over the APG-68 and is comparable to other AESA radars in these criteria. Pilots were generally satisfied with the human systems interface, although some limitations and tradeoffs were required to integrate the new radar with other F-16 systems. The tradeoffs increased pilot workload for some tasks, such as switching between different displays based on the current radar mode and function in use, but the pilots determined these issues were not a critically negative impact.

The ground training systems have not kept up with APG-83 capabilities. While training systems are not part of the F-16 RMP, the Air Force will need to ensure that F-16 training devices and courseware reflect the modernized aircraft systems.

» SURVIVABILITY

The survivability of the APG-83 in a cyber-contested environment was assessed during IOT&E. Testing identified some deficiencies in the APG-83 that were comparable to other AESA radars. Details are available in DOT&E's classified F-16 RMP IOT&E report in January 2024.

RECOMMENDATIONS

The Air Force should:

1. Correct the cyber survivability deficiencies identified during IOT&E, as recommended in the classified IOT&E report and the FY23 Annual Report.
2. Submit a test plan for DOT&E approval to evaluate in an FOT&E the remaining expanded radar capabilities after associated aircraft systems, such as the mission computer and data architecture, are modernized.
3. Update supporting training systems and courseware to reflect the modernized aircraft systems.

F-22A – Raptor Advanced Tactical Fighter Aircraft

In March 2024, DOT&E published a classified FOT&E report on the F-22A Release 2 (R2) Operational Flight Program (OFP) discussed in the FY23 Annual Report. In FY24, the F-22A program completed Force Development Evaluation (FDE) on the R3 OFP, their third annual capability release. DOT&E will publish a classified report on the R3 FDE in 2QFY25. Operational testing of the next capability release, R4, will begin in 1QFY25. During R3 testing, the Federal Aviation Administration (FAA) restricted Link 16 transmission, an ongoing issue that has impeded both testing and utilization of a combat capability already installed in the aircraft. Moreover, the lack of Open-Air Battle Shaping (OABS) instrumentation in the F-22A operational test aircraft continues to restrict the ability to accomplish adequate mission-level evaluations.

SYSTEM DESCRIPTION

The F-22A Raptor is a fifth-generation, air-superiority fighter aircraft that delivers low observability versus threat radars, high maneuverability, sustained supersonic speed, and advanced integrated avionics. The F-22 capability release program adds to the F-22A's already significant combat capability via increments that were originally planned for release annually, but have been extended to 18-month durations.

MISSION

Units equipped with the F-22A conduct offensive counter-air, defensive counter-air, and limited ground attack missions in high-threat environments, delivering air superiority to enable coalition air operations.

PROGRAM

The F-22A Raptor started as a major capability acquisition program, with the first production aircraft fielding in 2003. Since 2019, the Air Force has been implementing hardware and software modernization efforts as capability releases. The Tactical Link 16 and Tactical Mandates TEMP, approved by DOT&E in 2018, supported testing through the R2 FDE. DOT&E published a classified FOT&E report on the R2 testing in March 2024 and expects to publish a classified FDE report on the R3 testing in 2QFY25.

DOT&E approved the R3 test plan and a combined R3/R4 TEMP in 4QFY23. The R3/R4 TEMP provides a capstone test strategy and test concept for these two capability releases. DOT&E expects incremental updates to the TEMP every two capability releases, beginning with R5, planned for FY25. Planning for the next F-22A capability release, R4, is complete and operational testing will begin in 1QFY25.

» MAJOR CONTRACTOR

- Lockheed Martin Aeronautics Company – Fort Worth, Texas

TEST ADEQUACY

Prior to executing the operational testing portion of the DOT&E-approved F-22 R3 OFP FDE Test Plan, the Air Force recommended the OFP for Combat Air Force fielding. The Air Force decision was based on OFP maturity during integrated testing (IT) and on validation of deficiencies identified prior to fielding. R3 IT also included live employment of three AIM-120 Advanced Medium-Range Air-to-Air Missiles. This was the only portion of IT that was observed by DOT&E. Furthermore, the required OABS capability was not available during the R3 IT events.

The OABS limitation, which was also a limitation during testing of R1 and R2 OFPs, stemmed from omissions in the F-22A OFP and delays integrating the Common Range Integrated Instrumentation System (CRIIS) hardware into the F-22A. CRIIS is the current flight test instrumentation capability needed for OABS in the F-22A. OABS enables high-fidelity, real-time, kill removal for accurate mission-level results and the collection of critical data that will be used during verification, validation, and accreditation (VV&A) of the F-22A in the Joint Simulation Environment (JSE).

A longstanding Link 16 test limitation, which stems from FAA restrictions on Link 16 transmissions, continues to challenge testing. A more thorough evaluation of the Link 16 capability in the F-22A is being coordinated with the FAA through a recent memorandum of agreement.

The adequacy of future F-22A testing with the planned Sensor Enhancement (SeE) capability is at risk because delivery of the required SeE model in time for testing of the F-22A with SeE in the JSE is not funded. Nor is the required SeE on contract or planned for being on contract. Moreover, delivery of required environment upgrades to the JSE is currently at risk of being late for testing of the required F-22A release with SeE.

The F-22 program executed an updated analysis to determine the vulnerability of new low-drag external fuel tanks, pylons, and sensor pods. DOT&E did not require an updated alternative live fire test program, deeming an updated analysis to be sufficient, assuming no significant new vulnerabilities or data gaps are discovered in this update.

PERFORMANCE

» EFFECTIVENESS

An evaluation of the operational effectiveness of the R2 F-22A can be found in the classified FOT&E report published in March 2024.

Since the operational test phase of the R3 FDE Test Plan was not executed, DOT&E did not evaluate the mission-level operational effectiveness of the R3 F-22A. Analysis of the results from live weapons testing of the R3 F-22A with the AIM-120 will be discussed in the classified FDE report to be published in 2QFY25.

» SUITABILITY

An evaluation of the operational suitability of the R2 F-22A can be found in the classified FOT&E report published in March 2024.

An evaluation of the operational suitability of the R3 F-22A will be in the classified FDE report to be published in 2QFY25.

One suitability issue that remains from R1 and R2 testing is the significant delay in receiving an avionics component from the vendor, which is critical to enabling F-22A Link 16 capabilities.

» SURVIVABILITY

An evaluation of the cyber survivability of the R2 F-22A can be found in the classified FOT&E report published in March 2024.

Analysis of the cyber survivability of the F-22A's Identification Friend or Foe Transponder Mode 5 and Link 16 within the F-22A open system architecture, as well as the results from the LFT&E vulnerability assessment of the low-drag fuel tanks, pylons, and sensor pod, will be discussed in the classified FDE report to be published in 2QFY25.

RECOMMENDATIONS

The DoD should:

1. As recommended in the FY23 Annual Report, solidify a plan that allows routine accomplishment of Link 16 testing that demonstrates operational effectiveness and cyber survivability, while accommodating FAA protocols, restrictions, and test-specific operating procedures.

The Air Force should:

1. As recommended in the FY23 Annual Report, conduct all future mission-level evaluations of the F-22A with OABS to enable high-fidelity, holistic mission evaluations with new capabilities in operationally representative environments. The data collected by the OABS system capability is critical in accomplishment of VV&A of the F-22A in the JSE.
2. Fund and contract for the delivery of the SeE model in time to complete VV&A prior to use in the JSE, which is required for F-22A SeE IOT&E.
3. Continue to prioritize integration of the required JSE environment upgrades necessary to accomplish adequate testing during F-22A SeE IOT&E.
4. Incorporate VV&A requirements for F-22A operations with SeE in the JSE into flight test activities to ensure data collection requirements in the JSE VV&A plan occur during open-air testing.
5. As recommended in the FY23 Annual Report, prioritize addressing the delays to the delivery of Link 16 avionics components as soon as possible.

HH-60W Jolly Green II

The Air Force has completed two of five objectives in the current HH-60W FOT&E plan to evaluate deferred capabilities and deficiency corrections from the FY22 IOT&E. DOT&E intends to publish a classified FOT&E report when all five objectives are complete.

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, conduct out-of-ground-effect hover at its mid-mission gross weight, and improve survivability.

MISSION

Commanders will employ units equipped with the HH-60W to:

- Recover isolated personnel from hostile or denied territory, day or night, in adverse weather, and in a variety of threat environments from terrorist to chemical, biological, radiological, and nuclear.
- Conduct humanitarian missions, civil search and rescue, disaster relief, medical evacuation, and non-combatant evacuation operations.

PROGRAM

The HH-60W is an Acquisition Category IC program. DOT&E approved the LFT&E Strategy in April 2015, the Milestone C TEMP in January 2020, and an updated full-rate production (FRP) TEMP in March 2023. DOT&E published a combined IOT&E and LFT&E report with a classified annex in March 2023 to inform the FRP decision. DOT&E approved the current FOT&E test plan in June 2023. This test phase is evaluating upgraded hover symbology for reduced visibility approaches, the integration of a weapon deferred from IOT&E, and corrections of deficiencies discovered before and during IOT&E. Subsequent FOT&E plans will evaluate other deferred capabilities, primarily enhanced defensive systems, the full data link capability, and additional communications systems.

» MAJOR CONTRACTOR

- Sikorsky Aircraft Corporation, a subsidiary of Lockheed Martin Corporation – Stratford, Connecticut

TEST ADEQUACY

The Air Force Operational Test and Evaluation Center (AFOTEC) conducted FOT&E in November 2023 per the DOT&E-approved test plan and observed by DOT&E. This testing, along with data collected from earlier testing in June 2023, completed two objectives covering defensive system and mission planning updates. AFOTEC issued a periodic report in February 2024 covering these objectives. DOT&E has received the test data and will publish a classified report when all five test plan objectives are completed. The final FOT&E objectives evaluating the upgraded hover symbology during restricted visibility approaches, the redesigned external mounted gun system, and the deferred GAU-18 weapon are currently estimated for FY25 or FY26.

PERFORMANCE

» EFFECTIVENESS

Updates to the defensive system software have improved the display of situational awareness information to crews operating in threat environments. Updated mission planning software improved crews' ability to plan missions, transfer data to the aircraft, and replan missions in flight. Crew surveys highlighted some remaining shortfalls that occasionally slowed mission planning or caused a loss of map data that degraded situational awareness. However, improved stability of mission planning systems and changes to aircraft launch procedures enabled crews to perform alert launches in less than the required time on seven of eight FOT&E sorties.

DOT&E will publish a detailed assessment in a classified report when all objectives for this test phase are complete.

» SUITABILITY

Technical data supporting maintenance has improved, but aircraft availability remains challenged by spares shortfalls in the supply system, particularly for the mission computer, data transfer unit, radar warning receiver (RWR) antenna units, and hoist cables. DOT&E will publish a detailed assessment in a classified report when all FOT&E objectives are complete.

» SURVIVABILITY

Preliminary analysis of FOT&E data shows that updates to the RWR, missile warning system, and countermeasures dispensing system have improved crews' ability to conduct the personnel recovery mission in threat environments. The program is investigating further improvements to threat displays based on the latest test data. DOT&E will publish a detailed assessment in a classified report when all FOT&E objectives are complete.

RECOMMENDATIONS

The Air Force should:

1. Complete FOT&E objectives regarding the upgraded hover symbology, the GAU-18, and the updated external gun mount.
2. Conduct FOT&E of the remaining deferred capabilities and planned capability upgrades as recommended in the FY23 Annual Report.
3. Continue to develop and implement software improvements to defensive systems and mission displays.

KC-46A Pegasus

The KC-46A has not completed IOT&E. The Air Force Operational Test and Evaluation Center (AFOTEC) has collected all achievable IOT&E aerial refueling (AR) and secondary mission data on the current configuration of KC-46A until the program office updates the refueling boom and Remote Vision System (RVS). In FY24, AFOTEC completed operational testing of the Wing Aerial Refueling Pods (WARPs) and cooperative cyber testing of avionics systems. The Air Force continues to work with Boeing to develop critical upgrades to the refueling boom and RVS, to support starting integrated testing in late FY25.

SYSTEM DESCRIPTION

The KC-46A tanker aircraft is a modified Boeing 767-200ER commercial airframe with military and technological upgrades. KC-46A upgrades include: a fly-by-wire refueling boom, centerline and WARP hose-drogue baskets, a dual-remote Air Refueling Operator Station enabled by an exterior RVS, additional fuel tanks in the body, a boom refueling receiver receptacle above the cockpit, a Boeing 787 digital cockpit update, Large Aircraft Infrared Countermeasures, a modified ALR-69A radar warning receiver, and Tactical Situational Awareness System that integrates input from the Radio Frequency Self Defense System (RFSDS). The KC-46A cargo bay is designed to accommodate palletized cargo; aeromedical evacuation equipment; and roll-on command, control, and communications gateway payloads.

MISSION

Commanders will use units equipped with the KC-46A to:

- Perform AR in support of six primary missions of nuclear operations support, global strike support, air bridge support, aircraft deployment support, theater support, and special operations support.
- Accomplish the secondary missions of airlift, aeromedical evacuation, emergency AR, air sampling, and support of combat search and rescue.

PROGRAM

The KC-46A Pegasus is an Acquisition Category IC program intended to be the first increment of 183 replacement tankers for the fleet of more than 400 KC-135 and KC-10 tankers. DOT&E approved the Milestone C TEMP 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) will be ready for operational testing in late FY25. Air Mobility Command has approved the KC-46A as a deployable asset to support U.S. Transportation Command taskings with limitations.

» MAJOR CONTRACTOR

- Boeing Commercial Airplanes in conjunction with Boeing Defense, Space & Security – Seattle, Washington

TEST ADEQUACY

In April 2024, AFOTEC successfully completed all 18 IOT&E flight test points associated with the WARP system (WARPS). AFOTEC has now collected 85 percent of the planned IOT&E flight test data, but cannot complete the remaining IOT&E events until the program office implements the final boom and RVS upgrades. The test community expects to begin developmental flight testing of the boom redesign and RVS (version 2.0) in FY25. Operational testing will be fully integrated with this effort and all remaining IOT&E test events will be completed in conjunction with developmental test objectives. DOT&E will complete its assessment and publish an IOT&E report after integrated flight testing is complete for the boom redesign and RVS (version 2.0).

KC-46A IOT&E has been ongoing since May 2019. AFOTEC has continued to collect data, in accordance with the DOT&E-approved test plan, to support assessments for sortie generation, AR, airlift, aeromedical evacuation, survivability through threat-avoidance, and sustained operations under adversarial cybersecurity conditions. Since 2019, DOT&E has been periodically observing and continually monitoring all IOT&E testing.

In June 2024, two aircrews from the 22nd Air Refueling Wing completed the first KC-46A nonstop circumnavigation flight with a 45-hour refueling mission starting and finishing at McConnell AFB, Wichita, Kansas. As part of the Maximum Endurance Operation for KC-46A, the crew refueled B-2 bombers, C-17 airlift, F-15E, and other KC-46A aircraft over the 45-hour mission.

The KC-46A Joint Reliability and Maintainability Evaluation Team has adjudicated and analyzed over 90,000 flight hours of maintenance data. AFOTEC has collected 15 times its originally required operational suitability flight test data and no longer tracks detailed suitability data; the program office and developmental test organization continue to collect and analyze fleet suitability metrics. AFOTEC will conduct separate suitability test data analysis during operational test of upgrades to the refueling boom and RVS.

AFOTEC completed its final phase of cooperative vulnerability and penetration assessment cyber testing in December 2023 and plans to complete cyber testing with two adversarial assessments in 1QFY25.

PERFORMANCE

» EFFECTIVENESS

The KC-46A is capable of refueling 26 of 27 candidate receiver aircraft types with some restrictions that limit the availability in certain environmental conditions and aircraft configurations. The 26th candidate receiver will resume testing after the boom upgrades are complete.

Operational testing of the WARPS identified potential concerns while using the system in icing conditions. The Air Force has an interim plan to use the system if icing conditions exist and is pursuing a long-term solution.

Furthermore, when WARPS are installed, there is an aircraft and weight balance consideration affecting operations when refueling both boom and drogue receiver aircraft. This is expected to be resolved in a future weight and balance tool software upgrade.

The program office is continuing to remediate all previously reported Category 1 deficiencies. The program still has three outstanding Category 1 deficiencies related to the existing refueling boom and RVS that will be resolved with the boom telescope redesign and the RVS 2.0 upgrade. The Category 1 deficiencies are associated with the fuel manifold system, cracks and leaks in the refueling receptacle drain line, and cracks in the auxiliary power unit drain mast, which have not been resolved, but engineering redesigns of the receptacles are in progress.

The KC-46A is experiencing systemic failures of bleed air ducts, driving significant parts demand, additional maintenance, and resulting in damage to the aircraft. The deficiency was first identified in November 2023, and initially adjudicated as a Category 2. However, the number of aircraft affected, and the number of repeat failures, drove the program office to upgrade the deficiency to Category 1. This upgrade is appropriate due to no known acceptable workarounds in terms of supply support, repair support, and the significant additional burden on maintenance. Boeing and the Air Force are currently modeling and flight testing temporary procedures to alleviate the issue as they validate the temporary workarounds and future design modifications. This deficiency is not considered a safety of flight issue.

In FY24, the KC-46A Program Office obtained new receiver certifications for the following aircraft: E-6, F-15EX, F-16 Aggressors, and F-16 Thunderbirds. The KC-46A Program Office continues to work with the Air Force, as well as foreign partners, to obtain air refueling receiver certifications for additional aircraft. The program office is also waiting for a refueling boom upgrade to complete receiver certification on the A-10.

» SUITABILITY

The KC-46A is not meeting many of its suitability metrics. The operational availability (≥80 percent threshold) and mission capable rate (≥90 percent threshold) slightly decreased throughout FY24, well below their threshold requirements. Moreover, when accounting for partially mission capable aircraft that are unable to perform their primary AR mission (e.g., due to a broken boom), the effective mission capable rate falls an additional 24 percent on average. The program continues to suffer from prolonged maintenance repair times due to supply issues with parts needed for repair.

In March 2024, the KC-46A program experienced a two-month delay in delivering new aircraft due to the discovery of broken part associated with the boom. Inspections of aircraft off the production line found a broken gimbal nut lockwire, a part important for the directional movement of the refueling boom. Aircraft acceptance was temporarily delayed while inspection of all aircraft took place to ensure safety of flight. The program still achieved the planned delivery of 17 aircraft in FY24.

» SURVIVABILITY

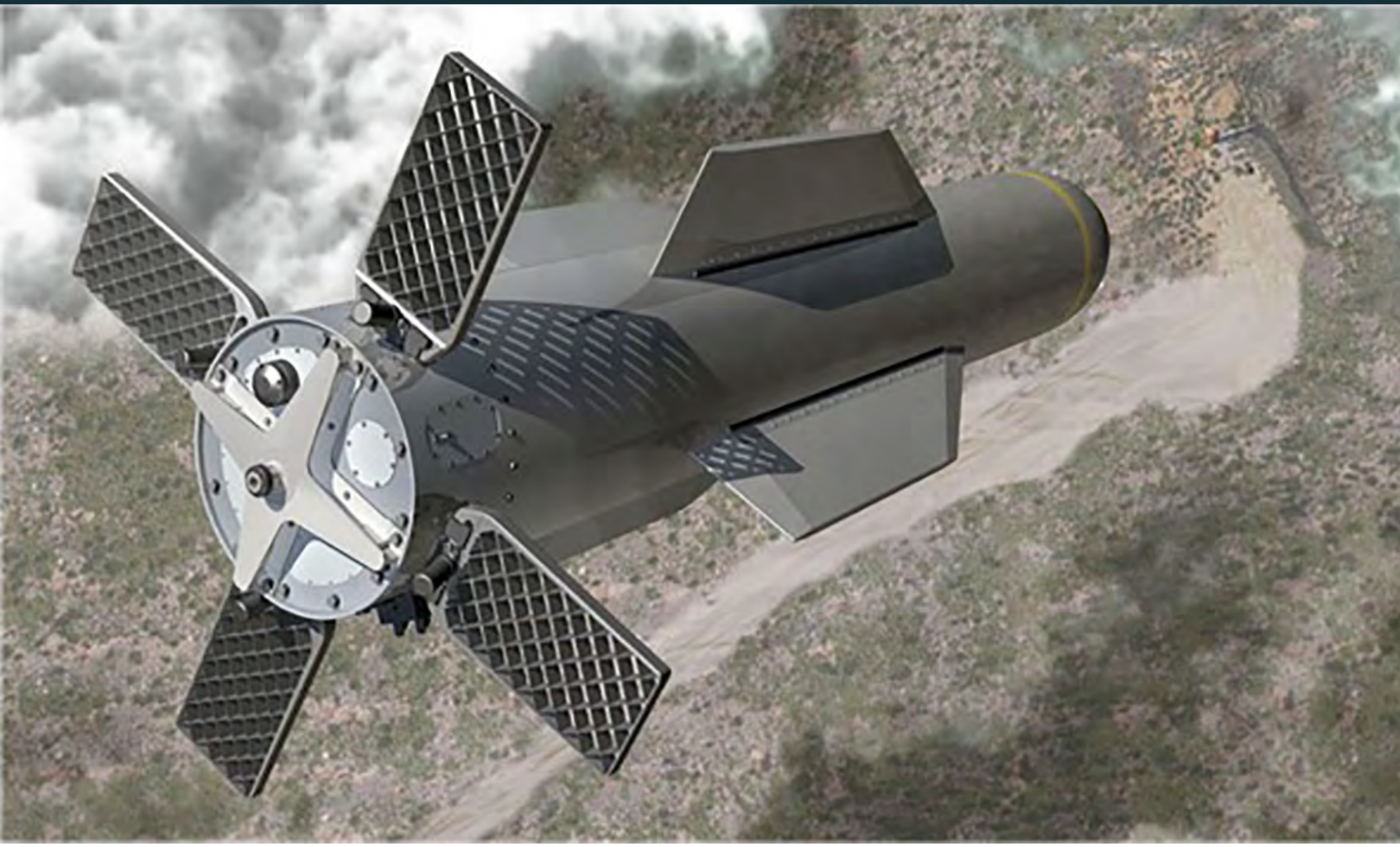
The KC-46A program office continues to develop RFSDS system software upgrades to improve survivability. The developmental testing of software version 6.0 will begin in 4QFY24. Flight testing of RFSDS (version 6.0) is scheduled for 1QFY25. Software updates to RFSDS are slated to improve the clarity of information presented to aircrew to support threat avoidance capabilities. Further testing is required to determine if version 6.0 upgrades are sufficient to support increased survivability of KC-46A in a contested environment.

RECOMMENDATIONS

The Air Force should:

1. As recommended in the FY23 Annual Report, continue to pursue design changes necessary to close the remaining Category 1 deficiencies.
2. Develop and implement a strategy to address high drivers of availability and mission capable rate shortfalls.
3. Collect additional operational test data on the RFSDS during developmental testing of software updates and share with DOT&E to use for IOT&E reporting.

Massive Ordnance Penetrator (MOP) Modification



In FY24, the Air Force concluded subscale lethality testing, conducted an end-to-end full-scale test of the smart fuze, and completed testing of a fix to an integration issue with the B-2. The Air Force has not fully funded the final full-scale tests required to support fielding of the Large Penetrator Smart Fuze (LPSF) enabled GBU-57 Massive Ordnance Penetrator (MOP).

SYSTEM DESCRIPTION

The 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 LPSF integrates advanced smart fuze capability into the MOP warhead, providing increased probability of kill against HDBTs by mitigating the risk of target intelligence uncertainty.

MISSION

Combatant commanders will use MOP to achieve national security objectives with a low-observable, platform-deliverable, conventional HDBT-defeat capability.

PROGRAM

The GBU-57 MOP Modification is an Acquisition Category II program. The Air Force established the LPSF Quick Reaction Capability program in August 2018 to respond to a validated urgent operational need, to integrate and qualify a smart fuze capability into the MOP that had been previously fielded as the Enhanced Threat Response weapon modifications. This upgrade, known as MOP Modification, provides the capability to hold at risk additional high-value HDBTs with limited threat intelligence.

The MOP Modification program intends to finalize the smart fuze software, improve weaponeering tactics, and validate through demonstration, lower-risk smart fuze capability against a full-scale, high-fidelity underground target.

Due to program funding reprioritization, Defense Threat Reduction Agency (DTRA) contract challenges that affected the ability to construct targets to support testing, and modifications to the delivery platform, the MOP Modification program was unable to execute planned testing in FY21 and FY22. The Air Force rescheduled the test events into FY23 and FY24. Changes made by DTRA to expedite the contracting and test plan review process have resulted in no material headway, and delays continue. While significantly delayed, the program was able to execute testing at the end of FY23 and in FY24. Despite the delays in test execution and reductions in subscale testing, the program is proceeding with key performance milestones.

The program office is planning to submit a TEMP in 1QFY25 to DOT&E for approval to formalize the test program and resource requirements. The TEMP will articulate the resources required to complete the LPSF MOP Modification test effort.

» MAJOR CONTRACTOR

- Boeing Defense, Space & Security – St. Louis, Missouri

TEST ADEQUACY

Subscale lethality testing was reduced in scope (by approximately 50 percent) due to funding redirection from the Air Force and test execution cost growth within DTRA. The reduced subscale test effort concluded in September 2024. The DoD has limited test locations that allow for subscale and full-scale test bed construction, leading to high-demand and expensive, long-lead time, and custom-tailored test beds.

The Air Force conducted two full-scale tests in FY24 to verify fixes to a B-2 integration issue. The second of the two full-scale test events also used the LPSF in a full-scale testbed.

PERFORMANCE

» LETHALITY, SUITABILITY, AND SURVIVABILITY

DOT&E sent a classified memorandum to the SECDEF in August 2024, providing an update on the MOP integration with the B-2. DOT&E will provide a classified report on the LPSF following the conclusion of the MOP Modification testing in FY28.

RECOMMENDATIONS

The Air Force should:

1. Submit to DOT&E a TEMP that reflects a resource plan to complete the remaining LPSF T&E activities.
2. Revalidate the urgent operational need requirement from July 2018 for the LPSF Quick Reaction Capability program, as recommended in the FY23 Annual Report.
3. Fully fund the remaining full-scale test events.

DTRA should:

1. Continue to streamline contracting and test plan review processes to minimize delays and cost growth for target construction and test execution, as recommended in the FY22 and FY23 Annual Reports.

MH-139A Grey Wolf

In February 2024, the MH-139A program completed government-led developmental testing (DT) and is progressing toward IOT&E. However, the program still needs to complete crucial maintenance and training objectives to meet IOT&E entrance criteria. IOT&E is currently scheduled to begin in 2QFY25.

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.

MISSION

The Air Force intends for the MH-139A to replace the UH-1N to provide rapid transport capability for two primary commands:

- Air Force Global Strike Command will use the MH-139A to support nuclear security missions by providing emergency security response and convoy escort at Minot AFB, North Dakota; Malmstrom AFB, Montana; and Francis E. Warren AFB, Wyoming.
- Air Force District of Washington will use the MH-139A to provide contingency response, continuity of operations, and executive transport for senior government officials in the National Capital Region.

In addition, the Air Force Reserve Command will provide formal flight training at Maxwell AFB, Alabama. All commands will perform search and rescue via the National Search and Rescue Plan and Defense Support of Civil Authorities.

PROGRAM

MH-139A is an Acquisition Category IB program. DOT&E approved the Alternative LFT&E Strategy in May 2019 and the Milestone C TEMP in January 2023. In February 2023, DOT&E published an observation report to inform the Milestone C decision, which the Air Force executed in March 2023.

In FY24, the Air Force reduced the planned aircraft procurement and no longer intends to support the Air Force Materiel Command at Eglin AFB, Florida, and the Air Education and Training Command at Fairchild AFB, Washington, with MH-139A.

The MH-139A acquisition strategy relies on contractor flight testing to obtain a series of civil Supplemental Type Certificate (STC) approvals to expand MH-139A capabilities and support the military flight releases (MFR) required for government-led DT and operational testing. The number of STCs has grown over the course of the program. To date, six of nine STCs have been approved. Due to further delays in the remaining STC approvals, the Air Force obtained approval of two MFRs in October 2024 to support aircrew training and operational testing. IOT&E is currently scheduled to begin in 2QFY25. DOT&E will provide a full assessment of operational effectiveness, suitability, and survivability following the completion of IOT&E.

» MAJOR CONTRACTOR

- Boeing Defense, Space & Security – Ridley Park, Pennsylvania

TEST ADEQUACY

The Air Force completed the planned government-led DT in February 2024. This FY24 testing included the SkyFlight mission planning system; flare effectiveness; M240 weapon system effects; and heavy weight, high-density-altitude testing. The Air Force is completing the DT reports and has provided preliminary data to support the program's entrance into IOT&E.

The Air Force is conducting two additional areas of DT to resolve early problem discovery. First, integration testing is required for an additional radio required for Air Force Global Strike Command missions. Second, early testing of austere landings showed that dust and debris from the ground may be ingested into engine air intakes and degrade engine performance. The Air Force is evaluating the need to conduct additional testing to determine the effect of austere landings on performance and maintenance of the engines.

Despite the completion of government-led DT, the MH-139A program has not met several IOT&E entrance criteria. First, the program is behind schedule on integrating contractor maintenance data into the Air Force Integrated Maintenance Data System. These maintenance data are required to support both IOT&E and normal operations with fielded aircraft. The remaining entrance criteria are the delivery of operationally representative aircraft; complete flight and maintenance technical orders with the new radio and environmental control system; and fully trained flight crews and maintenance personnel.

With DOT&E approval, the Air Force Operational Test and Evaluation Center conducted the first phase of cyber testing on the MH-139A in July and September 2024 in accordance with their submitted test plan and observed by DOT&E.

The Air Force completed live fire testing of the flight controls, vertical tail rotor drive, and fuel systems per DOT&E-approved test plans and observed by DOT&E. Low-energy laser, ballistic vulnerability, occupant casualty, and integrated survivability analyses are in progress.

As reported in previous years, the Air Force has not yet conducted the approved testing of the MH-139A against electromagnetic pulse (EMP), as required by the Alternative LFT&E Strategy. In lieu of the approved testing, the Air Force proposed to conduct an analysis of flight-critical systems to determine if MH-139A meets the EMP survivability requirement in the Capability Production Document. The program office submitted its EMP flight-critical analysis for DOT&E review in October 2024.

PERFORMANCE

» EFFECTIVENESS

The Air Force continues to make progress addressing previously reported deficiencies, but performance concerns remain that present a risk to MH-139A meeting operational effectiveness requirements.

To address previously reported concerns about the M240 weapon system malfunctions, the program developed changes in the spent-brass catch bag and the ammunition feed system. A gun mount redesign is in development but will not be completed prior to IOT&E.

The MH-139A intercommunication system in the cabin is expected to require a redesign, which will not be completed prior to IOT&E.

» SUITABILITY

The program needs to address several challenges for the MH-139A to be operationally suitable. As discussed above, engine ingestion of dust and debris may cause long-term maintenance issues if not resolved. This is in addition to previously reported concerns about engine maintenance caused by expansion of the aircraft flight envelope and higher power requirements. Moreover, carbon buildup has been identified in several parts of the aircraft's engine including the engine fuel nozzles.

Previously reported concerns regarding cabin seating constraints and the commercial-derivative mission planning software requiring stand-alone computer installations are not yet resolved.

» SURVIVABILITY

The program office needs to address challenges for the MH-139A to be survivable against anticipated threats. The original contractor-proposed fuel cell design did not meet the required self-sealing military requirements for vendor material qualification against the specified projectile threat. Subsequent testing focused on the design's ability to inhibit sustained dry bay fires.

RECOMMENDATIONS

The Air Force should:

1. Develop corrective action plans for deficiencies that affect operational requirements, including the intercommunication system, M240 weapon system, austere landings, and cabin configuration, as recommended in the FY22 and FY23 Annual Reports.
2. Ensure that sufficient aircraft in an operationally representative configuration, with trained flight crews, maintenance support, and all associated support equipment, consistent with approved concepts of operations, are available for the start of IOT&E.

Small Diameter Bomb Increment II (SDB II)

In February 2024, DOT&E published an early fielding report on Small Diameter Bomb Increment II (SDB II) as integrated on F/A-18E/F aircraft. In FY24, the SDB II program continued integration testing on the F-35B/C and F/A-18E/F. The program made significant progress resolving cryptographic information delivery limitations. However, military test range availability, weapon mission planning, and weapon and aircraft Operational Flight Program (OFP) compatibility issues continued to delay test progress. This resulted in zero successful F-35B/C operational tests and two successful F/A-18E/F operational tests in FY24, delaying completion of the quick reaction assessment (QRA) until FY25. The program office now anticipates SDB II initial operational capability (IOC) on F/A-18E/F in FY25 and on F-35B/C in FY26.

SYSTEM DESCRIPTION

SDB II, also known as the GBU-53/B Stormbreaker, is the second increment of a 250-pound air-to-ground glide bomb. It is a network-enabled weapon (NEW) equipped with an encrypted weapon data link (WDL) radio that allows it to destroy moving targets in adverse weather at standoff ranges. When launched, SDB II guides to a designated target cue using a GPS-aided inertial navigation unit. In normal attack mode, the attacking aircraft or a third party updates the target location with inflight target updates sent via the WDL. Finally, the weapon uses a multi-mode seeker to precisely locate, identify, and terminally guide to the target. SDB II also has laser illuminated attack and coordinate attack modes to engage laser-illuminated targets or GPS coordinates.

MISSION

Combatant commanders will use SDB II to attack stationary and moving ground and littoral targets at standoff ranges in a variety of conditions including adverse weather.

PROGRAM

SDB II is a joint interest Air Force and Navy Acquisition Category IC program intended to deliver expanded capability deferred from SDB I. DOT&E approved the SDB II Milestone C (MS C) TEMP in April 2015. The MS C TEMP outlines a two-phase Multi-Service Operational Test and Evaluation (MOT&E). Phase I achieved SDB II fielding on the F-15E in FY20 with IOC declared in September 2022. Phase II intends to achieve early fielding with limited capability on the F-35B/C in FY25, followed by IOC in FY26. In FY20, the Navy initiated a QRA to integrate SDB II onto the F/A-18E/F. DOT&E approved a six-event QRA test plan. Despite significant delays executing the test plan, the Navy declared early fielding on the F/A-18E/F in October 2023, prior to completing the QRA. DOT&E published an early fielding report in February 2024. DOT&E will publish a QRA report in FY25 to support the Navy's IOC decision.

The program office is drafting a full-rate production (FRP) TEMP and anticipates an FRP decision in 3QFY25, following completion of the F-35B/C testing and the publication of DOT&E's report.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX – Tucson, Arizona

TEST ADEQUACY

During FY24, the Navy conducted two of the remaining four live-fly operational tests for F/A-18E/F integration. DOT&E observed these events, which the Navy executed in accordance with a DOT&E-approved test plan and test plan change. Due to overland range safety limitations, the maximum employment range was limited below the program's threshold requirement. Other range safety restrictions continue to impose significant limitations on SDB II employment envelopes and F-35 self-lasing. These restrictions prevent testing SDB II's full operational capabilities.

The Navy attempted seven times to accomplish the remaining two test events at Point Mugu Sea Range to complete the F/A-18E/F QRA, with the following outcomes:

- One attempt was canceled in November 2023 due to a bomb rack unit issue resulting in a hung weapon.
- One mission in December 2023 and two missions in May 2024 were unsuccessful due to weather on the designated test range.
- Unsuccessful loading of the correct cryptographic keys into the weapon in February 2024 led to canceling two attempts. One of these attempts would have been canceled because the Federal Aviation Administration did not provide clearance to operate the weapon on the Link 16 network, which is a recurring issue affecting NEW testing across the DoD.
- The August 2024 attempt was unsuccessful due to a malfunction on one weapon and a combination of weather on the designated test range and incompatible Link 16 networks between the F/A-18E/F aircraft and the P-8 aircraft for the second weapon.

Due to these unsuccessful attempts, the last two test events are scheduled for 1QFY25. Moreover, delays in the F-35 30R08 OFP development and integration issues with SDB II prevented the program from conducting any operational tests on the F-35 in FY24.

MOT&E Phase I cyber survivability testing, conducted by the Air Force in FY19, was inadequate to support DOT&E survivability evaluation. The test asset was not production representative and testing lacked adequate documentation and engineering support to determine the emulated cyber threat's level of sophistication. The program office is working with DOT&E to rectify these shortfalls prior to the FRP decision. Cyber survivability testing is planned for FY25 as part of MOT&E Phase II.

PERFORMANCE

» EFFECTIVENESS

MOT&E Phase I verified SDB II's operational effectiveness on the F-15E. The program has not yet demonstrated operational effectiveness on the F/A-18E/F or the F-35B/C. As discussed in the FY23 Annual Report, operational users had difficulty employing full SDB II NEW functionality on the F/A-18E/F. Many of these challenges were resolved prior to the two FY24 operational tests, during which the SDB II performed as expected in normal mode against one static and one moving land-based target. Recent laboratory testing also revealed the potential cause of extended Link 16 network entry times. The Navy will verify the proposed fix on the remaining two QRA test events in FY25.

FY22 reporting highlighted a hardware issue affecting F/A-18E/F SDB II employment during bomb rack ejection. While formal analysis is ongoing, initial results indicate the materiel solution implemented in FY24 will reduce the likelihood of degraded weapon performance.

A developmental test in 2QFY24 on SDB II revealed a targeting software anomaly, which will be resolved in the SDB II OFP and verified in FY25 during F-35 MOT&E Phase II.

» LETHALITY

MOT&E Phase I verified SDB II's lethality against a variety of static and moving targets including main battle tanks, infantry fighting vehicles, anti-aircraft guns, surface-to-air missile target erector-launchers, and small patrol boats. Additional modeling and simulation would be necessary to verify SDB II lethality against small patrol boats and fast attack craft, if included in the SDB II target set.

» SUITABILITY

Current data available are insufficient to provide a preliminary assessment of SDB II suitability. MOT&E Phase I, completed in FY20, first highlighted concerns with cryptographic key loading and SDB II mission planning for the SDB II as employed by the F-15E. The process for synchronizing cryptographic keys across the weapon, the mission planning environment, and the key filler devices remains cumbersome and error prone. However, the program office has made significant progress. Operational squadrons are now consistently able to load the correct keys into the weapon and achieve NEW functionality in FY24. The program has not yet demonstrated interoperability with the F/A-18E/F or the F-35B/C.

» SURVIVABILITY

The cyber shortfalls from MOT&E Phase I have not yet been addressed during MOT&E Phase II. The Navy's Operational Test and Evaluation Force is working with the program office to submit an updated cyber survivability test plan to DOT&E before conducting a cyber survivability evaluation.

RECOMMENDATIONS

As stated in the FY23 Annual Report, the DoD should:

1. Continue to streamline cryptographic material delivery, management, training, loading, and verification processes.
2. Continue to work with military test ranges to mitigate F-35 self-lasing restrictions and allow operationally representative SDB II employment by all platforms.
3. Work with the Federal Aviation Administration to develop a timely approval process and

reasonable safety measures that will allow the DoD to test NEWs in restricted airspace.

As stated in the FY23 Annual Report, the Navy should:

1. Continue to develop and fund an adequate MOT&E Phase II cyber survivability T&E.

As stated in the FY23 Annual Report, the SDB II Program Office should:

1. Update the FRP TEMP to reflect the updated MOT&E Phase II cyber survivability strategy and submit for DOT&E approval.
2. Continue efforts to improve the mission planning process across all platforms, particularly regarding cryptographic data entry.

T-7A Advanced Pilot Training (APT)

In FY24, Boeing continued T-7A developmental testing (DT) using contractor-owned-and-operated prototype aircraft; and the Air Force began government-led DT using engineering-and-manufacturing-development (EMD) aircraft. The program office plans to begin IOT&E in FY27.

SYSTEM DESCRIPTION

The Advanced Pilot Training (APT) Family of Systems (FoS) includes the T-7A Red Hawk aircraft and ground-based training systems (GBTS). It replaces the Air Force's fleet of T-38C aircraft and associated simulators.

The T-7A is a two-seat trainer powered by a single afterburning turbofan engine. The aircraft uses digital avionics and fly-by-wire flight controls that emulate the characteristics of fifth-generation fighters. GBTS devices include the aircrew ground-egress trainer, part-task trainer, and three types of simulators with varying levels of fidelity. T-7A aircraft can be networked with each other and with the simulators via a training data link.

MISSION

Air Education and Training Command (AETC) will use the APT FoS to train student pilots and combat systems officers for assignments in fourth- and fifth-generation fighter and bomber aircraft. Pilot training in the T-7A will include the basic and advanced fighter fundamentals taught in the T-38C and will add sustained high-g maneuvering, advanced sensor management, night-vision goggle operations, and in-flight refueling training.

PROGRAM

APT is an Acquisition Category IB program. The Air Force awarded the contract to Boeing in September 2018. DOT&E approved the Milestone B (MS B) TEMP in January 2018. After declaring a schedule breach in June 2022, the Air Force approved an updated program schedule, which moved the MS C decision threshold date from December 2023 to February 2026 and the full-rate production decision threshold date from September 2025 to January 2028. The MS C TEMP is currently under development.

AETC plans to procure 351 T-7A aircraft, 46 simulators, and associated GBTS for deployment to its five Undergraduate Pilot Training bases: Joint Base San Antonio-Randolph, Texas; Columbus AFB, Mississippi; Laughlin AFB, Texas; Vance AFB, Oklahoma; and Sheppard AFB, Texas.

» MAJOR CONTRACTORS

- The Boeing Company – St. Louis, Missouri
- Saab AB – Linköping, Sweden and Lafayette, Indiana

TEST ADEQUACY

Boeing flew a total of 548.5 hours in two contractor-owned-and-operated prototype aircraft (36.5 hours in FY24). DOT&E will not include test data from these prototype aircraft in its final evaluation of system performance as the prototypes are substantially different from the EMD aircraft contracted. The EMD aircraft will be used for government-led DT and operational testing. Boeing's FY24 DT focused on resolving safety-of-flight issues required for airworthiness certification. These issues including the escape system, flight control software, high angle-of-attack portion of the flight envelope, propulsion, noise and vibration, and departure resistance. The Air Force Operational Test and Evaluation Center (AFOTEC), Detachment 5, provided operational perspective and continuous feedback throughout Boeing's initial design efforts and early DT. AFOTEC published five periodic reports assessing progress towards operational effectiveness and suitability, with a total of 41 recommendations, 37 of which remain open. DOT&E concurs with AFOTEC's assessments and recommendations.

Government-led DT began in December 2023 at Edwards, California. Boeing has delivered three of the five contracted EMD aircraft; two of the aircraft ferried to Edwards in FY24. The Air Force flew 46.9 hours over 46 missions in EMD aircraft, testing wing flutter, flying qualities, and radio navigation test points. The majority of test points in the government DT test plan remain untested. These events include structural loads, subsystems, tanker formation, crew systems, On-Board Oxygen Generation System (OBOGS), mission systems, and high-angle-of-attack testing, which have the potential to drive further software and flight control changes. The program office expects to complete DT in 4QFY26, a delay of more than a year from what was projected in the FY23 Annual Report.

In February 2024, the program completed initial cold and hot weather testing at the McKinley Climatic Laboratory in Eglin, Florida. This initial round of testing revealed several problems that require a second test event at the McKinley Laboratory in 3QFY25.

IOT&E is scheduled to begin in FY27 at Joint Base San Antonio-Randolph, Texas. The APT Program Office, AFOTEC, and DOT&E are collaborating on a MS C TEMP. IOT&E entrance criteria include: four operationally representative aircraft, a full complement of GBTS devices plus one extra weapon system trainer, embedded training software integrated with mission planning in the aircraft and GBTS, and an operationally representative embedded-training, live-virtual-constructive gateway to connect aircraft and simulators. The program office is also working with Boeing to contract testing in the aircraft's transonic region prior to IOT&E. While the APT contract only requires a flight envelope up to Mach 0.95, the T-7A is capable of supersonic flight. Student pilots are highly likely to exceed Mach 1.0 during T-7A designated missions, particularly during the advanced fighter fundamentals course.

PERFORMANCE

» EFFECTIVENESS

Available data are insufficient to provide a DOT&E assessment of operational effectiveness. The program appears to have a clear pathway to resolving known effectiveness issues, such as limited sortie duration and flight characteristics at high angles-of-attack, prior to MS C.

» SUITABILITY

Available data are insufficient to provide a DOT&E assessment of operational suitability. The program office continues to work through known suitability limitations, most notably the aircraft escape system, logistic supportability issues, and Automatic Ground Collision Avoidance System (AGCAS).

As reported in the FY22 and FY23 Annual Reports, the T-7A emergency escape system does not meet minimum safety requirements for the Air Force's airworthiness certification and is currently operating with high-risk acceptance for air worthiness. A February 2024 sled test showed improvement at medium-speed ejections for the ejection seat sequencing. The program executed a high-speed test in June 2024 where the seat sequenced correctly, but a seat hose interfered with the seat sequencer switch, which could lead to an incorrect ejection mode. In the same test, the redesigned canopy fracturing system pattern did not function properly. The program must successfully complete seven more sled tests before the escape system can be certified for airworthiness and IOT&E.

The program office also continued to make progress on the T-7A OBOGS. The draft T-7A OBOGS test plan calls for 46 data points collected over 10 ground and 100 hours of flight test events, including high and sustained-g maneuvering. The integrated test team will continue to collect OBOGS test data during future IOT&E, as system components age and approach regularly scheduled maintenance and replacement. DOT&E will evaluate OBOGS performance in accordance with the current military standards document (MIL-STD-3050A), which incorporates lessons learned from several fighter aircraft mishaps.

AGCAS is another known suitability limitation. Fighter aircraft employ AGCAS to prevent loss of life during sustained high-g maneuvers, which can cause the pilot to lose consciousness. While the formal requirements for APT did not include AGCAS, the program office is developing a strategy to start AGCAS integration in FY26.

» SURVIVABILITY

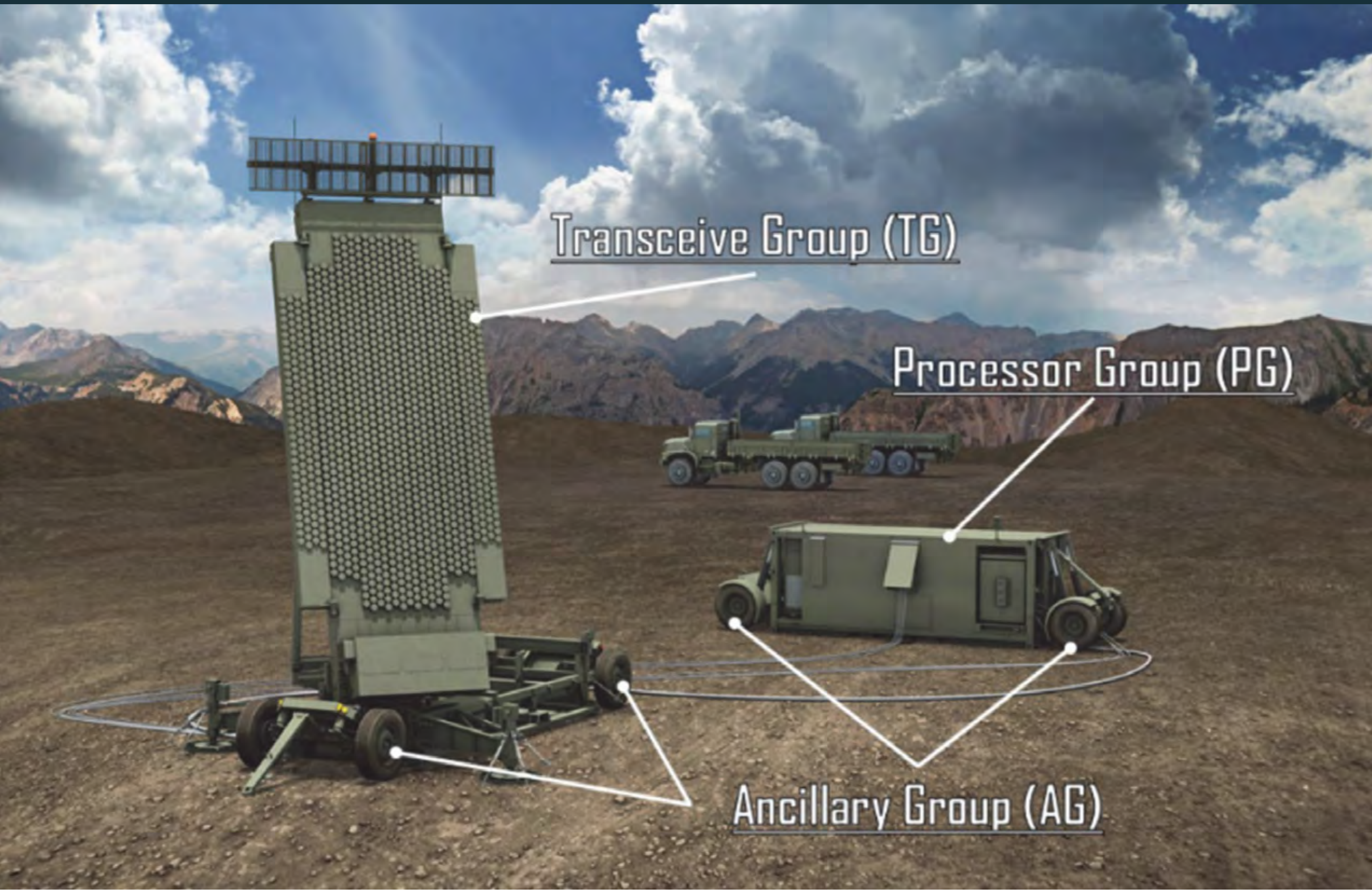
Currently available data are insufficient to provide any survivability assessment. The APT FoS uses a training data link to connect T-7A aircraft with each other and to ground-based training systems. During FY24, the APT Program Office updated the Mission-Based Cyber Risk Assessment and conducted a fourth adversarial cyber developmental assessment of aircraft hardware, using a manned flight hardware simulator and GBTS simulator devices. These events will define the scope and resources outlined in the MS C TEMP to conduct cyber survivability testing on operationally representative aircraft and GBTS during IOT&E.

RECOMMENDATIONS

The Air Force should:

1. Continue addressing AFOTEC's periodic report recommendations and make necessary design changes prior to the start of IOT&E.
2. Continue testing the emergency escape system and implement fixes as needed to meet minimum safety of flight requirements.
3. Complete the integration of AGCAS capability to reduce safety risks.
4. Incorporate on-aircraft and data link cyber risk assessments during integrated testing and IOT&E.
5. Complete testing above Mach 0.95, prior to beginning IOT&E, for safety of flight.
6. Submit the MS C TEMP for DOT&E approval.

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



In FY24, the Air Force paused formal government-led developmental testing (DT), due to system deficiencies, and transitioned to a risk-reduction event after one of four planned weeks of testing. Lockheed Martin continued troubleshooting Three-Dimensional Expeditionary Long-Range Radar (3DELRR) performance and reliability problems during the scheduled test period. The Air Force continued with the Lot 2 production contract award in January 2024 and now plans to start 3DELRR government-led DT in 2QFY25 and IOT&E in 1QFY26.

SYSTEM DESCRIPTION

The 3DELRR TPY-4 is designed to serve as the organic radar for the Air Force Control and Reporting Center (CRC) Weapon System (WS), providing the capability to perform long-range detection of both air-breathing threats and theater ballistic missiles. The 3DELRR employs a single-face, rotating, active electronically scanned array with a highly distributed and scalable digital beam forming architecture.

The active electronically scanned array incorporates power-efficient, reliable, and commercially sourced Gallium Nitride transmitters; low-noise digital receivers; and efficient power conversion.

MISSION

The Air Force employs the CRC WS to conduct battle management, command and control, air surveillance, combat identification, airspace management, and tactical data link management to enable fluid, continuous offensive and defense operations. The 3DELRR is designed provide the CRC WS with a precise, real-time air picture of sufficient quality to:

- Conduct long-range, wide-area surveillance
- Detect and track air-breathing threats and theater ballistic missiles
- Support CRC WS threat evaluation for timely defensive and offensive action
- Provide positive control of military aircraft

PROGRAM

The Air Force awarded the Lot 2 production contract in January 2024. The 3DELRR program is currently operating as a Middle Tier of Acquisition rapid fielding program, which the Air Force plans to transition to a major capability acquisition program in 1QFY26. The 3DELRR program has a DOT&E-approved TES, which the program office is revising to capture test strategy updates as a result of schedule delays.

» MAJOR CONTRACTOR

- Lockheed Martin Corporation – Syracuse, New York

TEST ADEQUACY

Due to delays in the Federal Aviation Administration's approval of the Radio Frequency Authorization, the Air Force was unable to complete a planned operational assessment (OA) prior to the 3DELRR Lot 2 production contract award in January 2024. The Air Force planned to complete the OA in two parts: (1) data collection at the production acceptance test (PAT), and (2) data collection during the government-led DT. DOT&E observed the validation and verification of requirements and the PAT on Lockheed Martin's 3DELRR test article at a contractor-owned test facility.

The Air Force initially delayed the OA and government-led DT from 1QFY24 to 3QFY24 to give the Air Force time to gain Federal Aviation Administration approval for 3DELRR to radiate. In May 2024, DOT&E observed a period of government-led DT, using Lockheed Martin's 3DELRR test article. Due to system deficiencies, the Air Force paused the formal government-led DT period after one of four planned weeks of testing. This allowed Lockheed Martin to troubleshoot 3DELRR performance and reliability problems during the scheduled test period. Along with production delays, the testing delays will impact the schedule of planned testing outlined in the approved 3DELRR TES.

The Air Force plans to use integrated testing at every opportunity and resource tests for near-peer, threat-representative targets as part of the planned DT that is now scheduled to start in 2QFY25. The Air Force plans to start dedicated IOT&E in 1QFY26.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Lockheed Martin executed the 3DELRR PAT using a pre-production prototype 3DELRR system. Both the 46th Test Squadron and Air Force Operational Test and Evaluation Center personnel were on site for the PAT. While Lockheed Martin assessed that they met 37 system specification requirements, testing did not provide DOT&E adequate data to determine 3DELRR progress toward meeting key operational effectiveness, suitability, and survivability requirements. The 46th Test Squadron scheduled six instrumented aircraft flights during the PAT to collect data on 3DELRR detection capabilities and accuracy, but none of the scheduled aircraft were able to fly during the PAT, due to poor weather conditions.

The Air Force's major goal of the government-led DT was to characterize 3DELRR detection and tracking performance against calibrated spheres, which have known radar cross sections, as aircraft towed the spheres and flew within the 3DELRR detection envelope. However, the Air Force paused formal testing after discovering two system deficiencies: one related to 3DELRR operational effectiveness; and the other related to 3DELRR suitability.

DOT&E will assess 3DELRR progress towards operational effectiveness, suitability, and survivability after the Air Force completes a planned OA in 3QFY25.

RECOMMENDATIONS

The Air Force should:

1. Plan and resource for appropriate threat representative targets, as recommended in the FY22 and FY23 Annual Reports.
2. Update the 3DELRR TES to include describing how the Air Force will mitigate the current schedule-induced risks for an adequate and successful IOT&E and submit to DOT&E for approval.
3. Update the 3DELRR OA test plan to account for the change in testing timelines and scope and submit to DOT&E for approval, prior to transitioning the program to the major capability acquisition pathway.

This page intentionally left blank.

Space Force Programs

This page intentionally left blank.

Global Positioning System (GPS) Enterprise

Ongoing development delays of the Next Generation Operational Control System (OCX) and the Military-Code (M-code) GPS User Equipment (MGUE) program schedules are continuing to delay the U.S. Space Force's GPS-modernized civil, M-code, and navigation warfare functions and the fielding of operationally acceptable M-code-capable receivers. These delays put U.S. and allied warfighters at risk of a lack of access to modernized GPS position, navigation, and timing (PNT) capabilities to support operations.

SYSTEM DESCRIPTION

The GPS Enterprise is a Space Force operated satellite-based global radio navigation system of systems that provides accurate and secure PNT information to users worldwide. It consists of three operational segments: space, control, and military user equipment. The space segment includes 31 operational satellites in the GPS constellation that transmit both civilian and encrypted military signals to users. The control segment (primary and alternate sites) 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 MGUE intended to modernize military GPS receivers, including the ability to receive and use M-code. Beyond military GPS users, there are billions of daily civilian users freely using the civilian signals, including many federal agencies within the U.S. Department of Transportation (DOT) and other various state and tribal agencies.

MISSION

Military and civilian users across the globe use GPS to access PNT information that allows them to conduct a wide variety of missions. GPS military receivers allow military commanders to navigate and maneuver within strategic, operational, and tactical theaters. MGUE Increment 1 receivers will allow military users to access the more secure M-code signal, which is now available across the globe for developmental and user equipment testing. MGUE Increment 2 receivers will include the ability to use Regional Military Protection (RMP), which will concentrate higher M-code signal power broadcast by GPS III Follow-On Production (GPS IIIF) satellites in a targeted region to ensure the warfighter has continued access to PNT data in contested environments.

OCX will provide full M-code and modernized civil signal operations, including: a more accurate Kalman filter to calculate satellite orbits, increased PNT monitoring capabilities, more robust and sophisticated cyber defense capabilities, and additional support to civil signals.

PROGRAM

The GPS Enterprise consists of multiple programs pursuing separate acquisition paths to advance the space, control, and user segments.

- GPS III Satellite – An Acquisition Category (ACAT) IC program which achieved Milestone C (MS C) in January 2011. The last of the GPS III satellites, Space Vehicle 10, was made available for launch in December 2022. Since 2018, the Space Force has successfully launched six GPS III satellites and plans to launch the remaining four satellites between FY25 and FY26.
- GPS IIIF Satellite – An ACAT IB program. These satellites will provide enhanced RMP signals and support for search and rescue services. The Air Force made the GPS IIIF MS C decision in July 2020 following completion of the program's Critical Design Review. The Space Force plans to launch the first GPS IIIF satellite in 3QFY27 and operationally accept it in 2QFY28.
- Operational Control System (OCS) Architecture Evolution Plan (AEP) – The Air Force fielded OCS AEP in 2007. It features two ACAT III upgrades: Contingency Operations (COps) and M-code Early Use. These upgrades allow the system to command and control (C2) GPS III satellites and provide core M-code capability from the existing GPS constellation while maintaining previous civilian and military services.
- OCX – An ACAT ID program awarded in February 2010 with an initial expected completion date of early 2016. OCX achieved MS B in June 2017 and was relieved of MS C requirements. OCX will provide full control of modernized civil and M-code signals and navigation of warfare functions. OCX will replace OCS AEP following a successful constellation transfer that the Space Force currently plans in 4QFY25 with operational acceptance in 1QFY26.
- OCX 3F – A tailored ACAT II program that builds on the software delivered by OCX.

Contingent on successful OCX deployment, the subsequent OCX Block 3F upgrade will allow OCX to support launch as well as C2 GPS IIIF satellites. The Space Force anticipates delivery from the vendor in FY27 and plans to operationally accept OCX 3F in FY28. Since OCX 3F builds on the software delivered by OCX, corresponding schedule slips to OCX affect operational acceptance and reduce any remaining margin in the OCX 3F delivery schedule.

- MGUE Increment 1 – An ACAT IC program that achieved MS B in January 2017 and was relieved of MS C requirements. The program was designed to deliver personnel- and vehicle-based M-code receivers to the warfighter, including improved GPS signal availability in degraded threat environments. Due to program delays resulting in Application-Specific Integrated Circuit (ASIC) obsolescence and limited production, the Army and Marine Corps will not field their respective MGUE lead platforms (i.e. Joint Light Tactical Vehicle and Stryker) with the ground-based MGUE Increment 1 receiver cards. Instead, the Army and Marine Corps plan to use commercially available, MGUE-derived M-code receivers for their ground-based platforms. The commercially derived M-code receivers will undergo user evaluations in fielded platforms outside of the MGUE Increment 1 program of record. The MGUE Increment 1 program delivered an interim functional aviation/maritime receiver card in September 2022. As reported in the FY23 Annual Report, delays continue with both software and hardware builds by MGUE Increment 1 vendors due to multiple open deficiencies. These delays impacted the planned operational test schedules for the two remaining MGUE Increment 1 lead platforms (i.e., the B-2 aircraft and the *Arleigh Burke*-class destroyer). The test schedule of both the B-2 aircraft and the *Arleigh Burke*-class destroyer is unknown, pending investigation into the operational impacts and resolution timeframe of these open deficiencies
- MGUE Increment 2 – The program is structured as two Middle Tier of Acquisition rapid prototyping efforts. The first is the Miniaturized Serial Interface (MSI) receiver with next-generation ASICs that will deliver improved jam resistance, address MGUE Increment 1 ASIC hardware obsolescence, support the enhanced RMP offered by GPS IIIF satellites, and support low-power applications (e.g., guided munitions). The second is the handheld receiver, which will incorporate the MSI receiver with the prototype unit planned for FY28 availability. The MSI development continues, and the test community is developing test plans for the prototype handheld unit.

DOT&E approved the GPS Enterprise TEMP (E-TEMP) Revision C in August 2021. The Space Force continues to revise the GPS E-TEMP to update threat requirements; address cyber testing; and define the test strategies for OCX, MGUE Increments 1 and 2, Nuclear Detonation Detection System control system upgrades, GPS IIIF satellites, and OCX Block 3F. DOT&E continues to actively support development of updates to the E-TEMP and its annexes, which should consider a full-spectrum threat environment – adequately addressing kinetic, cyber, electromagnetic spectrum, nuclear, and directed energy threats. In FY24, DOT&E supported the Department of Transportation’s (DOT’s) development of an E-TEMP annex and planned testing of civilian signals under OCX control.

» MAJOR CONTRACTORS

Space Segment

- Lockheed Martin Space – Denver, Colorado (GPS III / IIIF satellites)

Control Segment

- Lockheed Martin Space – Denver, Colorado (OCS AEP)
- Raytheon, a subsidiary of RTX – Aurora, Colorado (OCX)
- Raytheon, a subsidiary of RTX – Aurora, Colorado (OCX 3F)

User Segment (MGUE Increments 1 and 2)

- L3Harris Technologies, Inc. – Anaheim, California

- Raytheon, a subsidiary of RTX – El Segundo, California
- BAE Systems – Cedar Rapids, Iowa
- Technology Advancement Group – Ashburn, Virginia

TEST ADEQUACY

No operational testing was conducted in FY24 across the GPS Enterprise. In February 2024, the M-code signal became globally available, giving U.S. and allied forces the ability to conduct testing of the M-code signal anywhere in the world. The Program Management Office conducted initial integrated cyber testing of the GPS IIIF simulator, in preparation for cyber testing of OCX 3F with the first GPS IIIF satellite in FY27. The OCX cyber assessment originally scheduled for 2023 has been delayed until 4QFY25 (a change from 4QFY24 in last year's annual report), the GPS Enterprise IOT&E is scheduled for 1QFY26, and the GPS Enterprise OCX/GPS III/MGUE Inc 1 Multi-Service Operational Test and Evaluation is scheduled for 2QFY26.

As part of the recommendations from the 2016 Nunn-McCurdy program breach for OCX, the Air Force implemented additional cyber survivability improvements to OCS AEP due to the expected delay in OCX delivery. Due to these cyber improvements and ongoing further delays to OCX, the current instantiation of OCS AEP may now be more cyber secure than the initial delivery of the OCX system that will eventually replace it. DOT&E is funding, through its Cyber Assessment Program, a base cyber evaluation of OCS AEP in 2QFY25 to assess the current cyber defense posture and inform the OCX cyber evaluation schedule for mid-late FY25. This will provide a baseline to measure the cyber defense improvements that OCX brings to the GPS Enterprise and inform the decision to transfer the GPS constellation from OCS AEP to OCX in 4QFY25.

The current MGUE Increment 2 handheld receiver operational test schedule does not align with the GPS IIIF launch strategy. The GPS IIIF family of satellites delivers an RMP capability that the MGUE Increment 2 user equipment provides to military units. Without GPS IIIF satellites on orbit, operational testers will be unable to verify that the MGUE Increment 2 user equipment can take advantage of RMP signals in a contested environment. Additionally, due to delays with the program schedule, the MGUE Increment 2 program office does not have a customer for the MGUE Increment 2 handheld receiver. Since operational testing would involve assessing a military unit's ability to carry out their mission using the MGUE Increment 2 user equipment, the current lack of a buyer has delayed the development of an operational test plan.

The DOT and the Federal Aviation Administration have responsibilities for testing civilian GPS-based PNT systems outlined in the Federal Radionavigation Plan. The PMO and operational test agency are incorporating DOT's request to test OCX with a four-GPS-satellite "mini constellation" as a part of a risk reduction opportunity prior to the full constellation transition to OCX. This is a key event, planned for 4QFY25 – ahead of full operational testing – to build confidence the civil signal is compatible with OCX and will support safe and effective commercial air transportation within the United States.

PERFORMANCE

» EFFECTIVENESS

Based on previous operational testing, the current OCS AEP control segment is operationally effective for legacy military signals, legacy civil signals, and M-code signals. GPS operators can currently C2 all GPS satellites except for future GPS IIIF satellites. OCS AEP received the COps upgrade to C2 the newer GPS III satellites. OCX requires the OCX 3F software upgrade to conduct launch and check out of the GPS IIIF satellites. The Space Force plans to operationally accept OCX in 1QFY26 and OCX 3F in FY28; both dates are a year later than what was reported in last year's Annual Report. The first GPS IIIF satellite is still expected to launch in 3QFY27. Any additional schedule delays to OCX 3F will likely impact the launch of the first GPS IIIF satellite.

Contractor system testing of OCX has been on-going since October 2022, with major delays caused by immature mission control software, mission simulator, and training systems. Software delays and overall program schedule slips have been mainly due to inadequate contractor testing, incomplete functional integration between various software components, and the contractor's lack of agile coding experience during development.

The MGUE Increment 1 aviation/maritime receiver card experienced software challenges that resulted in delays that the Space Force is working to address with the delivery of a new software build. Until the Space Force addresses these deficiencies, which likely affect operational performance, the operational test schedules for both the B-2 aircraft and the *Arleigh Burke*-class destroyer lead platforms are on hold. Delays in MGUE receivers have resulted in the Services developing their own M-code receiver capabilities, separate from the MGUE program.

» SUITABILITY

Based on previous operational test reporting, both GPS III satellites and the OCS AEP C2 system are operationally suitable.

Ongoing OCX contractor and development testing continues to reveal software instability and sustainment concerns with operator training and maintenance technical orders that the program office is working to address.

The OCX 3F's first critical capability release adds launch and checkout capabilities to support the launch of GPS IIIF satellites. Delays to OCX, and consequentially OCX 3F, may put the GPS constellation at risk because OCS AEP will be unable to launch or C2 new GPS IIIF satellites to replenish older satellites as they exceed their service life.

» SURVIVABILITY

The Space Force is placing a renewed focus on understanding all threats to the GPS systems across the space vehicle, C2, and user segments to better evaluate the survivability of the GPS Enterprise in operational testing against realistic threats.

RECOMMENDATIONS

The Space Force should:

1. Work with the Services to identify a military unit to operationally use the MGUE Increment 2 handheld receiver and can also support operational testing.
2. Use the cyber survivability findings from the scheduled operational cyber assessments of OCS AEP and OCX to further strengthen the cyber posture of the GPS Enterprise and inform the OCX operational acceptance decision.
3. Adequately address kinetic, cyber, electromagnetic spectrum, nuclear, and directed energy threats to the GPS Enterprise in future TEMP updates and test plans.

Space Command and Control System (Space C2)

The Space Command and Control (Space C2) program continues to progress toward delivery of capabilities that will allow retirement of the Space Defense Operations Center (SPADOC) system. However, the process has been slower than planned. A cyber survivability cooperative vulnerability and penetration assessment (CVPA) was performed on the Advanced Tracking and Launch Analysis System (ATLAS) and other associated Space Domain Awareness (SDA) capabilities in May 2024, in accordance with the DOT&E-approved test plan. OT&E of Space C2 had been planned for FY23 and FY24 but has moved into FY25 due to ongoing software delays.

The Space C2 Program Management Office has increased system stability and made progress on developing operator training and on baselining an operationally relevant system configuration. However, integrated testing of ATLAS, Space C2's primary SDA C2 capability, did not produce relevant data to accomplish OT&E objectives.

SYSTEM DESCRIPTION

The Space C2 system uses a common commercially supported platform to access data and services for user applications that enable command and control operations. Space C2 uses a hybrid cloud — as well as hardware at operations centers — for resiliency and accessibility, and to enable multi-domain operations integrated with classified mission partner capabilities.

The Space C2 system is comprised of five lines of effort (LOE), including:

- LOE 0: System Engineering, Integration, and Test
- LOE 1: Platform, Infrastructure, and Data
- LOE 2: SDA Software
- LOE 3: Theater Support Software
- LOE 4: Space Defense Software

The LOEs deliver capabilities across three broad categories for Space Delta 2 (SDA and Space Battle Management), Space Delta 5 (Combined Space Operations Center), and Space Delta 15 (National Space Defense Center):

- SDA Software focuses on modernizing SDA astrodynamics toolsets.
- Theater Support Software focuses on developing space systems tasking, electronic warfare awareness, and combatant command integration capabilities.
- Space Defense Software focuses on providing operational command and control capability and supporting battle management services for the integration of new and legacy systems to address critical mission needs.

The system has its own continuous integration/continuous deployment pipeline, known as Kobayashi Maru, for capability and application development. As noted in the FY23 report, Space C2's development efforts are still primarily focused on delivering the capabilities that will allow retirement of the SPADOC.

MISSION

Space Force Guardians will use Space C2 to provide a wide range of space defense, SDA C2, and theater support capabilities to facilitate timely, quality battlespace decisions by DoD and mission partners at multiple classification levels. Those capabilities include infrastructure, data and enterprise services, and mission applications to enable responsive, resilient operational-level command and control capabilities for the Space Deltas 2, 5, and 15, and other command and control centers.

PROGRAM

The Space C2 program was initiated as a Development Security Operations (DevSecOps) pathfinder in 2019 and is using the software acquisition pathway. Space C2's entrance into the Execution Phase, originally expected in December 2022, is now expected no earlier than 1QFY25. The program has been on the DOT&E oversight list since FY19 and has a DOT&E-approved TES with approval caveats. An updated version of the TES to address those caveats was delayed by over a year and is now expected in 1QFY25, along with a classified appendix to detail testing for classified Space C2 capabilities.

In FY22, the Space C2 program restructured its capability development efforts to focus on the near-term challenge of retiring the SPADOC system. The restructure was intended to accelerate delivery of ATLAS capabilities to allow for the decommissioning of SPADOC, while deemphasizing the delivery of non-critical applications. The foundational capabilities required to allow for the retirement of SPADOC were the focus of product developers in FY23 and FY24. While progress was made because of the program restructure, product development remains slower than anticipated, and the projected date to decommission SPADOC continues to extend further into approximately mid-FY25, a delay of more than three years from the original timeline.

The Space C2 program uses an integrated testing construct but continues to struggle with implementing the Space Force's Integrated Test Force vision. The program currently implements quarterly integrated testing events to assess SDA C2 capabilities but struggles to define incremental capability operational acceptance

T&E goals and test methodology. The Space C2 Integrated Test Force, established in September 2023, has not yet been able to close out any operational test objectives and now plans to conduct dedicated operational test events, rather than integrated test events, in FY25 to demonstrate the operational capabilities currently performed by SPADOC.

» MAJOR CONTRACTORS

Space C2 is comprised of a multitude of contracts and contractors developing capabilities, including:

- Parsons Corporation, Space Operations Division – Centreville, Virginia
- Omitron, Inc. – Colorado Springs, Colorado
- Tecolote Research, Inc. – Goleta, California
- Systems Planning and Analysis, Inc. – Alexandria, Virginia
- The Boeing Company – El Segundo, California
- General Dynamics Missions Systems – Fairfax, Virginia
- Lockheed Martin Corporation – King of Prussia, Pennsylvania
- Peraton, Inc. – Herndon, Virginia
- Palantir Technologies, Inc. – Denver, Colorado
- L3Harris Technologies, Inc. – Colorado Springs, Colorado
- Leidos Inc. – Reston, Virginia
- ManTech – Herndon, Virginia

TEST ADEQUACY

While integrated test events for ATLAS occurred in FY24, they did not produce operationally relevant data and therefore cannot be used to meet operational test needs, primarily due to delayed capability delivery, a lack of trained operators, and non-operationally representative test environments. ATLAS operational testing is intended to be phased product release testing, aligned with quarterly program increment development timelines, executing as integrated tests known as SDA capability integrated tests (SCITs). SCITs are intended to produce usable data for both developmental and operational testing communities. However, the four SCITs conducted in FY24 did not produce relevant operational test data.

Test activities for ATLAS were useful to the contractor testers, government-led developmental testers, and numerical validation analysts responsible for ensuring ATLAS accuracy meets the minimum legacy program standards. Progress was made towards increasing system stability, baselining an operationally relevant system configuration and development of valid operator training.

A cyber survivability CVPA was performed on ATLAS and other associated SDA capabilities in May 2024 in accordance with a DOT&E-approved test plan. DOT&E observed the event. Test planning for FY25 has shifted towards dedicated operational test events once the ATLAS developers deliver the remaining required capabilities. The Space Force intends to perform end-to-end operational testing of all SPADOC decommissioning-related ATLAS capabilities in FY25. The Space C2 Integrated Test Force plans to conduct a cyber survivability adversarial assessment (AA) of all SDA capabilities, using insights from the CVPA, in 2QFY25.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Insufficient data were collected in FY24 to inform an assessment of operational effectiveness or suitability for the Space C2 program.

» SURVIVABILITY

The CVPA revealed cyber vulnerabilities that the Space Force should address prior to fielding. DOT&E intends to publish an ATLAS cyber survivability report based on results from the May 2024 CVPA and the planned 2QFY25 AA.

RECOMMENDATIONS

As recommended in the FY23 Annual Report, the Space Force should:

1. Continue focused efforts on development and adequate operational testing of SDA capabilities required

to complete the SPADOC decommissioning.

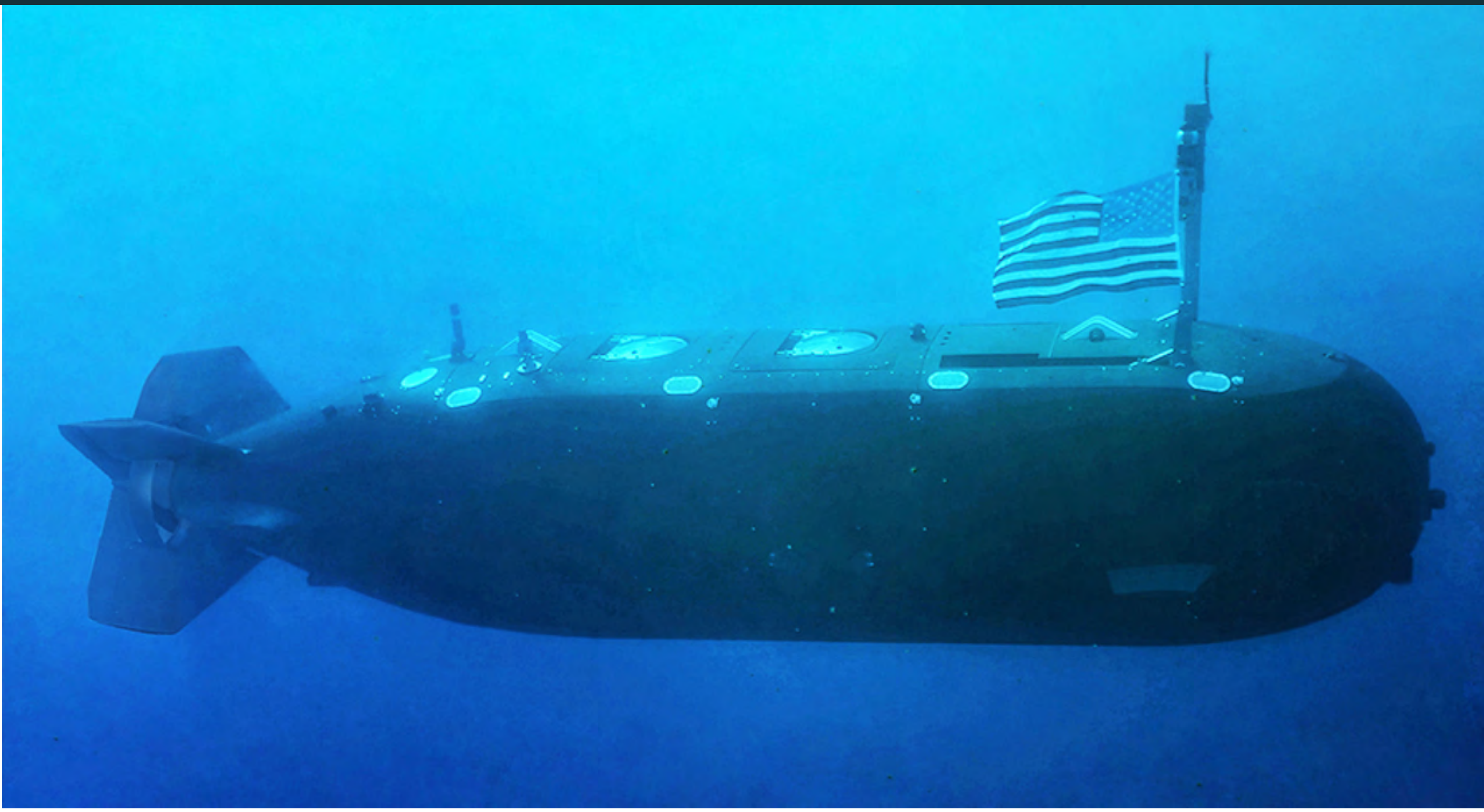
2. Perform additional government-led cyber survivability testing of Space C2 capabilities, including the continuous integration/continuous deployment pipeline and cross domain solutions, as part of major capability releases, once all relevant external users, data feeds, and operational applications are finalized across each applicable security domain.
3. Continue to refine the Integrated Test Force construct to clearly define OT&E phases, as well as common T&E goals and methodology across all Space Force programs, to satisfy the equities of all T&E stakeholders.
4. Finalize the placement of cyber defenders for Space C2-related capabilities.
5. Develop and submit test plans for DOT&E approval.

This page intentionally left blank.

U.S. SPECIAL OPERATIONS COMMAND PROGRAMS

This page intentionally left blank.

Dry Combat Submersible (DCS)



In October 2024, DOT&E published a classified Dry Combat Submersible (DCS) FOT&E report, which focused on the evaluation of DCS integration with a second type of support platform. Launch and recovery of the DCS from the FOT&E support platform improved from the support platform used during IOT&E.

SYSTEM DESCRIPTION

The DCS is a 39.4-foot long, dry submersible with lock-in/lock-out capability for up to eight special operations forces (SOF) occupants. The DCS is battery-powered and operated by two pilots. The DCS maintains a one-atmosphere dry environment within the personnel compartments.

MISSION

U.S. Special Operations Command (USSOCOM) developed DCS to provide SOF with an undersea mobility materiel solution for use in relevant special operations environments.

PROGRAM

DCS is an Acquisition Category III program managed by USSOCOM. DCS achieved Milestone C in 2018, and DOT&E approved a TEMP update within the same year. The Navy completed IOT&E in April 2023, DOT&E published a classified DCS IOT&E report in October 2023, and USSOCOM declared initial operational capability in June 2023. The program delivered three DCSs for SOF. The Navy completed the first phase of FOT&E of the DCS in April 2024. DOT&E published a classified DCS FOT&E report in October 2024. Additional phases of FOT&E are planned in FY25.

» MAJOR CONTRACTOR

- Lockheed Martin Rotary Mission Systems – Riviera Beach, Florida

TEST ADEQUACY

In April 2024, the Navy's Operational Test and Evaluation Force conducted FOT&E in accordance with a DOT&E-approved test plan and with DOT&E observation. Testing evaluated DCS integration with a second type of support vessel. Testing was adequate to determine operational effectiveness of DCS using the support vessel for launch, recovery, and transport of the DCS. Testing provided limited data on operational suitability of the DCS, due to the focus of test on launch and recovery as opposed to full-length missions. Testing did not assess cyber survivability due to the program making no changes to the DCS that would change findings in the October 2023 DCS classified IOT&E report. DOT&E published a classified FOT&E report in October 2024.

PERFORMANCE

» EFFECTIVENESS

DCS is operationally effective within limited operational environments and with limited mission capability from both evaluated support vessels. Launch and recovery from the second support vessel type met program requirements and took less time than that observed for the DCS support vessel in IOT&E. Details of DCS operational effectiveness are in the classified IOT&E and FOT&E reports of October 2023 and October 2024, respectively.

» SUITABILITY

DCS remains below the suitability threshold for some missions. While improvements were made, insufficient data were available from FOT&E to change the assessment from DCS IOT&E. Details are in the classified IOT&E and FOT&E reports.

» SURVIVABILITY

The assessment of DCS survivability in a cyber-contested environment is classified. Details are in the classified IOT&E report.

RECOMMENDATION

USSOCOM should:

1. Address the recommendations in the classified IOT&E and FOT&E reports.

MISSILE DEFENSE SYSTEM

BMD - Ballistic Missile Defense
BLK - Block
MPQ - Mobile, Position Locating, Special Purpose
SM - Standard Missile
SPY - Surface Ship Radar Surveillance
TPY - Transportable Radar Surveillance
UEWR - Upgraded Early Warning Radar

Missile Defense System (MDS)

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. 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 against a small number of medium-range ballistic missile (MRBM) or intermediate-range ballistic missile (IRBM) threats with ranges less than 4,000 kilometers, and against representative raids of short-range ballistic missile (SRBM) threats. DOT&E assesses that the top five challenges for the MDS remain the same as last year:

1. The need for realistic and emerging threat representations in flight and ground testing,
2. The need for an adequate, accredited federation of modeling and simulation (M&S) with well understood and documented limitations to assess MDS effectiveness,
3. Cyber-attack against the MDS,
4. Interoperability and maturation of engagement coordination, and
5. The need for test range infrastructure and instrumentation upgrades.

In FY24, the Missile Defense Agency (MDA) flight tested four significant new MDS capabilities:

- Increased battlespace for the GMD weapon system using the upgraded selectable 2/3-stage interceptor.
- Aegis Ballistic Missile Defense (BMD) ability to conduct an integrated air and missile defense engagement against a raid of two SRBMs with Standard Missile-3 (SM-3) Block IA guided missiles, while concurrently engaging two cruise missile targets with SM-2 Block IIIA guided missiles.
- Aegis BMD ability to track, discriminate, engage, and intercept a MRBM target with countermeasures using an SM-3 Block IIA guided missile.
- Aegis BMD ability to detect, track, engage, and intercept an advanced MRBM target using its Sea-Based Terminal Increment 3 capability with SM-6 Dual II guided missiles with software upgrade.

DOT&E will provide additional information and recommendations in the classified DOT&E FY24 Assessment Report of the MDS to be published in February 2025.

SYSTEM DESCRIPTION

The 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. As shown in Table 1, the MDS consists of six weapon systems, a sensor architecture (i.e., terrestrial, maritime, and global sensors), and a command-and-control element.

Table 1. Elements of MDA's Missile Defense System

Type	U.S. Homeland Defense	Global Regional/Theater Defense	Hypersonic Defense
Weapon Systems	**GMD[a]:** Defends the U.S. homeland against IRBM/ICBM attacks using GBIs to defeat threat missiles during the midcourse segment of flight. The MDA is developing a Next Generation Interceptor to augment the current GBI fleet.	**Aegis BMD[a]:** 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 Aegis SBT (Inc 2 and Inc 3) uses for endo-atmospheric engagements. Aegis BMD can provide or accept target cues via C2BMC. **THAAD[a]:** 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 via C2BMC. THAAD complements the upper-tier Aegis BMD and the lower-tier PAC-3 weapon systems. **Patriot[b]:** Defends U.S. deployed forces and allies from SRBM and MRBM 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. Patriot can accept or provide target cues via C2BMC.	**Aegis SBT (Inc 3)[a]:** Provides critical asset protection at sea and for joint forces ashore against ballistic, maneuverable, and hypersonic glide threats in the terminal phase. **GPI[a]:** Will provide an additional layer of hypersonic defense augmenting Aegis SBT (Inc 3) to increase depth of fire against hypersonic threats. The program is currently competitively developing two prototype interceptors.
Terrestrial and Maritime Sensors	**Cobra Dane Radar[d]:** L-band fixed site phased array radar. **UEWRs[d]:** Ultrahigh frequency fixed site phased array radars. **SBX[a]:** X-band mobile phased array radar located aboard a self-propelled, ocean-going platform. **LRDR[a,d,e]:** S-band two-face fixed site phased array radar.	**AN/SPY-1 Radar[c]:** 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]:** S-band four-face radar being installed on new construction Aegis DDG 51 Flight III destroyers. It will extend Aegis threat detection ranges and provide simultaneous ballistic missile and air defense support. **AN/TPY-2 (FBM) Radar[a]:** X-band single-face transportable phased array radar that also supports U.S. homeland defense. **LTAMDS[b]:** C-band three-face multi-function, multi-mission radar interfacing with IBCS and supporting interoperability with PAC-3.	Leverages U.S. homeland defense, global regional/theater defense, and global sensors.
Global Sensors	**SBIRS[d]:** Satellite constellation of infrared sensors. **BOA[a]:** 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 hypersonic and limited ballistic missile threats and provide fire-control quality data to MDS sensors and weapon systems. MDA launched prototypes in 2QFY24.		
Command and Control	**C2BMC[a]:** 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 LRDR, AN/TPY-2 (FBM) radars, and provides cueing support to BOA.		

Notes:
[a] Under MDA development/sustainment. [b] Under Army development/sustainment. [c] Under Navy development/sustainment. [d] Under Space Force development/sustainment. [e] Under Air Force development/sustainment.

Acronyms: AN/SPY – Army Navy/Surface Ship Radar Surveillance; AN/TPY – Army Navy/Transportable Radar Surveillance; BMD – Ballistic Missile Defense; BMDS – Ballistic Missile Defense System; BOA – BMDS Overhead Persistent Infrared Architecture; C2BMC – Command and Control, Battle Management, and Communications; FBM – Forward-Based Mode; GMD – Ground-based Midcourse Defense; GBI – Ground-Based Interceptors; 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 Radar; SKA – Space-Based Kill Assessment; SM – Standard Missile; SRBM – Short-Range Ballistic Missile; THAAD – Terminal High Altitude Area Defense; UEWR – Upgraded Early Warning Radar

MISSION

The Commanders of U.S. Northern Command (USNORTHCOM), USINDOPACOM, USEUCOM, USCENTCOM, and U.S. Space Command (USSPACECOM) employ the assets of the MDS to defend the United States, deployed forces, and allies against missile threats at all ranges and in all phases of flight.

PROGRAM

The MDS is a single Acquisition Category (ACAT) ID program that encompasses five of its six weapon systems (all but Patriot), most of its sensor architecture, and its command-and-control element. In 2002, the SECDEF granted the MDA special acquisition authorities for the MDS. These authorities allowed it to use tailored processes and milestones to deploy new capability, as soon as technologically possible, to defend the United States and its allies against limited ballistic missile attacks. The mission of MDA is to develop and deploy a layered MDS to defend the United States, its deployed forces, allies, and friends from missile attacks in all phases of flight.

The MDA manages the MDS through a single Missile Defense System Acquisition Baseline (MAB). Each Component Program of Record MAB will contain three baselines for Cost, Schedule, and Performance. MDA maintains responsibility for integrating all elements into the MDS, whether or not the MDA developed the element. The MDA publishes a test program plan 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 is dated September 2024 (version 26.0).

The Army manages the Patriot and Lower Tier Air and Missile Defense Sensor (LTAMDS) programs. Patriot is an ACAT IC program. DOT&E approved the Patriot Post Deployment Build (PDB) 8.1 TEMP in FY20. The LTAMDS program is a Middle Tier of Acquisition program rapid prototyping effort. The Army expects to designate LTAMDS as an ACAT IC program at its Milestone C decision review, planned for 2QFY25. DOT&E approved the LTAMDS initial TEMP in 2019. The program office submitted a TES, which DOT&E approved in August 2024.

The Navy manages the AN/SPY-1 and AN/SPY-6(V)1 radar programs. The AN/SPY-6(V)1 radar is an ACAT IC program. DOT&E approved its TEMP in September 2022.

The Space Force operates and sustains four sensor systems integrated into the MDS: Cobra Dane, five Upgraded Early Warning Radars (UEWRs), the Space-Based Infrared System (SBIRS) constellation, and the Long Range Discrimination Radar (LRDR). The Air Force completed development and initial operational testing for the first three sensor systems prior to them becoming Space Force assets. LRDR will not complete transition and transfer to the United States Space Force until the end of FY25 with the completion of the FTX-26a operational flight test. LRDR has already started providing Space Domain Awareness (SDA) data to the United States Space Force in FY24.

» MAJOR CONTRACTORS

- The Boeing Company
  - GMD Integration, Test and Readiness: Huntsville, Alabama
- Lockheed Martin Corporation
  - Aegis BMD, AAMDS, Aegis SBT, AN/SPY-1 radar, LRDR, and GPI: Moorestown, New Jersey
  - C2BMC: Huntsville, Alabama and Colorado Springs, Colorado
  - NGI AUR in product development: 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
  - GMD Weapon Systems Development and GPI prototype: Huntsville, Alabama
  - GBI Boost Vehicles: Chandler, Arizona

- BOA: Boulder, Colorado; Colorado Springs, Colorado; and Azusa, California
- HBTSS through Prototype Demonstration Phase: Redondo Beach, California and Azusa, California

- RTX
  - GMD EKV, SM-3/6 Interceptors, LTAMDS, and GPI: Tucson, Arizona
  - Patriot 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
- L3Harris Technologies
  - HBTSS through Prototype Demonstration Phase: Fort Wayne, Indiana
- Johns Hopkins University, Applied Physics Laboratory
  - Space-Based Kill Assessment

TEST ADEQUACY

The MDA IMTP established and documents the test requirements, configurations, resources, test objectives, and target solutions for testing Missile Defense System Phased Implementation Plan Increments with specific focus on collecting the data needed for capability assessment and declaration, as well as the verification, validation, and accreditation (VV&A) of the MDS M&S. The Army documents their test strategy through the Patriot TEMP, and the LTAMDS TES, approved by DOT&E in September 2022 and August 2024, respectively. The MDA conducted testing in accordance with the DOT&E-approved IMTP, although some events experienced technical and programmatic delays. Table 2 outlines the 33 flight, ground, high-fidelity M&S, and cyber survivability test events that the MDA, or Army performed or participated in during FY24. For each test event in Table 2, the footnotes indicate whether DOT&E approved the test plan and whether DOT&E observed the event.

Table 2. FY24 Testing

Date	Test	Mission Area	Description
June 2022 – October 2023	Patriot PDB-8.1 LUT[a,d]	Regional/Theater Defense	The Army conducted this OT to assess the effectiveness, suitability, and survivability of the Patriot PDB-8.1 system through flight testing, accredited HWIL scenarios, and cyber survivability testing (CVPA and AA).
October 2023	Air-Launched Rapid Response Weapon Test Flight-3[c,e]	Hypersonic Defense	The MDA participated in this Air Force event to collect hypersonic missile phenomenology and tracking data to inform future capability development.
October 2023	FTM-48[a,d]	Regional/Theater Defense	The Navy and the MDA demonstrated an Aegis BMD IAMD capability to engage a raid of two SRBMs with two SM-3 Block IA guided missiles, while concurrently engaging a raid of two subsonic anti-ship cruise missile drones with four SM-2 Block IIIA guided missiles. This was the first Aegis BMD IAMD flight mission with raids of both BMD and AAW targets, and the largest IAMD test event in the USINDOPACOM AOR to date.
October 2023 – May 2024	UEWR 22-1 Upgrade[a,e]	Homeland Defense	STARCOM conducted OT on each of the five UEWRs to evaluate the operational effectiveness, suitability, and survivability of those systems after the 22-1 upgrade.
November 2023	Glory Trip 248[c,e]	Homeland Defense	The MDA participated in this Air Force Global Strike Command event to collect data, exercise MDS communication links, and perform future capability assessments, although the flight had anomalies.

Table 2. FY24 Testing, continued

Date	Test	Mission Area	Description
November 2023	Tactical Boost Glide-4[c,e]	Hypersonic Defense	The MDA participated in this DARPA/Air Force event to collect hypersonic missile phenomenology and tracking data to inform future capability development.
November 2023	High Operational Tempo for Hypersonics Campaign-3[c,e]	Hypersonic Defense	The MDA participated in this joint Service flight test event, collecting data on new technologies in hypersonic environments.
November 2023	LTAMDS IFTC 23 OA[d]	Regional/Theater Defense	This Army-conducted OA consisted entirely of a three-day HWIL air battle using unaccredited M&S in the primary sector of LTAMDS. The lack of M&S accreditation was not in accordance with the DOT&E-approved test plan and created uncertainty that the results represented reality. Thus DOT&E determined the OA was not adequate to operationally assess the system performance.
November 2023	LTAMDS DT Missile Flight Test – Air Breathing Target[c,d]	Regional/Theater Defense	The Army demonstrated the capability of a unit equipped with LTAMDS to detect, track, engage, intercept, and kill a subscale aircraft target with one PAC-3 missile.
December 2023	LTAMDS DT Missile Flight Test – Patriot-as-a-Target[c,e]	Regional/Theater Defense	The Army demonstrated the capability of a unit equipped with LTAMDS to detect, track, engage, intercept, and kill a close-range ballistic missile target with two PAC-3 missiles.
December 2023	FTG-12[a,d]	Homeland Defense	The MDA and MDS OTA conducted a DT/OT flight test that demonstrated increased battlespace for the GMD weapon system via the upgraded selectable 2/3-stage interceptor.
February 2024	FTX-23[c,d]	Regional/Theater Defense	The MDA and OPTEVFOR conducted a DT/OT that demonstrated an Aegis BMD capability to detect, track, discriminate, engage, and intercept an MRBM target with countermeasures in the midcourse phase of flight using an SM-3 Block IIA guided missile.
February 2024	System Integration and Checkout-09-4 (USEUCOM/ USCENTCOM)[c,e]	Regional/Theater Defense	The MDA and the MDS OTA conducted this DT/OT limited architecture distributed event using operational assets and focused on the verification of operational communication and message flows of regional/theater capabilities.
March 2024	Cyber Test-09[a,d]	Regional/Theater Defense	The MDA conducted CVPA and AA cyber testing on the C2BMC Spiral 8.2-5.1 as configured for USEUCOM defense to assess cyber survivability.
March 2024	Air-Launched Rapid Response Weapon Test Flight-4[c,e]	Hypersonic Defense	The MDA participated in this Air Force event to collect hypersonic missile phenomenology and tracking data to inform future capability development.
March 2024	FTM-32[a,d]	Regional/Theater Defense	The MDA and OPTEVFOR conducted a DT/OT flight test demonstrating Aegis SBT Increment 3 capability to detect, track, engage, and intercept an advanced MRBM target in the terminal phase of flight using SM-6 Dual II guided missiles with software upgrade.
March 2024	LTAMDS DT Missile Flight Test – Long-Range Cruise Missile[c,d]	Regional/Theater Defense	The Army demonstrated the capability of a unit equipped with LTAMDS to detect, track, engage, intercept, and kill a long-range cruise missile target with one PAC-3 missile.

Table 2. FY24 Testing, continued

Date	Test	Mission Area	Description
March 2024	UEWR Cape Cod CVPA[a,d]	Homeland Defense	STARCOM conducted a CVPA on the Cape Cod UEWR to assess its cyber survivability from insider and nearsider threat postures.
March – May 2024	Patriot Communication Obsolescence Upgrade/Digital Exciter Radar Set Operational Demonstration[a,d]	Regional/Theater Defense	The Army conducted this OT to assess the effectiveness, suitability, and survivability of the Patriot Communication Obsolescence Upgrade and Digital Exciter Radar Set system with accredited HWIL scenarios and cyber survivability testing (CVPA and AA).
April – May 2024	SM-3 Block IIA M&S OT Runs for Record, Phase 2B[a,d]	Regional/Theater Defense	The MDA executed and delivered a set of high-fidelity M&S OT runs for record to assess Aegis BMD remote and organic engagement performance against raids of select threats in scenarios relevant to the USINDOPACOM AOR.
April – June 2024	GTI-08b (USNORTHCOM/ USINDOPACOM)[c,e]	Homeland Defense and Regional/Theater Defense	The MDA and the MDS OTA conducted this DT/OT using HWIL laboratory test assets supporting MDS-level capability assessments in USNORTHCOM/USINDOPACOM geographic regions and examining new functions of Aegis BMD and AN/TPY-2 (FBM).
May 2024	Desert Lion[c,e]	International Partner Exercise	The MDA participated in this exercise to test the MDS capability to acquire & collect data on a high velocity, low altitude target for development of future capabilities against similar threats, and to further continued cooperation & partnership with the Australian Defense Force in missile defense development.
June 2024	Joint Flight Campaign Stool Launch[c,e]	Hypersonic Defense	The MDA participated in this Army/Navy event to collect hypersonic missile phenomenology and tracking data to inform future capability development.
June 2024	Glory Trip 250[c,e]	Homeland Defense	The MDA participated in this Air Force Global Strike Command event to collect data, exercise MDS communication links, and perform future capability assessments.
June 2024	Hypersonic Test Bed-1[c,e]	Hypersonic Defense	The NSWC and MDA conducted this experiment to collect data on the hypersonic environment. The rocket-launched hypersonic vehicle was observed by the HBTSS space sensors.
June 2024	Mk21a-2[c,e]	Homeland Defense	The MDA participated in this Air Force launch of an Mk21a reentry vehicle aboard a Minotaur rocket to collect data, exercise MDS communication links, and perform future capability assessments.
July 2024	GMD HWIL Cyber Lab Event[c,e]	Homeland Defense	The MDA conducted a developmental cyber survivability evaluation of the GMD 8B software configuration in an HWIL environment.
July – December 2024	LTAMDS IFTC 24 OA[a,d]	Regional/Theater Defense	The Army conducted this OT to assess the effectiveness, suitability, and survivability of a unit equipped with LTAMDS through flight test, conditionally accredited HWIL scenarios and cyber survivability testing (CVPA and AA).

Table 2. FY24 Testing, continued

Date	Test	Mission Area	Description
July – August 2024	Live Radiate-08b[c,e]	Space Domain Awareness	The MDA and MDS OTA conducted this DT/OT event to assess MDS tasking (C2BMC) and sensor capability (LRDR and AN/TYPY-2 (FBM) in support of the USSPACECOM space domain awareness mission while maintaining missile defense surveillance.
August 2024	C2BMC HWIL Cyber Lab Event[c,e]	Homeland Defense	The MDA conducted a developmental cyber survivability evaluation of the C2BMC Spiral 8.2-5.1 software configuration in support of NORTHCOM/INDOPACOM in an HWIL environment.
August 2024	AN/TPY-2 HWIL Cyber Lab Event[c,e]	Homeland Defense	The MDA conducted a developmental cyber survivability evaluation of the AN/TPY-2 (FBM) CX 5.0 software configuration in an HWIL environment.
August 2024	Pacific Dragon-24[c,e]	Regional/Theater Defense	The MDA participated in this five-event multilateral warfighter exercise. U.S. and allied naval vessels conducted live and simulated intercepts against SRBM targets with SM-3 Block IA or SM-6 Dual I guided missiles. The exercise demonstrated interoperability between U.S. and allied assets.
September 2024	LRDR HWIL Cyber Lab Event[c,e]	Homeland Defense	The MDA conducted a developmental cyber survivability evaluation of the LRDR 1.0.2 software configuration in an HWIL environment.

Notes:
[a] Testing performed per DOT&E-approved test plan. [b] Test plan not approved by DOT&E. [c] Test plan not required by DOT&E. [d] Test observed by DOT&E. [e] Test not observed by DOT&E.

Acronyms: AA – Adversarial Assessment; AAW – Anti-Air Warfare; AN/TPY - Army Navy/Transportable Radar Surveillance; AOR – Area of Responsibility; AUR – All-Up Round; BD+ – Black Dagger Plus; BMD – Ballistic Missile Defense; C2BMC – Command and Control, Battle Management, and Communications; CVPA – Cooperative Vulnerability and Penetration Assessment; DARPA – Defense Advanced Research Project Agency; DT – Developmental Test; FBM – Forward-Based Mode; FTG – Flight Test GMD Weapon System; FTM – Flight Test Aegis Weapon System; FTX – Flight Test Other; FY – Fiscal Year; GMD – Ground-based Midcourse Defense; HBTSS – Hypersonic and Ballistic Tracking Space Sensor; HWIL – Hardware-in-the-Loop; IAMD – Integrated Air and Missile Defense; IFTC – Integrated Fires Test Campaign; LRDR – Long-Range Discrimination Radar; LTAMDS – Lower Tier Air and Missile Defense Sensor; LUT – Limited User Test; M&S – Modeling and Simulation; MDA – Missile Defense Agency; MDS – Missile Defense System; MFT – Missile Flight Test; MRBM – Medium-Range Ballistic Missile; MSE – Missile Segment Enhancement; NSWC – Naval Surface Warfare Center; OA – Operational Assessment; OPTEVFOR – Operational Test Force; OT – Operational Test; OTA – Operational Test Agency; PAC – Patriot Advanced Capability; PDB – Post Deployment Build; SBT – Sea-Based Terminal; SM – Standard Missile; SRBM – Short-Range Ballistic Missile; STARCOM – Space Training and Readiness Command; UEWR – Upgraded Early Warning Radar; USCENTCOM – U.S. Central Command; USEUCOM – U.S. European Command; USINDOPACOM – U.S. Indo-Pacific Command; USNORTHCOM – U.S. Northern Command, USSPACECOM – U.S. Space Command

As previously reported, the need for additional threat representations, independently accredited M&S, and system survivability data in a cyber-contested environment presents significant challenges for completing a comprehensive assessment of the MDS. Specifically:

- The current MDS M&S is not adequate to conduct operational assessments. Realistic and up-to-date representations of threat missile scenes are critical to the assessment of MDS performance. As DOT&E has noted since FY21, the rate of adversary threat development is currently faster than the pace of flight test target and ground test high-fidelity M&S threat model development. The MDA, in conjunction with the MDS Operational Test Agency (OTA), recently chartered a Lethality Model Working Group to support sharing and VV&A of theater threat models among the elements. The MDA has made advancements to their threat modeling process, but models can still take several years to develop.

- Independent accreditation of M&S used in ground tests and high-fidelity analyses is needed to ensure adequate representation of current threat missile capabilities, electronic attacks, countermeasures, vulnerabilities, post-intercept debris, and realistic raid sizes. DOT&E has emphasized this need in previous annual reports. The rate at which the MDA's models have been independently accredited has increased, but significant gaps remain. While over 90 percent of element and sensor models are accredited in ground tests, critical M&S components like newer threat models and post-intercept debris models remain unaccredited. Validation of post-intercept debris models requires flight testing with targets that include threat-representative payloads. As threat and system model capabilities become more complex, the MDA has struggled to maintain a real-time test architecture that can handle this complexity. This issue will become critical as more complex capabilities are added to the MDS, such as the Next Generation Interceptor (NGI) and the Glide Phase Interceptor (GPI), and to support Guam Defense scenarios involving numerous simultaneous air and missile threats. As a complement to the real-time testing, the MDA had been developing the End-to-end Digital Integrated System-level Simulation, a high-fidelity digital modeling architecture needed to assess effectiveness of the MDS. In FY24, the MDA removed funding from the effort. The operational effectiveness of the MDS cannot be fully assessed without such a tool.
- The MDS has an extensive cyber-attack surface, which to date, has not been rigorously tested in operationally realistic settings at the MDS-level. MDS-level cyber survivability assessments with multiple elements, warfighter participation, and federated M&S accredited for performance, are needed to identify the full mission effects of cyber-attacks. To date, the MDA has struggled to maintain the scope of such MDS-level tests as specified in the IMTP, in part because of lack of MDS operational element availability, due to real-world events. The MDA, in coordination with the Services and MDS OTA, should routinely conduct rigorous, operationally realistic cyber testing of the MDS to assess and improve the cyber survivability of critical missile defense capabilities.
- While the MDA strives for operational realism, however, flight and ground test programs and high-fidelity M&S analyses at both the MDS system- and element-level have been limited in the variety of realistic threat countermeasures, electronic attack, post-intercept debris scenes, raid sizes, and multi-element engagement scenarios. As reported in the DOT&E FY22 and FY23 Annual Reports, the MDA often designs flight tests to demonstrate a specific new capability, but not for operational realism. Operationally realistic intercept flight tests are necessary to provide: (1) needed referent data to support VV&A of models used in high-fidelity M&S and ground testing; (2) realistic data on multi-element interactions; and (3) data in multi-domain operations.
- The Army, Navy, and MDA, in coordination with DOT&E, are working to develop a test strategy for the Guam Defense System, which is intended to provide persistent, 360-degree, layered, and integrated air and missile defense capability for the defense of Guam. The proposed architecture is made of both new and existing systems in close proximity and with overlapping areas of regard, with all components working together to defend against cruise, ballistic, and hypersonic threats. This architecture presents a significant integration and test planning challenge. DOT&E assesses that the current test strategy needs significant further development to achieve adequacy. An Agile test program that fully explores interoperability and engagement planning through a coordinated strategy of mutually supporting ground testing, digital M&S, tracking exercises, and intercept flight testing is warranted. Comprehensive suitability and cyber tests are also needed.
- The MDA is also facing a significant test resource shortfall, with two major test support ships, the Pacific Collector and the Pacific Tracker, nearing end-of-life. The MDA has been considering courses of action, but there is a funding gap. NGI and future target characteristics will require shipboard radar upgrades for

these assets. These ships also support flight testing of other major DoD programs.

PERFORMANCE

» U.S. HOMELAND MISSILE DEFENSE

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. In FY24, the MDA demonstrated the increased engagement battlespace of GMD with an intercept flight test using the selectable 2/3-stage interceptor. The AN/TPY-2 Forward-Based Mode (FBM) and Sea-Based X-band (SBX) radars supported GMD during the test. In FY24, the MDA continued hypervelocity impact testing to support development of M&S for NGI lethality assessments.

» REGIONAL/THEATER MISSILE DEFENSE

The regional/theater MDS has demonstrated a capability to defend the USINDOPACOM, USEUCOM, and USCENTCOM areas of responsibility from a small number of MRBM or IRBM threats with ranges less than 4,000 kilometers, and from representative raids of SRBM threats.

Aegis BMD has demonstrated the capability to intercept non-separating, simple-separating, and complex-separating ballistic missiles in the midcourse phase of flight with SM-3 guided missiles, although flight testing and M&S have not addressed all expected threat types, threat features, and raid sizes. In FY24, Aegis BMD conducted its first-ever integrated air and missile defense engagement with a raid of ballistic missiles and a concurrent raid of cruise missiles, and its most stressing engagement against a ballistic missile target with countermeasures. In April 2024, for the first time in a live combat environment, two Aegis BMD destroyers successfully engaged Iranian ballistic missile threats targeting Israel with SM-3 Block IB guided missiles. In FY24 and prior years, Aegis BMD has demonstrated a capability to intercept select ballistic missiles in the terminal phase of flight with its Sea-Based Terminal capability with SM-6 guided missiles.

All fielded Aegis BMD variants have demonstrated sufficient reliability, with operational availabilities that exceed the specification. SM-3 Block IB Threat Upgrade and SM-3 Block IIA guided missiles are reliable, as they meet their threshold reliability metrics, but not with statistical confidence because of the relatively small number of live firings to date. The full production acquisition decision memorandums for the SM-3 Block IB and SM-3 Block IIA require periodic flight testing of these missiles throughout the life of the program, which improves reliability data counts over time. SM-6 missiles have been reliable in anti-air warfare and BMD flight testing.

The Terminal High Altitude Area Defense (THAAD) system has demonstrated the capability to intercept and destroy SRBMs, MRBMs, and IRBMs inside or outside the earth's atmosphere during the terminal phase of flight. However, flight testing and M&S still need to address more complex engagement conditions and realistic raid scenarios. In FY24, the MDA canceled Flight Test THAAD Weapon System-25 (FTT-25) due to the operational status of equipment and unit unavailability resulting from real-world events. The FTT-25 flight test requirements have been reallocated to FTT-26, a FY27 scheduled DT/OT event. The last flight test to use a THAAD interceptor was in FY19, and a future test will not occur until FY27, generating a large flight test gap for the THAAD interceptor. Despite this, the MDA continues to develop and deploy updates to the THAAD software and hardware for the radar, and software updates to THAAD Fire Control and Communications. The MDA and the Army continue to address THAAD training and component reliability shortfalls.

Patriot has demonstrated the capability to provide point defense against missile and aircraft attacks on deployed forces and critical assets and to defeat enemy aircraft. The Patriot PDB-8.1 Limited User Test (LUT) assessed how Patriot effectiveness, suitability, and survivability have changed since the last Patriot operational test that concluded in April 2019. DOT&E published the results of the PDB-8.1

LUT in a separate classified report in 1QFY24. Patriot PDB-8.1 training and human system integration improved over PDB-8, but shortfalls remain in reliability and survivability. As reported in the DOT&E FY23 Annual Report, the Patriot M&S representations for ground tests used the Battalion Simulation under development by the Army, but the Army has not yet provided sufficient verification and validation (V&V) evidence to accredit the Battalion Simulation for performance assessments. The Army should provide sufficient V&V evidence for the Battalion Simulation or work with MDA to determine a way ahead for a new Patriot representation to integrate and use to support regional/theater performance assessments during MDS ground tests.

AN/TPY-2 (FBM) and AN/SPY-1 radars contribute to regional/theater defense and monitoring. In the future, AN/SPY-6(V)1 radars on Aegis Flight III destroyers will also contribute to those missions. AN/TPY-2 (FBM) detected and tracked an IRBM target in an FY24 GMD flight test. In FY24, AN/SPY-1 demonstrated the capability to detect, track, and discriminate an MRBM with countermeasures during a live intercept flight test, and the capability to detect and track an IRBM during a GMD flight test. The AN/SPY-6(V)1 radar prototype at the Pacific Missile Range Facility, Hawaii, continues to track all classes of ballistic missiles, as available, during MDA flight tests. The first Aegis Flight III destroyer with Aegis Baseline 10, USS *Jack H. Lucas* (DDG 125), detected and tracked two MRBM targets in FY24 with its AN/SPY-6(V)1 radar, though corrective action is needed to address observed anomalies. These anomalies created shortfalls in the data needed to validate the high-fidelity M&S for Aegis Baseline 10 operational test runs for record.

The Army conducted an LTAMDS operational assessment as part of the Integrated Fires Test Campaign 23 (IFTC 23). DOT&E determined that IFTC 23 was inadequate to support an assessment of operational effectiveness for the LTAMDS system, due to immature and unaccredited LTAMDS M&S tools. These M&S challenges persist in IFTC 24. The Army should focus on efficiently using developmental testing to support M&S tool development, verification, validation, and accreditation. See the IFTC article in this Annual Report for additional details.

» HYPERSONIC MISSILE DEFENSE

The MDA collected hypersonic test data throughout FY24 to inform future sensors, sensor detection and tracking algorithms, and M&S validation. The MDA also conducted ground hypervelocity impact, thermal, and aerodynamic testing to support the development of the M&S architecture for hypersonic missile defense.

» COMMAND AND CONTROL AND SPACE SENSORS

Almost every FY24 test conducted by the MDA included space sensors acquiring, tracking, and reporting on observed objects. The prototype Hypersonic and Ballistic Tracking Space Sensor (HBTSS) performed its first data collection on a hypersonic target. Command and Control, Battle Management, and Communications (C2BMC) globally and regionally integrates and synchronizes autonomous sensors, weapon systems, and operations. C2BMC is also a part of all system ground and flight tests, which verify and exercise current and future MDS capabilities. In FY24, C2BMC and the BMDS Overhead Persistent Infrared Architecture (BOA) continued to support real-world situational awareness in USEUCOM and USCENTCOM. In a live-radiate event in FY24, C2BMC communicated with Space Command and Control for space domain awareness, tasking LRDR and AN/TPY-2 (FBM) and receiving reports back from the radars on resident space objects.

» SUMMARY

DOT&E will provide additional information in the classified DOT&E FY24 Assessment Report of the MDS due out in February 2025.

RECOMMENDATIONS

The MDA should:

1. Increase the rate of U.S. homeland defense, regional/theater target, and threat model development to keep pace with emerging

real-world threats, as recommended in the FY23 Annual Report.

2. To ensure adequate operational assessments, prioritize development and independent accreditation of M&S used in ground tests and high-fidelity analyses and ensure M&S accurately represent current threat capabilities, electronic attack, countermeasures, vulnerability, post-intercept debris, and realistic raid sizes.
3. Plan flight tests to support M&S VV&A to allow quantitative assessments of both current MDS capability, as well as more complex future capabilities that will require such a capability, like the Guam Defense System, NGI, and GPI.
4. Continue investments in ground test architecture improvements to accommodate more complex threat and system model features.
5. Ensure that relevant intercept flight testing with operationally representative targets is conducted prior to any planned M&S operational testing runs for record, to provide referent data to support VV&A of the models representing post intercept debris to enable adequate operational assessments.
6. Conduct high-fidelity M&S runs for record with independently accredited M&S to assess individual weapon system and MDS-level operational effectiveness against emerging threats.
7. Prioritize working with the DoD to find a solution to extend or replace the Pacific Tracker and Pacific Collector ships and install new shipboard radars before NGI testing begins.
8. Ensure comprehensive cyber test and evaluation plans are created and developmental and operational cyber testing is completed, prior to capability delivery of MDS element and interceptor builds to the warfighter.
9. Conduct routine operational cyber survivability assessments with multiple elements, warfighter participation, and federated M&S accredited for performance.
10. Coordinate with the Army and Navy to ensure the test strategy for the Guam Defense System incorporates multi-element interoperability and coordination into intercept flight testing, tracking exercises, ground testing, and digital M&S. Additionally, ensure comprehensive system-level suitability and cyber testing is planned, as recommended in the FY23 Annual Report.

The Army should:

1. Provide sufficient V&V evidence for the Battalion Simulation or work with MDA to identify a new Patriot representation to integrate and use to support regional/theater performance assessments during MDS ground tests.
2. Coordinate with MDA to ensure the test strategy for the Guam Defense System incorporates multi-element interoperability and coordination into intercept flight testing, tracking exercises, ground testing, and digital M&S. Additionally, ensure comprehensive system-level suitability and cyber testing is planned, as recommended in the FY23 Annual Report.
3. Ensure that the M&S tools required for LTAMDS performance evaluations are validated, verified, and accredited prior to test execution.

This page intentionally left blank.

DOT&E-MANAGED ACTIVITIES

This page intentionally left blank.

Center for Countermeasures (CCM)

In FY24, the Center for Countermeasures (CCM) performed 32 test events in support of the following: (1) evaluation of aircraft-based countermeasures (CMs), (2) evaluation of counter-unmanned aircraft systems (C-UASs), (3) development and evaluation of directed energy weapons (DEW) for potential use as CMs and counter-CMs, (4) warfighter pre-deployment training exercises with CMs, (5) data collection for threat characterization to advance the threat CMs' development and testing, (6) a partnership supporting the OUSD(R&E)'s experimentation initiative, and (7) development and fielding of unique instrumentation for CM testing. CCM also partnered with allies on project arrangements to advance the infrared (IR) and radio frequency (RF) threat CMs' development and testing.

PROGRAM

CCM was established and chartered in 1972 by OSD to address the emergence of technologically advanced weapons systems, including rapid development of terminally guided weapons and CMs. In 1999, CCM was transferred to DOT&E from the Deputy Director, Defense Research Engineering Test and Evaluation. Today, CCM operates and deploys mobile testing instrumentation capable of simulating an array of threats to measure and evaluate the operational effectiveness of CMs employed by DoD and foreign weapon systems. The portability of CCM test tools and personnel provide the test agility and efficiency required by DoD to develop and field critical CMs at operationally relevant speeds, minimizing the logistical burden on each program office and preserving schedules and resources.

MISSION

CCM expedites the development and fielding of CMs and counter-CMs employed by U.S. systems by supporting T&E activities with portable instrumentation. CCM supports the T&E community by preparing for future needs in DoD emerging technology areas, such as DEWs, hypersonics, and space CMs. Moreover, CCM leverages allies' support to advance T&E of IR and RF threat CMs. CCM also provides the threat environment for pre-deployment training to ensure warfighters are trained in combat-representative environments.

FY24 KEY ACTIVITIES

In FY24, CCM conducted 32 test events. Each event is detailed in the following sub-sections:

» T&E OF AIRCRAFT PROTECTION SYSTEMS

CCM executed 20 test events in support of aircraft survivability. These efforts enabled the evaluation of hardware and software upgrades of developmental and fielded systems to protect against IR-guided, RF-guided, and laser threats. Testing included the following:

Common Infrared Countermeasure (CIRCM)

CCM supported the Army with the assessment of the CIRCM's system upgrades and performance on UH-60M aircraft. Testing measured laser energy response to substantiate the system's ability to counter IR-guided threat missiles. Testing also assessed the system's ability to receive a hand-off from the Common Missile Warning System (CMWS).

CCM also supported the Army with a four-phase test of the CIRCM, Limited Interim Missile Warning System, and Advanced Threat Warner (ATW) software upgrades. These tests aimed to improve the survivability of rotary-wing aircraft. Flight testing was conducted with MH-60M aircraft in four different geographic regions to assess the CIRCM's performance when cued by the Limited Interim Missile Warning System or the ATW sensors.

CMWS

CCM supported FOT&E of the Air Force's HH-60W aircraft equipped with the CMWS. CCM provided IR and laser threat-representative opposition forces, enabling aircrews to employ operationally relevant tactics as well as combat search and rescue doctrine.

CMWS with CIRCM

CCM supported an Army free-flight missile test by providing missile simulations to evaluate updated CMWS software and cueing to CIRCM. Also, CCM deployed instrumentation to collect threat signature data of high-priority threats to support modeling and simulation (M&S) efforts.

Large Aircraft Infrared Countermeasure (LAIRCM) Next Generation (NexGen) Missile Warning System (MWS)

CCM supported the Navy with LAIRCM NexGen MWS tests to demonstrate system performance on P-8A aircraft. The tests demonstrated the LAIRCM NexGen system performance was within nominal expectations based on historical test data.

Department of the Navy LAIRCM ATW

CCM supported the evaluation of three Department of the Navy LAIRCM ATW configurations installed on an MV-22B aircraft. The configurations included changes to the software versions as well as hardware. The test demonstration was used to support a decision for the best system suite to protect the platform.

AN/AAR-47B(V)2 MWS

CCM supported the Air Force with evaluating the AN/AAR-47B(V)2's ability to accurately detect and display missile, laser, and hostile fire threats as installed on the MH-139A rotorcraft platform.

Distributed Aperture Infrared Countermeasure (DAIRCM)

CCM supported testing of the DAIRCM software upgrade installed on the MH-6R aircraft. Testing produced data to assist the Army with evaluating the operational suitability of the rotary-wing aircraft's system software enhancements.

Future MWS Development Testing

CCM supported the Army with characterization and data collection for two potential future MWS sensors in a laboratory environment as well as open-air test environments. During the open-air testing, the sensors were carried on UH-60M aircraft. The sensors are under consideration for the Army's Improved Threat Detection System and future Air Force MWS.

NexGen Electro-optical (EO) Distributed Aperture System

CCM supported joint F-35 flight test activities evaluating the NexGen EO Distributed Aperture System's IR tracking capabilities. These activities included simulations of multiple air-to-air missile and surface-to-air missile engagements.

AN/APR-39 Radar Warning Receiver (RWR)

CCM supported testing of the AN/APR-39D(V)2 and AN/APR-39E(V)2 RWR systems. CCM supported the evaluation of the AN/APR-39D(V)2 RWR installed on MV-22B aircraft to determine the system's threat detection capabilities. For the AN/APR-39E(V)2 RWR, which was augmented with a vendor's research and development components, CCM supported a demonstration objective to show the RWR's threat detection and geolocation capabilities while installed on a UH-60L aircraft.

» T&E OF DEW

CCM supported the rapid capabilities development and fielding of prototype DEWs and made significant progress in equipping the DoD with the tools and methods needed to adequately test and evaluate the operational effectiveness of DEWs and directed energy (DE)-based CMs. CCM supported six DE test events for the following programs:

Air Force Prototype

CCM supported the Air Force with evaluating the ability of several contractors' palletized High Energy Laser (HEL) systems to defeat adversary small-UASs. CCM conducted HEL beam diagnostics at the contractor facility pre-delivery. During the open-air test events, CCM performed UAS flights for beam characterization as well as system performance analyses at ground level and relevant slant ranges during on-the-move laser events at Kirtland AFB, New Mexico.

HEL with Integrated Optical Dazzler and Surveillance

CCM supported the Navy's demonstration on USS *Preble* (DDG 88) to verify and validate the functionality, performance, and capability of the HEL with Integrated Optical Dazzler and Surveillance system against an unmanned aerial vehicle target. CCM collected imagery of the engagements to support the evaluation of system performance.

Indirect Fire Protection Capability (IFPC)-High Power Microwave (HPM)

Testing evaluated the IFPC-HPM's technical performance and its operation as a Forward Area Air Defense weapon element subsystem. CCM supported the IFPC-HPM event with an EO and IR tracking system, which provided positive identification of targets and collected effectiveness data.

Probability of Weapon Effectiveness

CCM supported the OUSD(R&E) with a test series evaluating HEL weapon effectiveness against a series of dynamic targets and comparing the results to M&S predictions. CCM supported multiple tests within this test series.

» WARFIGHTER TRAINING

CCM deployed its unique test assets — such as a missile plume simulator, an instrumented Man-Portable Air Defense System (MANPADS) surrogate system, and an RF-threat simulator — to support three warfighter exercises. CCM provided data to the trainers to assist with their evaluation of tactics, techniques, and procedures employed by participating units to enhance their survivability in a combat environment. CCM also attended exercise planning conferences, specifically with units assigned to the U.S. Indo-Pacific Command region for future collaboration efforts.

EMERALD WARRIOR FTX1 and FTX2

The EMERALD WARRIOR FTX1 and FTX2 are Air Force Special Operations Command-led exercises that provide large-scale joint training scenarios simulating a build-up of hostilities against a complex near-peer threat. CCM threat support enables aircrews to hone CM tactics, techniques, and procedures in operationally realistic environments, thereby increasing combat effectiveness and mitigating casualties in actual warfare. The FTX1 was performed in various locations across New Mexico, Utah, and Colorado, while the FTX2 was conducted in Nevada.

NEPTUNE FALCON 24

Exercise NEPTUNE FALCON is a joint interoperability combat search and rescue exercise designed to maintain readiness and evaluate employment capabilities in a realistic training environment. CCM supported creation of the threat environment by deploying a RF-threat simulator, a MANPADS surrogate system, and an MWS stimulator to support the training exercise.

» EXPERIMENTATION SUPPORT INITIATIVES

CCM took initial steps in supporting DoD initiatives by merging current CCM capabilities and identifying capability requirements to support current and future experimentation initiatives. In collaboration with the OUSD(R&E) and the Naval Surface Warfare Center, Port Hueneme Division, CCM supported these experimentation initiatives by deploying personnel and instrumentation for two experimentation demonstrations.

VALIANT SHIELD 24 (VS24)

VS24 is a multi-national, joint biennial field training exercise aimed at ensuring the joint force is ready to conduct a wide range of combat operations. CCM supported the VS24 exercise by collaborating with the Naval Surface Warfare Center Port Hueneme

Division, White Sands Detachment at White Sands Missile Range, New Mexico, in providing a central network and communication site as well as two static threat emitter sites. The network provided the necessary capabilities to the VS24 analysis, operations, prototypes, and assessment teams throughout the exercise to monitor and evaluate the demonstrators' performance. The simulated targets provided a combined RF and visual signature for targeting to enable the evaluation of kill chain scenarios. CCM also helped to deploy opposing force assets in support of the OUSD(R&E) Rapid Defense Experimentation Reserve program's experimentation campaign during multiple vignettes.

C-UAS Experimentation

CCM supported the OUSD(R&E) C-UAS experimentation event by providing personnel, instrumentation, and certified UAS pilots. The OUSD(R&E) C-UAS event was a joint Service experimentation and development effort of innovative and realistic prototypes to counter ever-evolving UAS threats faced by combatant commands. CCM leveraged its DE and C-UAS T&E instrumentation to assist with data collection, analysis, and reporting on C-UAS prototype systems participating in the experiment.

» DATA COLLECTION FOR THREAT CHARACTERIZATION

CCM supported one threat data collection event held by the NATO/Aerospace Capability Group 3/Sub-Group 2. The Swedish Air-to-Air Missile Trial was held in Vidsel, Sweden, to enable threat signature data collection of air-to-air and ground-to-air IR-guided missile threats. CCM provided a subject matter expert to determine the health and suitability of each MANPADS threat asset for the planned live-fire event scenarios. CCM also collected radiometric data on the air-to-air and MANPADS threat assets. CCM provided the signature measurements to the M&S community to aid the verification, updating, and creation of new threat missile models that are critical to the testing of current and future MWS systems.

» DEVELOPMENT AND FIELDING OF UNIQUE INSTRUMENTATION FOR CM SYSTEMS

CCM continued to develop and upgrade test instrumentation and capabilities to keep pace with adversary advances and T&E needs to expedite testing, development, and fielding of CMs needed to survive in increasingly complex, multi-domain environments.

Joint Standard Instrumentation Suite (JSIS)

JSIS is used to collect missile plume and hostile fire threat signatures, missile attitude, and time-space-position information data during live-fire events. JSIS's collected data will further develop the Missile Space and Intelligence Center's threat models to support MWS and CM development and evaluation. In FY24, the JSIS Missile Attitude Subsystem for tracking imagery and time-space-position information was accepted and delivered. All remaining instrumentation is scheduled to be delivered by 1QFY25, completing all three phases of the JSIS project and providing full operational capability to the T&E community. JSIS personnel continue to update and improve automated mission-based data collection and reduction features and are investigating the feasibility of using enterprise engineering platforms for artificial intelligence and machine learning to enhance data analysis.

High-Elevation Target Simulator (HETS)

HETS is a new test capability being developed to provide a low-cost, portable IR target simulator and radiometric data collection platform designed to collect missile signature data at high-elevation angles to enhance current threat fly-out models. Existing models were developed from limited static and low-angle-of-attack live missile firings. Once complete, HETS will compliment current capabilities to collect data to update threat models for improving current and future IRCM T&E effectiveness. In FY24, two risk reduction events were held at Dugway Proving Ground, Utah, which revealed the HETS balloon concept was not feasible to collect high-elevation signature data.

In FY25, CCM plans to evaluate alternative courses of action to collect the desired missile signature data.

DoD Space T&E Instrumentation Initiatives

In collaboration with the Test and Evaluation Threat Resource Activity (TETRA), CCM continues to identify gaps in space CM T&E capabilities and actions or investments required to fill those gaps. A draft report identifying gaps in space T&E capabilities was generated in FY24, and a final report will be published in FY25.

DE Instrumentation

CCM assisted in the development and implementation of tools to support DEW testing. CCM supported development or acceptance testing for the following joint DE T&E tools and instrumentation:

- Free-flying UAS-mounted target boards for directly measuring HEL performance on an inflight platform at operationally representative slant ranges.
- HEL irradiance target boards for directly measuring HEL performance against surrogate cruise missiles.
- Instrumentation that captures HEL beam energy and safely dissipates heat to provide a backstop for HEL testing.
- Tethered HPM-hardened UAS with instrumentation for measurement and characterization of HPM beam on target.
- HPM beam evaluation instrumentation for providing visual indication of relative field mapping at source-to-target distances of HPM system beam profiles.
- Class 1 and Class 2 UAS threat targets for DE and C-UAS experimental prototype demonstrations.

» SUPPORTING PROJECT ARRANGEMENT WITH ALLIES TO ADVANCE CM T&E

CCM and TETRA continued to support the execution of the Australia, Canada, United Kingdom, and United States Aircraft Electronic Warfare Cooperative Test and Evaluation Project Arrangement (Air EW CTE PA) intended to advance and standardize Airborne EW T&E capabilities. Air EW CTE PA project officers and steering committee members from the four nations met in the United Kingdom to review advances made by the four Air EW CTE PA working groups (WGs) and the results of multiple Air EW trials conducted in FY24. Accomplishments in FY24 include the following:

M&S and Threat Environment Representation WG

The WG conducted confidence trials of existing IR, RF, and EO CM models. The WG continued validating a high-fidelity chaff model and improving a double MANPADS M&S tool to allow for the assessment of flares and Directed Infrared Countermeasure systems versus multiple MANPADS.

Air EW T&E Methodology WG

The WG completed the standardized T&E Terminology and Methodology documentation. The WG started drafting an M&S verification and validation process as well as documenting and developing the layout for a data repository to support the Air EW CTE PA efforts.

Integrated Aircraft Survivability Equipment and Air Platform M&S WG

The WG is investigating how to utilize artificial intelligence capabilities in future aircraft survivability equipment M&S tools. The WG, in cooperation with the other Air EW CTE PA WGs, is developing test objectives and plans to manage future M&S activities.

RF Threats and CM WG

The WG completed five trials that incorporated Air EW M&S tools into an overarching battlespace environment simulation hub by using a pre-determined Air EW scenario to evaluate CM effectiveness against an integrated air defense system.

Cyber Assessment Program (CAP)

In FY24, the DOT&E Cyber Assessment Program (CAP) observed continued improvements in DoD cyber defenses. New cyber-defense tools provide heightened capabilities for detecting malicious activity within networks, and also offer greater levels of automation in threat response, resulting in the potential to provide more timely alerts to cyber defenders. These cyber defense improvements have occurred, in part, because of the advocacy and support of the CAP. However, these enhancements are not yet applied consistently throughout the DoD. There remain many areas where only limited sensors are in place, even in some networks aligned with critical infrastructure and in critical weapons systems. DoD Cyber Red Teams performing adversary assessments with CAP found gaining and retaining access on many DoD networks more challenging than in previous years. However, these teams often lack the tools, time, and other resources representative of the advanced adversaries they are asked to emulate.

As stated in previous Annual Reports, DOT&E recommends for the DoD to substantially increase DoD Cyber Red Team capabilities and capacity to better emulate the advanced cyber threats. Expanded Red Team capabilities will help ensure critical DoD missions are practiced in contested environments and can continue during a conflict. Key recommendations from FY24 CAP assessment activities are:

- Assume networks and systems have been breached, and prepare accordingly;
- Routinely allow DoD Cyber Red Teams to access target systems and networks immediately, rather than forcing them to use scarce resources breaking into those systems and networks;
- Increase implementation of Zero Trust principles;
- Perform more training and mission rehearsals in contested environments representative of the full spectrum threats an adversary may employ, including electromagnetic spectrum operations (EMSO) coordinated with kinetic and cyber-attacks;
- Update and exercise Primary, Alternate, Contingency, and Emergency (PACE) plans associated with all critical missions;
- Increase resources for DoD Cyber Red Teams and other cyber threat emulation capabilities to enable more consistent advanced cyber threat emulation in events; and
- Routinely conduct threat-representative assessments of commercial clouds containing critical DoD data, including the commercially operated portions of the clouds.

DoD's Cyber Red Teams have demonstrated that given enough time and resources, they can obtain access to critical DoD networks and systems. The DoD must assume our adversaries can do the same. To defend against this, the DoD is implementing Zero Trust best practices, which by design assume that any entity in a DoD network or system should not be trusted, and therefore must provide appropriate credentials to perform any actions in that network or system. However, full implementation of Zero Trust will take several years, and will likely require a level of training, expertise, and automation that is not currently planned. Zero Trust can only be achieved if user identities can be tracked, and access to data can be verified via Identity, Credential, and Access Management (ICAM) tools that limit access to data until verification of users' documented needs. The Department will need to properly label all future and legacy data with dissemination controls. With effective ICAM tools, adversary presence in systems and networks will be more quickly detected, and ICAM tools should also preclude adversary access to critical warfighter data and functions.

The DoD continues to increase the amount of critical operational data being stored in commercial clouds, without conducting its own threat-realistic assessments of the security of these clouds. This is despite language in the FY23 National Defense Authorization Act (NDAA) requiring such assessments. To adequately conduct such assessments, it is imperative that Cloud Service Providers (CSPs) work side-by-side with the DoD, sharing detailed technical data about commercial cloud security technologies, personnel, and processes; and supporting independent DoD Cyber Red Team assessments on the commercial side of clouds. DoD and CSP Cyber Red Teams and cyber defenders should routinely work together to improve identification of risks, and defenses against attacks upon CSP and DoD applications and data.

Events in Ukraine and other parts of the world are highlighting the criticality of EMSO in modern warfare. CAP is growing its EMSO team and planning to make combined EMSO and cyber-attacks a standard part of the contested environment that warfighters are subjected to during training exercises assessed by CAP.

Many combatant commands (CCMDs) are working toward increased threat realism during exercises. These events will afford opportunities to examine the alternate modes and backup capabilities contained in each commands' PACE plans and to identify where those plans provide insufficient resilience to perform critical missions in combat. Currently, PACE plans are seldom fully exercised during the major exercises that CAP supports, but with immature implementation of Zero Trust and ICAM, and ever-growing adversary capabilities, this needs to change. For PACE plans to be effective, they should be stressed and assessed routinely, updated where needed to optimize resilience and mission assurance, and demonstrated to be available and effective no matter what the adversary does.

CAP intends to use the DoD National Cyber Range Complex (NCRC) to assist in more thorough demonstrations and assessments of adversary impacts in the cyber and EMSO domains. More often than not, exercise authorities determine that allowing unfettered Cyber Red Team activity would impact too many other training objectives, which results in an environment that is not realistic for either training or assessment. Warfighter training and mission rehearsals in benign cyber and EMSO environments are also inadequate for assessment of readiness or mission assurance against advanced nation-state threats. Range events, coupled with major exercises and experiments, would help improve warfighter readiness and confidence that their missions can be accomplished in combat.

Significant advances in artificial intelligence (AI) and machine learning (ML) occurred in the commercial sector during FY24, and the DoD is also ramping up AI/ML efforts on many fronts. In FY24, CAP – in partnership with the Chief Digital and AI Office (CDAO), federally funded research and development centers (FFRDCs), National Laboratories, academia, and DoD Cyber Red Teams – continued to develop and demonstrate assessment methods and tools unique to AI/ML technologies and will refine and employ these capabilities in FY25 on emerging AI-enabled systems. CAP is also experimenting with the use of large language models and generative AI to assist with assessment activities, including creation of high-fidelity range environments.

PROGRAM OVERVIEW

CAP is a congressionally directed program, established in FY03, focused on assessing the cyber survivability of CCMD and Service missions in contested environments. Congress directed DOT&E to plan and conduct these operational evaluations during major exercises.

DOT&E resources DoD Cyber Red Teams to emulate realistic adversaries during major CCMD and Service exercises, and to provide assessment venues to help warfighters improve their ability to fight through cyber-attacks and accomplish critical missions.

DOT&E also provides resources to assessment teams from the Operational Test Agencies and FFRDCs to plan and execute mission-focused assessments and analyze and report on the results at the system, network, and operational levels.

Although exercises are the primary venues for CAP assessments, DOT&E also employs Cyber Readiness Campaigns (CRCs) that include non-exercise events to examine specific elements of warfighter missions and defenses. These CRC events may include pre-exercise Red Team activities, cyber-stimulation events to help cyber defenders fine-tune their sensors and response actions, tabletop exercises with leadership to explore various contingency plans, and range-based events to examine mission elements and threats that may not be appropriate for operational networks.

CRCs provide advanced training opportunities for the CCMDs and Services to rehearse their missions in environments that include realistic adversary emulation. The CRC events that culminate with an exercise capstone event enable CAP to assess cyber warfighting in a realistic mission context.

MISSION

The DOT&E CAP conducts continuous objective analysis of DoD cyber capabilities via assessments of defensive and offensive cyberspace operations of the Services and CCMDs. Through these assessment efforts, DOT&E supports and advocates for improvements in DoD's cyber posture. CAP conducts assessments both as part of Tier 1 exercises as well as through discrete missions and capabilities across the spectrum of joint and multi-domain operations. The program reports findings to Congress, relevant operational and acquisition authorities, and other stakeholders as required to identify key achievements and shortfalls, and to make recommendations for future investments and operations.

FY24 KEY ACTIVITIES

In FY24, CAP brought together focused intelligence expertise, pre-exercise Red Teams (see Persistent Cyber Operations below), and exercise DoD Cyber Red Teams into a unified cyber OPFOR that affected a wide range of missions and supporting components at U.S. Indo-Pacific Command (USINDOPACOM), U.S. European Command (USEUCOM), U.S. Strategic Command (USSTRATCOM), U.S. Special Operations Command (USSOCOM), and other venues. These activities set the conditions for rigorous assessments with representative adversary emulation and improved the realism of mission rehearsal for the participating commands.

During these assessment activities, CAP teams identified cyber vulnerabilities and demonstrated potential impacts that could degrade CCMD missions. CAP communicated these findings to system owners and network defenders so that vulnerabilities could be remediated, and missions made more resilient. The assessment teams also identified improvements in cyber defenses, such as well-defended enclaves that have been assessed and enhanced through multiple cycles and have incorporated some Zero Trust principles. Room for improvement remains, particularly at Service-level components, which can be targeted through long-duration persistent Red Teams and other more advanced means.

To help keep pace with evolving cyber adversaries, in FY24 CAP continued to develop new cyber-attacks targeting cloud technologies and AI/ML capabilities. CAP developed cyber-attacks using the radio frequency (RF) spectrum, and techniques integrating cyberspace effects with both kinetic and non-kinetic effects. CAP also developed new capabilities that automated data collection for DoD Cyber Red Team operations, and improved collection methodologies for cyber-defense data.

» CCMD AND SERVICE ASSESSMENTS

During FY24, CAP performed cyber assessments at 10 CCMDs (U.S. Africa Command [USAFRICOM], U.S. Central Command [USCENTCOM], U.S. Cyber Command [USCYBERCOM], USEUCOM, U.S. Northern Command [USNORTHCOM], USINDOPACOM, USSOCOM, U.S. Southern Command [USSOUTHCOM], USSTRATCOM, and U.S. Transportation Command [USTRANSCOM]), and four Services (Air Force, Army, Navy, and Space Force).

As projected in the FY23 Annual Report, DOT&E ramped up assessment activities with the U.S. Space Force and continued engagement with the U.S. Space Command (USSPACECOM). In FY24, CAP conducted assessments during SPACE FLAG exercises, and continued assessments of U.S. Space Force's suite of cyber defense tools and the personnel strategy to support cyber defense operations. CAP also collaborated with USSPACECOM to enhance the command's cyber and physical security posture.

CAP prepared a classified report for each assessment, documenting the assessment's planning, execution, analyses, and recommendations. Overall, CCMDs continue to demonstrate a willingness to understand how cyber-related vulnerabilities and shortfalls can lead to mission risks and are working to bring new and emerging capabilities to bear to mitigate identified issues.

New cyber defense tools on DoD networks are providing heightened capabilities for detecting malicious activity within the network. These tools provide greater levels of automation in threat response and have the potential to provide timely alerts to cyber defenders. There is, however, an inconsistent application of cyber defense sensors throughout the Department and areas where there are no sensors in place, to include critical infrastructure and weapons systems. Cyber defenders are, in many cases, not fully trained on the use of new cybersecurity tools. This lack of training leads to situations in which the defenders are unable to properly tune their tools to provide key threat detection alerts, which is a concern because a persistent adversary is highly likely to penetrate any defensive perimeter, given enough time. At several CCMDs, perimeter cyber defenses were improved from prior years, as were abilities to detect and respond to threats rapidly. These improvements resulted in a greater number of events where Red Team activity was stopped before these exercise adversaries could achieve OPFOR objectives. Once inside perimeter defenses, Red Team activities were generally successful, at the expense of warfighter missions and objectives.

In FY24, CAP expanded exercise assessments to include more component commands, Service cyber components, and U.S. allies and partners. These assessments included Purple Team events, which combine DoD Cyber Red Team activities and cooperative assessments simultaneously, to identify shortfalls in detection and help cyber defenders implement improved detection processes or other mitigations. DOT&E observed a range of cyber defense capabilities across the participating components. Some groups of local defenders were better resourced and trained than others, and CAP observed those defenders to be more capable at defending their networks and missions. The CCMDs should ensure that their subordinate components are adequately resourced to counter cyber threats and inform the components of how their cyber vulnerabilities affect CCMD missions.

Exercises with more realistic adversary portrayal would provide warfighters and defenders with improved opportunities to practice their missions in the expected contested environments and help them enhance their fight-through capabilities. In FY24, leadership at several CCMDs emphasized the shift from “training exercises” to more operationally realistic “mission rehearsals.” CAP continued to incorporate cyber OPFOR leads in exercise assessments to help translate cyber effects into mission effects for the exercise control group. Exercise controllers included those mission effects in multiple exercise scenarios, providing dynamic training opportunities for the command staff and exercise participants. This training could be improved by including a wider range of disruptive effects representative of those that potential adversaries could deliver.

A significant limitation to enhanced operational realism during CAP assessments is that DoD Cyber Red Teams remain under-staffed and under-resourced. Compounding this issue are continuing challenges with retention of Red Team experts who are being stressed by ever-increasing demand, and a lack of development pipelines for advanced cyber tools and tradecraft. DoD Cyber Red Teams lost many of their journeyman- and master-level operators over the last several years, and it will take many years and significantly more resources to recover from these losses. Unless remedied, DoD Cyber Red Team shortfalls will lead to inadequate preparation during mission rehearsals, inadequate program acquisition activities, and ultimately critical warfighter capability deficits. In response to the FY24 NDAA Section 1507, DOT&E collaborated with the DoD Chief Information Officer (CIO) to survey the current capabilities of the DoD Cyber Red Teams and coordinated on the DoD CIO’s subsequent report to Congress. DOT&E will continue to monitor and report on DoD Cyber Red Team capabilities.

As in FY23, DOT&E observed in FY24 that cyber-related information sharing, and coordination could be improved across the DoD at all levels. Successful cyber defense requires completing prevent, detect, respond, and recover actions, and organizations should ensure they can reliably conduct incident reporting and cyber threat intelligence sharing. The interconnected nature of networks and systems, trust relationships across commands, and the ability for data to be rapidly disseminated means that an individual CCMD’s data security depends on all participating DoD parties. Combatant commanders and DoD leadership should fully understand the mission risks associated with data sharing initiatives across the Department.

» SPECIAL ASSESSMENTS

CAP performed the following special assessments in FY24 in collaboration with the USD(R&E), USCYBERCOM, USSTRATCOM, the DoD CIO, CDAO, Joint Forces Headquarters DoD Information Network (JFHQ-DoDIN), the Defense Information

Systems Agency, and the Department of Energy's Sandia National Laboratories:

- Joint Fires Network (JFN) assessments
- Zero Trust architectures
- Cross-Domain Solution (CDS) assessments
- Nuclear Command, Control, and Communications (NC3) assessments
- Offensive Cyberspace Operations (OCO) and Non-Kinetic Effects (NKE) assessments
- RF-enabled cyber operations and Transponder –Combat Identification (TCID) assessments
- Wargames to improve and expand assessments beyond the limits of exercises
- Preparations for assessments of AI/ML technologies

Special assessment methodologies and outcomes were shared with requesting organizations and will inform the broader CCMD and Service CRCs, as well as cybersecurity OT&E of acquisition programs. These special assessments are discussed further below.

Joint Fires Network (JFN) Assessments

During FY24, the DOT&E CAP, as part of support to USINDOPACOM, completed several JFN cyber assessments. JFN is considered a top priority within USINDOPACOM and is a pathfinder for Combined Joint All-Domain Command and Control. Involvement of CAP within the JFN governance and capability development structure was geared toward informing OUSD(R&E) of the cybersecurity posture of the JFN, as the capability continues to be refined in preparation for transition of JFN to a program management office during the FY25/FY26 timeframe.

CAP JFN-related activities included a deep dive of JFN network architecture, an initial DoD Cyber Red Team assessment, and observation of JFN capabilities during a Tier 1 exercise in key locations. Findings from these assessments are currently being addressed within the JFN development cycle, and future CAP assessments are planned as part of OUSD(R&E)'s commitment to ensure cyber viability of the JFN.

Zero Trust Environment Assessments

The DoD CIO describes Zero Trust as "protecting critical data and resources, not just the traditional network or perimeter security" (DoD Zero Trust Reference Architecture). In keeping with recommendations made by DOT&E over the past several years to move from boundary-focused to data-focused protections, the DoD CIO has many ongoing efforts to move to a Zero Trust architecture, and CAP has observed positive outcomes because of the adoption of various combinations of the tenets and pillars of Zero Trust, as defined by the DoD CIO.

CAP has not yet observed a complete implementation of Zero Trust that includes continuous multi-factor authentication, micro segmentation, encryption, endpoint security, automation, analytics, and robust auditing. CAP performed limited assessments of Zero Trust-enabled classified networks in FY24. In one assessment, deficiencies were noted in network hygiene that caused the failure of Zero Trust protections. In another assessment, Zero Trust data protection was inoperable during the assessment timeframe due to technical issues with the Zero Trust software. CAP will continue looking for and consider assessing Zero Trust pilots as DoD implementation matures.

Cross Domain Solution (CDS) Assessments

A CDS is an integrated hardware/software system that enables access and exchange of sensitive data across networks at different levels of security classification. CDS capabilities are essential for the movement of data across myriad DoD systems that are critical to warfighting capabilities.

In FY24, CAP reviewed CDS implementation and identified the need for further evaluation of the cyber survivability of DoD CDS capabilities. As a result, DOT&E placed CDS on oversight to ensure rigorous testing and full awareness of the operational state of CDS capabilities.

The Trusted Network Environment (TNE) is an enterprise CDS that provides a connection between U.S.-only networks and coalition partner networks. With its connections to non-U.S. users, TNE has a particularly high level of importance in safeguarding U.S.-only data. Full assessments of TNE are therefore a high priority going into FY25. Enterprise CDS services have also been offered to the Department and Services from Commercial Cloud Providers. These cloud-enabled connections offer new and flexible ways to move data between U.S. networks and are therefore also a high priority for assessment in FY25.

Nuclear Command, Control, and Communication (NC3) Assessments

CAP and USSTRATCOM continued a partnership for assessing and improving the cyber survivability of the NC3 enterprise. The complex nature of the hybrid legacy and modernized system of systems that comprises NC3 poses challenges to assessments of this mission space; however, progress is being made across the NC3 enterprise as a result of the continued partnership. Barriers to cyber assessments of the NC3 enterprise include a lack of operational capacity to support operations and testing simultaneously, as well as ongoing modernization efforts.

In FY24, CAP conducted ongoing assessments of NC3 sensing and monitoring capabilities, as well as special assessments of NC3 capabilities, and routinely briefed stakeholders of the NC3 Cyber Summit. CAP also assessed operational NC3 capabilities and informed related guidance.

CAP is collaborating on the development of a high-fidelity range environment for a subset of NC3 legacy systems. This environment will assist with assessments and Red Team activities that would otherwise be challenging on the operational networks. Once validated, the environment will also help assess and experiment with improved cybersecurity defenses and allocation of sensors deployed across the transitioning NC3 system of systems.

Offensive Cyber Operations (OCO) and Non-Kinetic Effects (NKE) Assessments

In FY24, CAP conducted OCO/NKE assessments on capabilities developed and fielded by the Air Force, Army, and by USCYBERCOM's innovation team working on Rapidly Deployable Access Capabilities. CAP also conducted assessments on the integration and synchronization of OCO/NKE in major exercises with USINDOPACOM, U.S. Forces Korea (USFK), USEUCOM, Army Multi-Domain Task Forces, and key events with Joint Special Operations Command (JSOC).

The DoD continues to develop many OCO/NKE capabilities without formal operational testing. Although CAP provides operationally realistic assessments for a small subset of these capabilities, there are many more OCO/NKE capabilities being developed in multiple DoD components with no such assessments. OCO/NKE capabilities continue to grow in importance to DoD missions, and insufficient testing in operational environments with representative threats may result in capabilities failing to work as needed, or in a lower confidence regarding the scope and duration of capability effects.

In addition to continuing OCO/NKE assessment activities at all the commands mentioned above, in FY25 CAP plans to assess capabilities and events supporting USSOUTHCOM, USSPACECOM, and USSTRATCOM's Joint Electromagnetic Spectrum Operations Center (JEC). CAP will also continue to expand its partnership with the Defense Advanced Research Projects Agency (DARPA) and with OUSD(R&E) to support early assessments of unique, "fast-tracked" capabilities.

RF-Enabled Cyber Operations and Tactical Combat ID (TCID) Assessments

The 2022 National Defense Strategy notes that electromagnetic spectrum and other non-kinetic threat developments are challenging U.S. response capabilities, and rapidly developed and low-cost technology is eroding U.S. technology leads. In close partnership with the Air Force Cyber Resiliency Office for Weapon Systems, CAP is expanding its assessments to include RF-enabled cyber-attacks to facilitate an enhanced OPFOR that is not solely focused on traditional cyber and internet protocol (IP) networks but includes the RF spectrum.

TCID is a capability to identify friend or foe via a transponder signal. During FY24, DOT&E consolidated multiple years of data showing potential for mission effects from degraded TCID and operationalized these data during a major exercise. The resulting findings highlighted both IP vulnerabilities as well as RF- and non-IP-based threat vectors. CAP worked with numerous partners to better understand, defend against, and safely replicate these threat vectors for integration into exercises.

Cyber Wargames

The inaugural Cyber Maneuver, Operations, and Combat Knowledge Wargame (CMOCK-W) was executed during AFRICAN LION 24 and provided a critical learning opportunity for U.S. joint forces, allies, and partners working together on a combined mission. CAP designed the CMOCK-W with an emphasis on the operational level of cyber warfare. This wargame extends traditional assessments beyond the limitations of exercises on operational networks by helping demonstrate potential mission impacts of advanced cyber-attacks to warfighters and leaders. The wargame depicts the virtual maneuver of cyberspace forces defending friendly terrain from offensive actions, while emulating adversaries' capabilities and intent, forcing participants to think beyond traditional technical solutions.

The CMOCK-W will help leaders become more familiar with degraded environments not generally permitted during training exercises and assist in refinement of contingency and response-action planning. Rigorous and recurring CMOCK-W engagement will improve warfighter preparations to fight through contested cyber environments and improve mission assurance. CAP plans to conduct additional CMOCK-W wargames during FY25 and is considering options to scale to a larger number of wargames given growing warfighter interest across assessed commands.

AI and ML Assessments

In FY24, CAP continued efforts to prepare for assessments of AI-enabled technologies, working with the CDAO, FFRDCs, National Laboratories, academia, and DoD Cyber Red Teams on the development and demonstration of assessment methods and tools designed for AI/ML technologies. CAP will continue these efforts in FY25 in anticipation of deployments of AI-enabled capabilities to the CCMDs.

CAP is experimenting with the use of large language models and generative AI to assist with ongoing and overarching assessment activities, such as:

- Identification of trends in vulnerabilities and network defenses over several hundred assessments, and
- Assistance with development of advanced assessment and Red Team tools.

CAP will employ AI/ML technologies to help create high-fidelity range environments, operationally representative network traffic, and the tools to rapidly adjust network configurations and other variables in range environments to expose warfighters to realistic threat conditions.

» SUPPORTING ACTIVITIES

Persistent Cyber Operations (PCO)

PCO are long-duration exercises that allow DoD Cyber Red Teams an extended timeline to probe selected areas of DoD networks and portray more advanced adversaries. As opposed to two-week exercises or tests, long-duration activities through PCO offer Red Teams time for stealthier cyber reconnaissance to identify cybersecurity weaknesses and access points that might otherwise go undetected. These activities help identify subtler and more pervasive vulnerabilities and provide more realistic training for cyber defenders. The longer dwell time enables PCO Red Teams to escalate privileges and move laterally within target networks to cause effects at the time of their choosing, as an advanced persistent threat would. Accesses gained by PCO are handed off to exercise Red Teams acting as cyber OPFOR during specified exercises, but critical findings are reported immediately, in accordance with USCYBERCOM guidance.

During FY24, CAP worked with three DoD Cyber Red Teams to conduct PCO missions at seven CCMDs and on one Service network. Building on processes implemented during FY23, these missions extended available execution time and included more rigorous quarterly reporting, as well as end-of-mission reporting, to capture successes in reaching objectives and to incorporate lessons learned as the program matures.

In addition to exercise support, FY24 PCO missions aided CCMDs in strengthening their networks based on these longer-term assessments. Operations at USSOCOM were integral to helping that command prepare for their first Cybersecurity Service Provider evaluation conducted by JFHQ-DoDIN, from which they earned a two-year certification.

In FY24, in response to the FY23 NDAA Section 1656, DOT&E and the Missile Defense Agency (MDA) collaborated on plans for a PCO to cover missile defense systems and networks, in accordance with congressional direction. The collaboration resulted in development of an MDA approval process for PCO activities that MDA will exercise in coordination with CCMD approval processes, and a multi-phase plan for PCO activities on the Missile Defense System. CAP and the MDA will exercise the approval processes developed as part of new and ongoing PCO activities in FY25.

Advanced Cyber Operations (ACO) Team

CAP built on existing relationships across multiple organizations that can provide master- level cyber operators to serve as members of the CAP's ACO team. CAP utilizes the ACO team to conduct assessments of emerging technologies, provide cutting-edge expertise as part of continuous augmentation to DoD Cyber Red Teams, and facilitate the portrayal of more advanced cyber threats. Organizations participating in the ACO team include DoD Cyber Red Teams, FFRDCs, National Laboratories, University-Affiliated Research Center Laboratories, academia, and industry. Demand for ACO support almost doubled in FY24 and is expected to continue growing in FY25 and beyond.

During FY24, the ACO team participated in multiple assessments, to include:

- Initial assessment of Advana, the DoD's enterprise-wide, multi-domain data, analytics, and AI platform
- CDS assessments of the JFN
- Special assessment activities within USAFRICOM, USCENTCOM, USEUCOM, USSOCOM, USSOUTHCOM, JSOC, and USFK, as well as Service-level assessments for the Air Force, Army, and Space Force
- Assessments of emerging capabilities as part of ongoing Capabilities Development Working Group (CDWG) efforts

Advanced Cyber-Threat Emulation Capabilities

DOT&E CAP sponsors the CDWG, providing the DoD Cyber Red Team community with a collaborative forum to acquire more advanced tools and tradecraft. DOT&E CAP also continues to pursue additional resources for tool development and acquisition that include RF, AI, and other special cyber capabilities that are needed for assessments of new and emerging technologies.

During FY24, the DOT&E CAP CDWG:

- Tested various Red Team tools, including solutions to address a major concern regarding detectability of Red Team infrastructure.
- Developed and deployed an automated logging tool for capturing and processing data produced by operators during Red Team operations. This tool automates the traditionally manual generation of action maps, reducing the associated workload on Red Team operators by an estimated 50 percent.
- Developed and delivered initial capability for a tool that can create modular executable code to emulate adversary cyber capabilities.

Engagement with the Intelligence Community

CAP's collaboration with the Intelligence Community remains an essential element of CCMD mission-focused assessments and OT&E events. High security classifications assigned to intelligence information on advanced adversary capabilities and intent limit the ability of most assessment teams to completely understand representative adversary capabilities. This limitation results in incomplete emulation of the full-spectrum adversary against which warfighters should routinely practice their missions. The lack of opportunity to experience the most representative and advanced threats may leave warfighters unprepared to defend and sustain their critical missions. DOT&E is working with the Defense Intelligence Agency, the National Security Agency, DoD Cyber Red Teams, the National Ground Intelligence Center, the National Air and Space Intel Center, and the Missile and Space Intelligence Center to improve the information sharing and the resulting realism of the threats portrayed in mission assessments and OT&E.

Collaboration with Operational Testing Activities

In FY24, CAP increased collaboration with DOT&E's operational testing activities at USCYBERCOM and USNORTHCOM. At USCYBERCOM, CAP collected data and user feedback on the operational use of systems in the Joint Cyber Warfighting Architecture during CCMD Tier 1 exercises to inform oversight of operational testing. At USNORTHCOM, CAP integrated operational testing results into an assessment of the air defense mission. CAP representatives also supported several cyber survivability test events associated with the F-35 program.

In response to the FY23 NDAA Section 1514, the DoD CIO issued a policy for "Operational Testing of Commercial and Non-Commercial Cybersecurity Capabilities" in August 2024. This policy mandates that cybersecurity capabilities are "appropriately tested, evaluated, and meet operational requirements." As part of this policy, DoD components are required to prepare test plans for "software and associated hardware procured to address broad component cybersecurity requirements," and to submit those test plans via the DoD CIO to DOT&E for review to ensure test adequacy. DOT&E, in collaboration with DoD CIO, will report on the status of plans reviewed and systems tested each year as part of the DOT&E Annual Report, beginning in FY25. As the policy was only recently issued, there are no plans or tests to report in the FY24 Annual Report.

Table 1. CAP FY24 Activity

Type of Event
Physical Security Assessment (6 Events) USN (2), USEUCOM, USINDOPACOM, USNORTHCOM, USSOCOM
Assessment of Mission Effects during Exercises (15 Events) USN (3), USCYBERCOM, USEUCOM, USINDOPACOM (3), USNORTHCOM, USSOCOM (3), USSOUTHCOM, USSTRATCOM, USTRANSCOM
Assessments of Network Security, Purple Team Exercises, and Tabletop Exercises (18 Events) USAF, USSF (2), USAFRICOM (2), USCENTCOM (4), USEUCOM, USINDOPACOM (3), USNORTHCOM, USSOCOM (3), USSOUTHCOM
Range Event (3 Events) USAF, USCENTCOM, NCRC
Assessment of Cyber Fires Processes for OCO (15 Events) USAFRICOM, USEUCOM (3), USINDOPACOM (4), USSOCOM (3), Other (4)
PCO (8 Events) USAF, USCENTCOM, USEUCOM, USINDOPACOM, USSOCOM (2), USSTRATCOM, USTRANSCOM
Assessment of Special Capabilities and Projects (13 Events) Special Capabilities (9), SME Support (2), AI/ML (2)
Acronyms: AI – Artificial Intelligence; ML – Machine Learning; NCRC – National Cyber Range Complex; OCO – Offensive Cyber Operations; PCO – Persistent Cyber Operations; SME – Subject Matter Expert; TCID – Transponder- Combat Identification; USAF – U.S. Air Force; USAFRICOM – U.S. Africa Command; USCENTCOM – U.S. Central Command; USEUCOM – U.S. European Command; USFK – U.S. Forces Korea; USINDOPACOM – U.S. Indo-Pacific Command; USN – U.S. Navy; USNORTHCOM – U.S. Northern Command; USSF – U.S. Space Force; USSOCOM – U.S. Special Operations Command; USSOUTHCOM – U.S. Southern Command; USSTRATCOM – U.S. Strategic Command; USTRANSCOM – U.S. Transportation Command

International Test and Evaluation Program (ITEP)

In FY24, the Director signed 16 new project agreements (PAs) supporting international T&E. These PAs facilitate the planning and execution of cooperative T&E projects, transfer of necessary test equipment and materials, and exchange of T&E-relevant information through working groups (WGs), reciprocal use of test facilities (RUTF), and cooperative testing under the International Test and Evaluation Program (ITEP). The ITEP holds an additional 17 ongoing PAs established with our partners prior to FY24.

PROGRAM OVERVIEW

The United States holds 12 bilateral memorandums and two multilateral memorandums with international partners. During FY24, discussions continued with additional prospective international partners pursuant to negotiating bilateral agreements. ITEP was established pursuant to a legislative proposal submitted by DOT&E and enacted into law in 2001. The SECDEF delegated administration of the program to DOT&E in 2003. Prior to ITEP, test services were generally provided to international partners through foreign military sales.

MISSION

The ITEP permits establishment of bilateral and multilateral memorandums between the United States and international partners. Such agreements are enablers for expediting the development and fielding of advanced warfighting technologies and supporting T&E infrastructure and capabilities.

FY24 KEY ACTIVITIES

In FY24, DOT&E signed 16 new PAs and/or annexes/amendments to existing PAs and supported 17 previously established PAs. Each PA is described below in alphabetical order by partner country and contains the title at the time the PA was signed. Bilateral agreements are first, followed by multilateral PAs. The 33 PAs in effect during FY24 are as follows:

1. Test and Evaluation of the Australian Special Operations Engineer Regiment (SOER) Chemical, Biological, Radiological, and Nuclear (CBRN) Defense and Explosive Ordnance Disposal (EOD) Tactics, Techniques, and Procedures (TTPs) RUTF PA

- This PA with Australia went into effect in September 2021 and lasts until September 2031. It permits testing at Dugway Proving Ground, Utah.
- The PA included one new annex in FY24 that allows the Australians to conduct additional testing.

2. Laboratory and Field Test and Evaluation (T&E) of the Chemical and Biological (CB) Defensive Material of the Australian Defence Science and Technology Group (DSTG) RUTF PA

- This PA with Australia went into effect in April 2022 and lasts until April 2032. It permits testing at Dugway Proving Ground, Utah.
- The PA allows Australian Defence Force's personnel to periodically test and evaluate CB agent testing in both laboratory and field environments. The goal is to provide support to improve the Australian Defence Force's CBRN defensive capabilities through the protection of personnel from the strategic, tactical, and physiological impacts of exposure to toxic chemicals, materials, and CBRN weapons.
- The PA included one new annex in FY24 that allows the Australians to conduct additional testing.

3. Electronic Warfare Operational Test 2016 RUTF PA

- This PA with Canada went into effect in March 2020 and lasts until October 2025. It permits testing at Naval Research Laboratory Hawaiian Operating Areas, and Marine Corps Air Station, Kaneohe Bay, Hawaii.
- The PA enables the United States and Canada to continue the at-sea T&E of the electronic warfare (EW) suites fitted in Canadian Navy ships. It is conducted in Hawaii, where the United States will simulate anti-ship missile attacks to validate the Canadian Softkill System.
- The PA included one new amendment in FY24 that extended the duration of the testing due to delays related to COVID-19.

4. SIMULATION DISPLAY (SIMDIS™) Sustainment for Sensors, Weapons, Analysis and Tactical Display Developments RUTF PA

- This PA with Canada went into effect in March 2020 and lasts until October 2025. It permits testing at the Naval Research Laboratory, Washington, DC.
- The PA provides T&E support to the Canadian Department of National Defence's SIMDIS Integration Laboratory and technical staff

for the sustainment, testing and validation of the SIMDIS display software development. SIMDIS data from various sensors, weapons, and simulations will be evaluated for use in operational analyses for tactical development and platform procurement programs.

- The PA included one new amendment in FY24 that allows the Canadians to conduct additional testing.

5. Tactical Armored Personnel Vehicle Testing RUTF PA

- This PA with Canada went into effect in February 2022 and expired in December 2023. It facilitated testing at Aberdeen Test Center, Aberdeen Proving Ground, Maryland.
- The PA permitted the U.S. DoD to provide T&E support to a Canadian Department of National Defence acquisition program. The testing and validation of the tactical armored personnel vehicle consisted of tilt table test (one and two axles), circular test, double-lane change test, J-turn test, sine and dwell test, on-center steer test and a step steering test, suspension vibration, and tire characterization.

6. Combat Hammer Omnibus RUTF PA

- This PA with Canada went into effect in November 2006 and lasts until November 2026. It permits testing at various U.S. Air Force bases.
- The PA addresses operational effectiveness and suitability testing of all aspects of the CF-18 air-to-ground weapons system.

7. Her Majesty's Canadian Ship (HMCS) Windsor Testing RUTF PA

- This PA with Canada went into effect in April 2022 and lasts until April 2025. It permits testing at the Atlantic Undersea Test and Evaluation Center, Commonwealth of the Bahamas.
- The PA covers testing of the Mk 48 Mod 7 Advanced Technology Torpedo, as well as the combat systems of HMCS Windsor.

8. Crash Truck Foam Test (CTFT) Project Equipment Transfer (PET)

- This PA with Canada went into effect in October 2022 and lasts until October 2026. It permits testing at Tyndall AFB, Florida.
- The purpose of the CTFT PET is to test cleanout procedures to transition aircraft rescue firefighting vehicles from aqueous film-forming foam to fluorine-free firefighting foam.

9. The Canadian Forces Electronic Warfare Support Test and Evaluation (CFEWS T&E) RUTF PA

- This PA with Canada went into effect in March 2023 and lasts until March 2027. It permits testing at Shirley's Bay, Ottawa, Canada.
- The EW software and the Scenario Simulation Controller are part of a U.S. DoD-owned EW and reprogramming software suite managed by the U.S. Navy's Next Generation Electronic Warfare Program Office. Testing CFEWS at Shirley's Bay unique configuration can benefit from the testing of EW capabilities by the scenarios contained in the EW toolset. The testing of CFEWS capabilities utilizing the U.S. DoD's EW toolset and components of its EW programming toolset (i.e., the Scenario Simulation Controller), monitoring, and analysis.

10. Technology Experimentation and Characterization Field Trials (TECFT) RUTF PA

- This PA with Australia went into effect in May 2023 and lasts until October 2026. It permits testing at Dugway Proving Ground, Utah.
- The PA allows the Australian SOER to conduct Counter CBRN (C-CBRN) testing in increasingly realistic environments against updated threat representative scenarios in an operationally realistic environment. The goal is to enhance and improve current TTP and to develop additional TTP for operational gaps identified during these test events.

11. Combat Archer II Omnibus RUTF PA

- This PA with Canada went into effect in December 2015 and lasts until December 2025. It permits testing at Tyndall AFB, Florida.
- The PA addresses operational effectiveness and suitability testing of the Canadian Air Force's CF-18 air-to-air weapon systems using

a total system approach that includes man, munitions, and machines.

- The PA included one new annex in FY24 that allows the Canadians to conduct additional testing.

12. Reciprocal Use of Test Facilities (RUTF) Project Arrangement (PA) Concerning Electronic Warfare (EW) Operational Test (OPTEST) 2016 with Canada

- This PA with Canada went into effect in May 2016 and lasts until March 2026. It permits testing at Marine Corps Base Hawaii, Oahu, Hawaii.
- The PA provides a Naval Research Laboratory Learjet aircraft fitted with anti-ship missile simulators and technical staff for at-sea testing and validation for the Canadian Multi Ammunition Softkill System.
- The agreement included one new amendment in FY24 that allows the Canadians to conduct additional testing.

13. Advanced Distributed Modular Acquisition System (ADMAS) Instrumentation Equipment and Material Transfer Arrangement

- This PA with Germany went into effect in October 2020 and lasts until October 2024. It permits testing in Koblenz, Germany.
- The PA between the United States and Germany enables the U.S. Army's T&E Command to transfer the ADMAS instrumentation and software tools to the Bundeswehr Head of Robotics Research and Development in Koblenz. The transfer is valid for three years, and allows Germany to standardize test procedures, data analysis techniques, and T&E methodology for testing autonomous robotic vehicles and associated technology.

14. T&E of the German Bundeswehr CBRNE Defense TTPs RUTF PA

- This PA with Germany went into effect in June 2021 and lasts until June 2026. It permits testing at Dugway Proving Ground, Utah.
- The PA enables the German Bundeswehr to develop and test its defense TTP against Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) threats. The U.S. Army hosts 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 (PPE), and decontamination equipment in an operationally representative environment.
- The PA included three new annexes in FY24 that allow the Germans to conduct additional testing. Testing under all three annexes concluded in FY24.

15. Partnership for Autonomous Robotic Test Instrumentation WG TOR

- This WG with Germany went into effect in April 2018 and lasts until April 2028.
- The WG was established to harmonize T&E instrumentation and autonomous/robotic requirements, study feasibility of future cooperative T&E program activities, and exchange data reports on specific T&E issues of mutual interest with Germany.

16. Reciprocal Use of Test Facilities Project Arrangement (RUTF PA) Concerning Test and Evaluation of the German Special Forces Reconnaissance and Combat Vehicle (AGF2)

- This new PA with Germany went into effect in July 2024 and lasts until July 2025. It permits testing at various U.S. test facilities.
- The PA allows the German Army to test their new ground combat vehicle, AGF2, in a variety of climatic conditions.

17. Assault Rifle in Extreme Environments RUTF PA

- This new PA with Germany went into effect in May 2024 and lasts until May 2025. It permits testing at various U.S. test facilities.
- The PA allows the German Bundeswehr to test their new assault rifle in three different environments (desert, cold, and tropical) at U.S. test ranges.

18. Reciprocal Use of Test Facilities Project Arrangement Concerning Test and Evaluation

(T&E) of the German Special Forces G39 19 Suppressed Assault Rifle, P14 Pistol, and AG40-4 Grenade Launcher in Extreme Environments

- This new PA with Germany went into effect in May 2024 and lasts until May 2026. It permits testing at various U.S. test facilities.
- The PA enables the German Bundeswehr to test an assault rifle, pistol, and grenade launcher in three different environments (desert, cold, and tropical) at U.S. test ranges in the coming year.

19. Land Platforms Autonomy and Robotics WG Terms of Reference (TOR)

- This WG with Italy went into effect in January 2020 and lasts until January 2030.
- The WG, led by the U.S. Army, exchanges data with Italy on test operating procedures and standard operating procedures relevant to testing unmanned vehicle maneuverability and weaponized autonomous platforms. The group is also sharing technology development updates on data acquisition, precision tracking and system surveillance, and other measurement techniques concerning T&E of autonomous vehicle systems. This WG effort will facilitate demonstration of test capabilities at facilities responsible for testing autonomous systems' mobility and weapon systems performance.

20. Memorandum of Understanding between the Japanese Defense Forces and the US DoD for Test and Evaluation Program (TEP) Cooperation

- This new PA with Japan went into effect in March 2024 and lasts until March 2049.
- The purpose of the TEP memorandum of understanding is to allow T&E activities that are authorized in accordance with the national procedures of the participants.

21. Reciprocal Use of Test Facilities Project Arrangement Concerning Netherlands F-35 Follow-On Operational Test and Evaluation

- This new PA with the Netherlands went into effect in May 2024 and lasts until February 2034. It permits testing at Edwards AFB, California.
- The PA evaluates the operational effectiveness, suitability, survivability, lethality, and vulnerability of the capabilities for the Ministry of Defense F-35 Air System in an operationally realistic environment.

22. Memorandum of Understanding Between the Department of Defense of the United States of America and the Minister of Defence of the Kingdom of the Netherlands for Test and Evaluation Program (TEP) Cooperation

- This PA with the Netherlands went into effect in February 2004 and lasts until February 2034.
- The purpose of the TEP memorandum of understanding is to allow the general provisions and conditions that will apply to the initiation, conduct, and management of T&E activities that are authorized in accordance with the national procedures of the participants.
- The PA included one new amendment in FY24, which extended the duration by ten years until 2034.

23. Over-the-Horizon Weapon System Reciprocal Use of Test Facilities Project Agreement

- This new PA with Norway went into effect in April 2024 and lasts until April 2026. It permits testing at Andøya Test Center in, Andøya, Norway.
- The objective of the Over-the Horizon Weapon System RUTF PA is to test and evaluate two Over-the-Horizon Weapon System encanistered missile-test assets.

24. Oceanographic and Acoustic Systems (OAS) Reciprocal Use of Test Facilities Project Agreement

- This PA with Norway went into effect in September 2023 and lasts until September 2027. It permits testing in Norwegian territorial waters.
- The PA permits T&E of U.S. DoD oceanographic and acoustic systems aboard a Norwegian Ministry of Defense (NO MOD) vessel in Norwegian waters. The U.S. DoD and NO MOD will leverage the unique traits of the Norwegian waters and a NO MOD vessel under NO MOD command to (1) determine the viability of U.S. DoD oceanographic sensors to capture sub-

mesoscale and other oceanic motions, and (2) determine the capabilities of U.S. DoD acoustic instruments to evaluate the effects of sub-mesoscale motions on acoustic transmission-loss variability and other factors. The NO MOD will test and evaluate the U.S. DoD oceanographic and acoustic equipment during three sea trials.

25. T&E of the United Kingdom 28 Engineer Regiment (C-CBRN), Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Defense Tactics, Techniques, and Procedures (TTPs) RUTF PA

- This PA with the United Kingdom went into effect in January 2021 and lasts until January 2031. It permits testing at Dugway Proving Ground, Utah.
- The PA enabled the development and testing of partner defense TTP against CBRNE threats. The U.S. Army Dugway Proving Ground hosts the tests, providing threat-representative scenarios to support evaluation of the operational effectiveness of new detectors, PPE, and decontamination equipment in an operationally representative environment. Tests also included the firing of various weapons by soldiers in protective clothing to evaluate the clothing's potential effects on mission effectiveness.

26. T&E of Protective Ensembles Using the Porton Man Test Fixture CTE PA

- This PA with the United Kingdom went into effect in May 2020 and lasts until May 2027. It permits testing at Porton Down, Wiltshire, United Kingdom.
- The PA has enabled extensive use of the Porton Man mannequin to test chemical protective clothing for military personnel.
- Currently, the Porton Man tests are continuing to develop test methods and conduct performance testing of chemical protective ensembles (suits) against actual chemical warfare agents. Porton Man is an articulated, life-size, moving mannequin with a combination of cumulative and real-time sensors that can quantify the permeation and penetration of various threat agents through chemical biological PPE. The Porton Man Cooperative Test and Evaluation (CTE) PA supports U.S. DoD requirements to protect personnel from chemical biological threats.

27. TOR for Live Fire WG

- This WG with the United Kingdom went into effect in October 2010 and lasts until October 2025.
- The WG, led by DOT&E, was established to identify potential collaborative efforts in LFT&E, to include ground combat vehicles and PPE.

28. Integrated Air and Missile Defense (IAMD) Testing Reciprocal Use of Test Facilities (RUTF) Project Arrangement (PA)

- This PA with the United Kingdom went into effect in November 2012 and lasts until November 2027. It permits testing at the Hebrides Test Range, Scotland, United Kingdom.
- The PA with the United Kingdom permits large-scale missile defense tests every two years, including the latest in the series, Formidable Shield 2023 (FS23). In May 2023, the Maritime Theater Missile Defense Forum participated in Naval Striking and Support Forces NATO exercise FS23. The purpose of FS23 was to improve allied interoperability in a live-fire joint IAMD environment, using NATO command and control reporting structures. Testing included 12 NATO allied and partner nations; 24 ships; more than 35 aircraft; 8 ground units consisting of radars, National Advanced Surface-to-Air Missile System, High Mobility Artillery Rocket System; and nearly 4,000 personnel from across the alliance that participated in the event. Building on the achievements of previous Maritime Theater Missile Defense Forum events, FS23 increased coalition interoperability and joint capabilities through complex scenarios designed to meet tomorrow's air defense and ballistic missile defense challenges.
- The PA included one new amendment in FY24 that allows additional testing at FS25.

29. Counter-Laser Directed Energy Weapons (CLDEW) RUTF

- This PA with the United Kingdom went into effect in April 2023 and lasts until

April 2027. It permits testing at the Army Research Laboratory, Adelphi, Maryland.

- The purpose of this RUTF is to test the laser damage and vulnerability of the United Kingdom's cameras, imaging systems, and optical materials to various lasers.

30. Cybersecurity Assessment Working Group Terms of Reference

- This WG with Australia, Canada, New Zealand, and the United Kingdom went into effect in December 2022 and lasts until December 2027.
- The WG identifies and develops collaborative efforts to increase the cybersecurity of coalition missions and joint weapons systems.

31. Tactics Validation and Operational Readiness Assessment RUTF PA

- This PA with Australia, Canada, and the United Kingdom went into effect in August 2023 and lasts until August 2026. It permits testing at Naval Air Weapons Station, China Lake, California.
- The PA evaluates the effectiveness of the defensive tactics of Royal Canadian Air Force aircraft and to assess the capability of Canadian Tactical Aviation personnel to conduct realistic mission sets in an EW threat environment.

32. Aircraft Electronic Warfare Cooperative T&E Project Arrangement

- This PA with Australia, Canada, and the United Kingdom went into effect in May 2016 and lasts until August 2026. It permits testing at various partner test locations.
- Activities and plans for the coming years under this PA are described in detail in the Center of Countermeasures section of this Annual Report.

33. F-35 Follow-on Operational Test and Evaluation Cooperative Test and Evaluation Project Arrangement

- This new PA with Australia and the United Kingdom went into effect in October 2023 and lasts until October 2033. It permits testing at Edwards AFB and China Lake Naval Air Weapons Station, California.
- The PA allows cooperative FOT&E of the F-35 Joint Strike Fighter air systems. It will support the contributing participants' continued efforts to evaluate the operational effectiveness, suitability, survivability, and lethality of F-35 air systems in operationally representative environments. The contributing participants, under the F-35 FOT&E PA, will also evaluate the interoperability of the F-35 with multiple coalition systems; eliminate redundant T&E costs; increase commonality and interoperability; provide safety, airworthiness, and mishap investigation capabilities; and provide test reports.

Joint Aircraft Survivability Program (JASP)

In FY24, the Joint Aircraft Survivability Program (JASP) continued advancing tools, processes, infrastructure, and workforce to demonstrate progress towards transforming the OT&E and LFT&E of aircraft survivability. JASP also continued to deliver new techniques and technologies, demonstrating the potential to enhance the survivability of U.S. aircraft in contested, multi-domain operations.

JASP advanced aircraft survivability T&E capabilities by validating and releasing new modeling and simulation (M&S) capabilities, enabling enhanced evaluations of red threat engagements against blue rotary-wing aircraft in the low-altitude battlespace. In addition, JASP: (1) released defensive cyber analysis capabilities for OT&E and LFT&E in support of aircraft survivability evaluations and completed the first cyber LFT&E demonstration on a full-up operational aircraft, (2) completed design and development of advanced electro-optical (EO)/ infrared (IR) guided missile hardware-in-the-loop simulators and a new 2-Color Infrared (2CIR) missile warning system stimulator for IR countermeasures T&E, (3) significantly expanded the test dataset characterizing dry bay fire ignition on aircraft from kinetic threats (fragments and bullets) for development of version 2.0 of the Next Generation Fire Model (NGFM) beginning in FY25, (4) continued maturing and testing future concept of operations (CONOPS) that enable aircraft combat damage incident reporting in anti-access/area denial environments, (5) increased aircraft threat detection and countermeasure capabilities by completing an assessment of Directed Infrared Countermeasure escort protection capabilities and limitations, and by demonstrating new electronic attack (EA) techniques and analytical tools to counter advanced radar threats, and (6) improved aircraft and personnel protection by maturing a flammable fluid mist control additive through testing to characterize fire prevention performance, qualify the additive for use in avionics cooling systems, and demonstrate low-rate production with a path to scale up manufacturing.

PROGRAM OVERVIEW

The Joint Technical Coordinating Group on Aircraft Survivability (JTCG/AS) was chartered in 1971, in response to high aircraft loss rates experienced during the Vietnam War. The JTCG/AS initially focused on aircraft susceptibility reduction (design characteristics that make an aircraft harder to detect) and aircraft vulnerability reduction (design characteristics that give an aircraft the ability to withstand a hit). The JTCG/AS focus later grew to include M&S and establishing aircraft survivability as a design discipline through the development of a formal curriculum at the Naval Postgraduate School.

In 1985, the oversight responsibility of the JTCG/AS was assigned to the newly established Joint Aeronautical Commanders Group. Funding for the JTCG/AS was consolidated under what is now the DOT&E.

In January 2003, the Joint Aeronautical Commanders Group signed a new charter establishing JASP to replace the JTCG/AS, while expanding the JTCG/AS charter to include the Joint Combat Assessment Team (JCAT).

In 2005, the Service aviation systems commands (U.S. Army Aviation and Missile Command, U.S. Air Force Life Cycle Management Center, and Naval Air Systems Command [NAVAIR]) chartered JASP as it is known today.

MISSION

JASP develops cross-Service aircraft survivability solutions and evaluation methods needed to dominate the air domain and mitigate U.S. aircraft losses in combat. 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.
- Develops and manages enterprise-level digital tools required to support comprehensive evaluation of aircraft effectiveness and survivability, with confidence.
- Collects and analyzes U.S. aircraft combat damage and losses via the JCAT, 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 aircraft survivability enhancement features.

FY24 KEY ACTIVITIES

» ADVANCING THE CAPABILITY AND CREDIBILITY OF JOINT AIRCRAFT COMBAT EFFECTIVENESS TOOLS

Acquisition Community, Combat Mission Planning, Training, and Weapon Schools

JASP's Survivability and Lethality of Aircraft in Tactical Environments (SLATE) provides a two-sided combat simulation with "First Look," "First Shot," "First Kill" capability over the survival/kill chain. SLATE supports two-sided combat from one-on-one to several-on-several. The SLATE user selects which players (i.e., shooters, weapons, and targets) to include in the engagement simulation. The user defines events that cue shooter and target reactions. All inflight aircraft and weapons players are based on high-fidelity simulations.

Early in FY24, SLATE version 1.1.1 was released by the Defense Systems Information Analysis Center as a controlled unclassified information and classified application. During FY24, the SLATE development team worked several long lead tasks, as shown in the SLATE Operational View 1 in Figure 1. These tasks supported medium/high and low altitude, multi-domain, and two-sided air combat analysis capabilities. FY24 activities included:

- Radio frequency (RF) propagation losses
- Naval surface-to-air missile (SAM) simulations
- Electronic Warfare (EW) countermeasures
- Rotary-wing/tilt-rotor simulations
- Air defense artillery (ADA) sites

The SLATE user interface/user experience includes interactive, virtual range, and constructive batch capabilities. SLATE supports importing multiple types of terrain that are used for advanced displays and simulation effects. Figure 2 shows the SLATE user interface/user experience geographical displays for rotary- and fixed-wing aircraft with terrain imagery.

SLATE leverages the Hybrid Integration and Visualization Engine and the Agile Combat Effects Library (ACEL) to enable multi-domain two-sided air combat analyses with a growing suite of capabilities and data. This integration

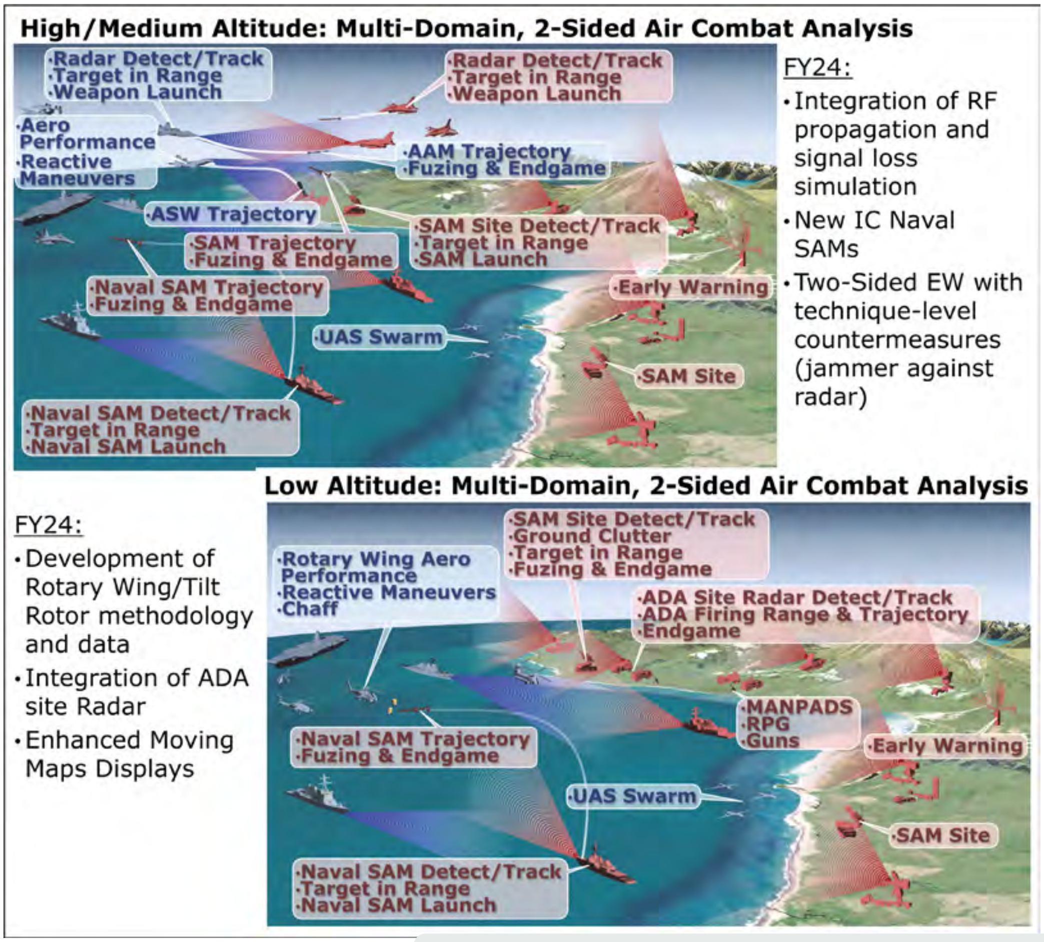


Figure 1. SLATE Operational View 1 (OV-1)

AAM – Air-to-Air Missile; ADA – Air Defense Artillery; ASW – Anti-Submarine Warfare; EW – Electronic Warfare; IC – Intelligence Center; MANPADS – Man-Portable Air Defense System; RF – Radio Frequency; RPG – Rocket-Propelled Grenade; SAM – Surface-to-Air Missile; UAS – Unmanned Aerial System

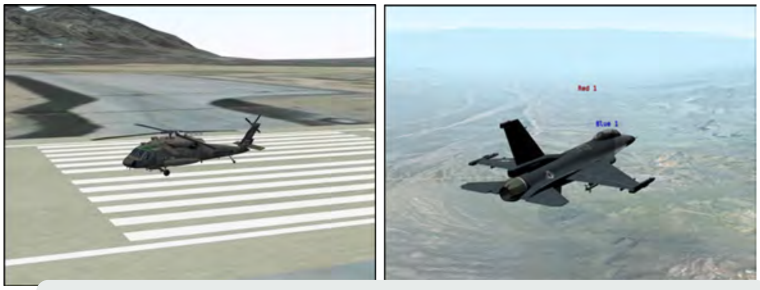


Figure 2. SLATE Rotary- and Fixed-Wing Aircraft Graphical Displays with Terrain Imagery

architecture enables fast implementation of supplier authoritative simulations and data (e.g., the intelligence community, system program office).

As SLATE evolves, it will become suitable for future LFT&E evaluations, provide a more complete evaluation with less time and cost, and provide a streamlined path for implementing blue system simulation and data into ACEL. ACEL is a major component of the Joint Technical Coordinating Group for Munitions Effectiveness Joint Anti-Air Model application. Leveraging this architecture enables sharing between the acquisition (SLATE) and operational warfighter (Joint Anti-Air Model) simulations.

In FY24, JASP completed long-lead development of the aero performance (BlueMax) rotary-wing capability. It was released by the Defense Systems Information Analysis Center as a controlled unclassified information application. BlueMax version 7.2 is included within SLATE and is accessible via the ACEL Application Programming Interface (API) and ACEL Micro API.

ACEL Micro APIs provide specific simulation capabilities that can be leveraged by external simulation frameworks. Current development is enabling the ACEL aero performance simulation and library of aero data to be reused as a "plug-in" into the Advanced Framework Simulation framework. Additional reuse with other frameworks (Joint Simulation Environment and Integrated Threat Analysis Simulation Environment) are being assessed. The reuse of the ACEL simulations and data through the Micro APIs provide authoritative and consistent results across the DoD.

JASP advanced SLATE and ACEL through integration of authoritative intelligence center EW red (hostile) players. SLATE simulates the interaction of the red (hostile) radars with blue jammers, using the pulse descriptor word interface, enabling two-sided EW with technique-level countermeasures. SLATE version 1.2 release is scheduled for November 2024.

» DEVELOPING AND MANAGING ENTERPRISE-LEVEL DIGITAL TOOLS

Supporting Comprehensive Evaluation of Aircraft Effectiveness and Survivability, With Confidence

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), multiple domain two-sided air combat simulation SLATE, and the vulnerability analysis code Computation of Vulnerable Area Tool, along with its supporting penetration and fire prediction codes Projectile Penetration, Fast Air Target Encounter Penetration, and the NGFM.

In FY24, JASP continued the effort to develop tools for cyber and high-energy-laser (HEL) non-kinetic threats. JASP continued to add cyber survivability evaluation capability to the Cyber Operations and Lethality Effectiveness tool. A new risk assessment module calculates the likelihood and mission impact of a potential threat against critical system components, informing decision authorities for determinations on risk tolerance/acceptance. New data flow modeling enables characterization and assessment of the impact to critical data from potential threats. Automated system characterization and data ingestion techniques improved the efficiency of assessing aircraft systems. New tools were added to semi-automatically perform standardized, repeatable cyber survivability assessments to quantify a mission system's ability to detect and recover from cyber events. This effort, in collaboration with the Air Force, Army, and Navy aviation cyber survivability communities, provides M&S capability and data standardization to develop and evaluate aircraft survivability in contested cyberspace.

JASP initiated a two-year effort to achieve interoperability of HEL-relevant M&S toolsets for practical HEL survivability analysis by 2025, with associated processes, metrics, and supporting test data. The effort will also identify data voids, M&S capability limitations, and other factors limiting platform-level survivability analysis.

Collect and Analyze U.S. Aircraft Combat Damage and Losses Using the JCAT

In FY24, JASP continued to enable aircraft combat damage incident reporting through the JCAT. The JCAT is heavily engaged with U.S. Indo-Pacific and European Commands supporting operational commanders with combat data collections while also leveraging operational exercises. They continued development of a new CONOPS utilizing Title 50 (i.e., intelligence) tools to enable the near real time forensics of aircraft combat damage in anti-access/area denial theaters of operation.

JCAT launched a third phase of aircraft combat damage assessment training with two objectives: (1) to impart to students a situational knowledge of naval aviation missions, capabilities, and tactics as well as present and potential threats; and (2) to offer practical training, including a hands-on exercise, in the use of National Technical Means tools. By completing this course, assessors learned to effectively characterize incidents, perform threat analysis, and develop aircraft combat damage reports that will inform combatant commanders rapidly and provide the DoD critical data to address aircraft survivability gaps.

To mature the JCAT CONOPS and further solidify the command-to-command relationships, the JCAT took advantage of previous large-scale exercise observations of the 692 ISR Group (DGS-5) and the 8th Intelligence Squadron Air Domain Awareness Cell. Moreover, the JCAT expanded observation and growth to additional sites for mission execution during Valiant Shield 2024. JCAT assessors executed daily operations for 15 consecutive days in support of JCAT CONOPS maturation, training and development of toolsets and procedures, and building working relationships with active component commands. The team also leveraged established DGS-5 and 8th Intelligence Squadron Air Domain Awareness Cell best practices and explored new tools, processes, and functional teams to support CONOPS maturation and refinement from prior years. The team focused on developing an assessment product that is viable and supports timely and relevant transfer of information to the respective operational commanders.

» DELIVERING INNOVATIVE SURVIVABILITY ENHANCEMENT FEATURES

Threat Detection and Countermeasures Technologies

In collaboration with OSD and Service organizations, JASP matured threat detection and countermeasure technologies needed to defeat advanced EO/IR and RF-guided threat systems. JASP's adaptability allows it to adjust its portfolio to quickly fill critical gaps in technologies required by Service programs while maintaining its core efforts of developing and testing self-protection countermeasure techniques. The Naval Research Laboratory (NRL) completed the Directed Infrared Countermeasure Escort Protection Concept project quantifying

Figure 3. 2CIR missile warning simulator hardware and primary beam improvement

countermeasure system performance in formation flight against several EO/IR guided threat classes.

NRL completed development and testing of a threat launch simulator for testing 2CIR missile warning systems. The new simulator reproduces missile launch features used by 2CIR missile warning systems while significantly reducing the recovery time between engagements. The simulator, shown in Figure 3, will transition to the Center for Countermeasures to support OSD and Service IR countermeasures T&E.

The Naval Surface Warfare Center Crane Division continued work on Reconfigurable Signal Injection Missile Simulation, using hardware-in-the-loop simulation of advanced threats. These hardware-in-the-loop simulators, for multiple reticle-based IR missiles utilizing actual missile seeker tracking and guidance hardware, support development and evaluation of aircraft threat countermeasure techniques and technologies, improving the efficiency and speed of delivering survivability effectiveness to the fleet.

NRL completed the Manipulative Geo-Indicator Countermeasures project to develop and validate analytical tools to develop EA techniques to counter advanced passive RF threat systems. In FY24, NRL validated Manipulative Geo-Indicator Countermeasures with testing at the Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland.

NRL continued work with NAVAIR's Advanced Tactical Aircraft Protection Systems Program Office (PMA-272) to develop firmware and software to support their next generation Digital Radio Frequency Memory system for countermeasure effectiveness development and training. The new user interface architecture and design will enable the development and test of new EA techniques to counter advanced RF-guided threat systems.

Aircraft Force Protection

In FY24, JASP matured a low-weight, retrofittable mist control additive to significantly reduce the ignition of flammable avionics cooling fluids from warhead fragmentation. The U.S. Army Combat Capabilities Development Command completed fragment threat testing of treated fluids, quantifying the probability of ignition reduction. The Army Research Laboratory conducted MIL-PRF-27252C testing to qualify the additivized cooling fluid for use in electronic applications, and Army Research Laboratory / California Institute of Technology worked with fluid efficiency to demonstrate low-rate production and develop a path to scale up production.

The NAVAIR's Naval Aviation Red Team (AIR-RT) performed a deep-dive cyber vulnerability assessment on the P-8A Poseidon, a U.S. Navy weapons system essential to the mission of hunting submarines. AIR-RT's evaluation identified novel cyber threat vectors to the Navy's program leadership and validated the remediation of previously identified cyber deficiencies. The effort also demonstrated a repeatable process and methodology for performing cyber LFT&E and full spectrum survivability evaluations. AIR-RT, in concert with its partners, took existing test approaches and techniques to new heights through this evaluation, which culminated with on-aircraft testing.

AIR-RT also partnered with industry to develop digital twins and models of P-8A avionics components (in this case, software and real-time operating systems rehosted on emulated hardware) to provide an accurate representation of the mission systems for cyber-attack tool development. The digital twins and models rehosted mission systems avionics software on emulated hardware, enabling cyber vulnerability research to be performed with increased efficiency. Partnering the cyber with the kinetic threat survivability community through this endeavor helped merge two worlds, and two separate lexicons, into one integrated test team. In developing a process for performing cyber LFT&E, this initiative paved the way for the joint Services to undertake similar efforts.

Aircraft Survivability T&E

JASP made notable progress in delivering validated models of red radar systems that can acquire and track blue rotorcraft in low-altitude RF environments. This initiative, termed Joint Aircraft Threat Model Simulation Validation, focused on signal propagation and processing, rotary-wing flight dynamics, and countermeasure effectiveness to simulate radar phenomena such as rotor blade flash, chaff dispense, and environmental clutter.

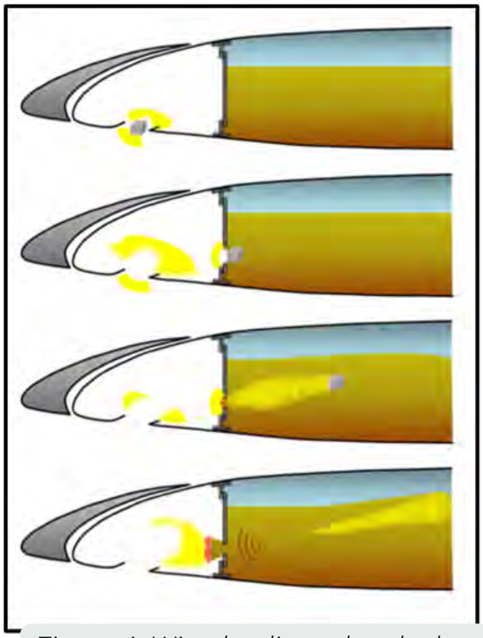


Figure 4. Wing leading edge dry bay fire ignition process

The team conducted open-air tests to validate and assess the accuracy of the BlueMax, ESAMS, and SLATE M&S capabilities using the MV-22B platform. These validated models will help evaluate the effectiveness of Blue-Sky chaff dispensing and rotorcraft detectability in cluttered environments against RF threats. The project's final deliverables will include the integration of updated ESAMS features into SLATE, reflecting new systems and capabilities.

Ballistically initiated fire presents the largest vulnerability for fixed-wing aircraft. The U.S. Air Force 704th Test Group Aerospace Survivability and Safety Office, Air Force Life Cycle Management Center, and U.S. Army Combat Capabilities Development Command Analysis Center conducted fragment and armor piercing incendiary testing to support development of NGFM version 2.0. This model, by credibly predicting dry bay fire ignition from kinetic threat impacts, will improve the capability to develop, test, and evaluate the survivability of aircraft from fire initiated by enemy weapon impacts. Figure 4 shows the wing leading edge dry bay fire ignition process; a fragment flash from hitting the leading edge, interacts with fuel spurting from the wing integral fuel tank to ignite a fire in the dry bay.

The team conducted hundreds of tests that significantly expanded the relevant dataset establishing statistical confidence in the prediction algorithms. To extract test data from high-speed video more effectively, the team is also looking into machine learning and artificial intelligence. Moreover, they are exploring the use of the Arbitrary Lagrangian Eulerian Three-Dimensional high-fidelity physics-based model to supplement the experimental data with variations in test configurations, such as tank sizes, ullage volumes, and shotline placement. This data, along with other test data, will be used to develop NGFM version 2.0 with a planned release in the 4QFY25.

Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) Program

In FY24, the Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) program applied modern software development methods to demonstrate the ability to increase the capability, user interface, experience, and integration of weaponeering tools more effectively and efficiently.

JTCG/ME uses target vulnerability data, standards, methodologies, and processes to advance the weaponeering capabilities and accuracy of lethality effects and collateral damage estimation (CDE) against kinetic, maritime, cyber, electromagnetic spectrum (EMS), and directed energy targets. In FY24, the JTCG/ME program used automated data collection to collect over 250,000+ strike and 48,000+ mission report products to analyze, inform reach-back support, and support weaponeering tool verification and validation, training, and expenditure analysis. In FY24, JTCG/ME generated 15 reach-back packages for weaponeering, CDE, and munition effectiveness assessment in support of current operations.

In coordination with the Joint Live Fire (JLF) program, JTCG/ME also continued to collect data to underpin the methodology required to advance full-spectrum survivability and lethality methods and tools applicable to operations planners and OT&E and LFT&E of DoD systems and services.

PROGRAM OVERVIEW

The JTCG/ME program was chartered in 1968 to serve as the DoD's focal point for munitions effectiveness information. It started by delivering Joint Munitions Effectiveness Manuals (JMEMs) – the sole source for all non-nuclear weapons effectiveness data and methodology for the DoD. The JMEMs have been the "how to" manuals for determining the type and number of ordnances on target. Today, JMEMs have transitioned to kinetic and non-kinetic tools used in operational weaponeering, and CDE in direct support of multi-domain operations, mission planning, and training. These tools are used by joint and Service planners in force-on-force effect estimations, mission area analysis, requirements studies, and weapon procurement planning. These tools are also used by the Service acquisition community in performance assessments, analyses of alternatives, and survivability enhancement studies. These include:

- The Digital Imagery Exploitation Engine (DIEE), a tool that enables users to plan and execute kinetic strikes by seamlessly performing the following Advanced Target Development steps:
    1. Geographically locate and characterize the target
    2. Weaponeer the target using JMEM Weaponeering System (JWS)
    3. Perform target coordinate mensuration
    4. Determine CDE using the Digital Precision Strike Suite Collateral Damage Estimation (DCiDE) tool
    5. Produce and output graphics to the appropriate databases
- The Joint Anti-Air Combat Effectiveness, a tool that supports development of aircraft and weapon tactics using the Joint Anti-Air Model (JAAM). Operators across the DoD are using JAAM daily to refine planning and debriefing air combat tactics, techniques, and procedures (TTP).
- Weaponeering tools capable of estimating lethal effects for directed energy weapons (DEW), cyber, maritime targets, and EMS fires.

The JTCG/ME program executes the JLF program. JLF performs a critical role within the survivability/lethality analytic community by delivering infrastructure, models, simulations, and data to support testing and experimentation of kinetic and non-kinetic systems in operationally relevant contexts to inform, improve, and act as a consistent foundation for LFT&E and warfighter tools and techniques.

MISSION

The JTCG/ME program develops, advances, and sustains weaponeering tools. These tools, frequently referred to as JMEM products, are used by the combatant commands (CCMDs) to estimate and optimize the type and number of U.S. offensive kinetic and non-kinetic capabilities required to achieve the desired lethal effect. These products support assessment against a range of kinetic and non-kinetic strategic or tactical targets, while mitigating risk for collateral damage including civilian casualties.

JTCG/ME partners with the JLF program to develop and enhance full-spectrum survivability and lethality digital tools (including kinetic and non-kinetic effects); improve survivability and lethality T&E methods and processes; and enable live data collection to support rigorous verification, validation, and accreditation of survivability and lethality digital tools.

FY24 KEY ACTIVITIES

» DELIVERING CREDIBLE WEAPONEERING TOOLS TO CCMD STRIKE AUTHORITIES

JMEMs are used daily by warfighters worldwide in direct support of operations, mission planning, and training. The user base includes approximately 26,000+ accounts, spanning the following entities:

- DoD Service members
- Joint Staff/CCMDs
- Multiple coalition partners
- Acquisition community

- T&E enterprise
- Intelligence Community
- National Laboratories

In FY24, JTCG/ME fielded updates to DIEE to improve product accuracy and efficiency in support of operational warfighters. Specifically:

- In collaboration with Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) and the Joint Staff Directorate for Intelligence (J-2), JTCG/ME has been improving the efficiency and effectiveness of the Joint Targeting Intelligence process by developing, standardizing, and integrating the Advanced Target Development federated workflow management tool, Workflow Application for Recording Products and Targeting History (WARPATH). As part of this process, operational users will be able to link desired effects to tactical tasks outlined in operational plans, which will increase the probability of meeting the commander's objective via enhanced integration and connectivity across the targeting enterprise to enable targeting at scale.
- JTCG/ME has been applying modern software development methods to enable continuous and incremental improvement in capability, user interface, and experience of JWS tools. JTCG/ME also added new weapon and weapon trajectory data to its scene-based weaponeering products, allowing the strike authorities to account for enhanced technologies and capabilities in their calculations of target defeat. To maintain consistency with the latest National Geospatial-Intelligence Agency mensuration methods, JTCG/ME updated calculation tools for both Mensuration Services Program and Common Geopositioning Services.
- JTCG/ME completed updates to collateral effects radii tables, reducing their error margins. It advanced the friendly force collateral effects library mitigation tool to increase the efficiency of collateral effects analysis and enhance risk estimate distance calculations used by DCiDE.
- The JLF program responded to DOT&E requests for information related to Traumatic Brain Injury (TBI). The program also hosted a large technical exchange to evaluate the current understanding of TBI from blast events and identify paths forward for improving characterization, prediction, and mitigation of TBI. JLF is partnering with Defense Center for Public Health, U.S. Army Medical Research & Development Command, and DOT&E to bring together the acquisition, analytical, operational and medical communities to execute projects designed to better inform the risk of TBI from blast events associated with weapons employment and training.
- JTCG/ME generated 15 reach-back packages for weaponeering, CDE, and munition effectiveness assessment in support of current operations.
- JTCG/ME facilitated 23 training classes/events for 350+ students. Training of integrated product capabilities (DIEE/JWS) continues to enable the operational community to successfully employ munitions while minimizing collateral damage.

» ADVANCING THE CAPABILITY, EFFICIENCY, AND ACCURACY OF TARGET DEVELOPMENT TOOLS

JTCG/ME advances the efficiency and accuracy of target development tools for a complex and dynamic multi-domain environment. JTCG/ME upgraded existing weaponeering capabilities to increase the effectiveness of kinetic strikes and developed new capabilities to enable deliberate and dynamic engagements using cyber, EMS, and DEW capabilities.

Advanced Target Development

The DIEE is a vital software program for the targeting enterprise at the global level. The DIEE provides digital solutions to the essential Joint Targeting Cycle functions for both the U.S. and coalition partners.

The DIEE software turns current workflow inefficiencies into automated and integrated solutions within one ecosystem. DIEE's essential targeting functions apply across the targeting spectrum and address basic, intermediate, and advanced target development. Key functions include target coordinate mensuration, weaponeering methodologies using

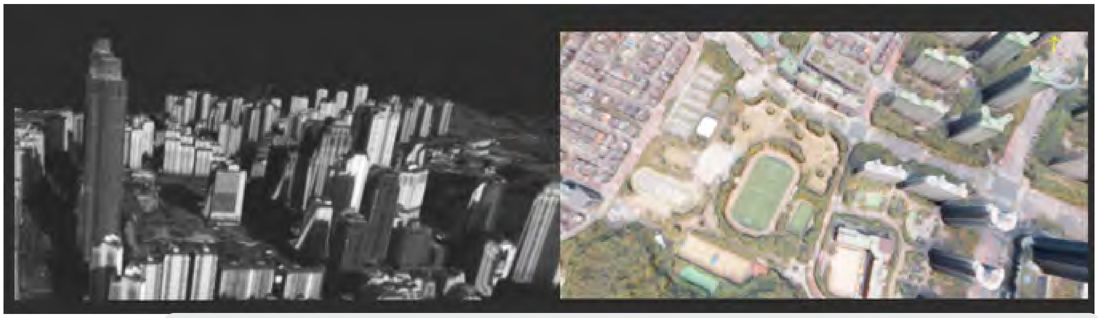


Figure 1. Examples of native 3D viewing capability no longer requiring additional hardware

JWS, CDE effects using the DCiDE tool, targeting graphics production, and combat assessment.

FY24 accomplishments include the first release part of the 3.x product baseline - DIEE v3.0.1. This release includes new capabilities such as native 3D viewing without hardware dependencies (as shown in Figure 1), ability to perform mensuration on emerging 3D datasets, and initial support for the Capability Solutions Package (CSP) construct. This version also includes updates to DCiDE to remain compliant with the latest policy updates. In addition, integration efforts with JWS and other external services/tools continues in support of all phases of target development.

As part of the OUSD(I&S) and J-2 Joint Target Intelligence Modernization (JTIM) initiative, JTCG/ME initiated the development of a federated workflow management tool, WARPATH. This tool aids in streamlining the targeting enterprise production, tracking process while reducing duplicative efforts and costs. WARPATH will be a standalone web application that is interoperable with DIEE and all other JTIM associated programs.

Weaponeering

The JWS combines a series of weapon system characteristics, delivery accuracy, and target vulnerability data needed to estimate the final aimpoint, delivery conditions, and number of weapons on target necessary to achieve combatant commanders desired lethal effects. In FY24, JWS v2.4.2 continued sustainment efforts with the next planned release in late 2024 to support urgent operational needs and to align with DoD cybersecurity requirements. The next generation JWS 1.x plug-in product line continues development of weaponeering capabilities including structural targets (shown in Figure 2), interior and exterior personnel, materiel targets, modernization of weaponeering support tools, and integration with DIEE 3.x. Capabilities of future versions of JWS include continued expansion of auxiliary tools, buried structures, bridge and linear targets, and the incorporation of higher fidelity methodologies for improved result computation.

CDE

In FY24, JTCG/ME made significant progress toward improving the ability of the DoD and coalition partners to accurately characterize the CDE associated with lethal effects of U.S. weapons. Specifically, JTCG/ME continued the execution of the multiyear Enhanced Weaponeering and CDE test program to quantify the collateral effects resulting from munitions detonating either in the ground or beneath structures. Data sets from the Enhanced Weaponeering and CDE test

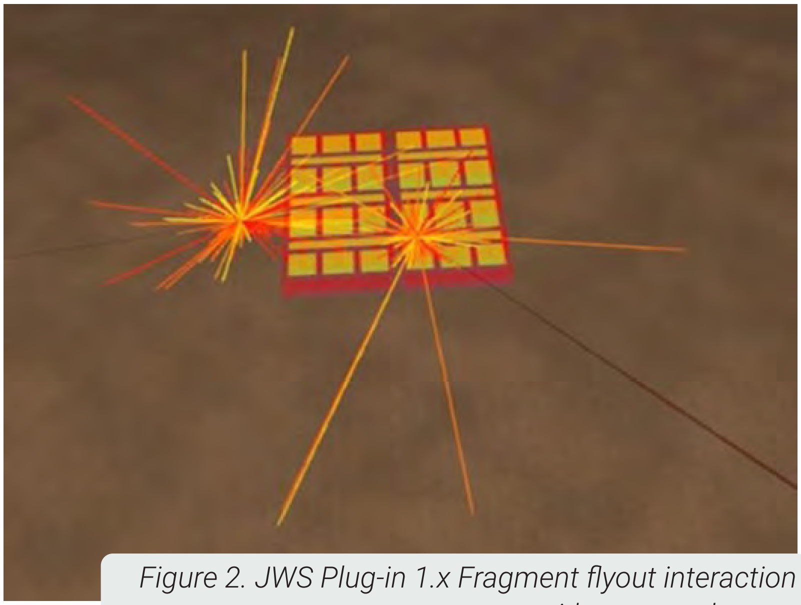


Figure 2. JWS Plug-in 1.x Fragment flyout interaction with structural target

Figure 3. Buried ordnance test conducted in partnership with the U.S. Army Engineer Research and Development Center at Fort Johnson, Louisiana

program were used to improve, verify, and validate high fidelity digital tools used to predict building debris mass and velocity distributions from multiple structure types, along with crater ejecta, ground shock, and blast pressure for various soil types and munition burial configurations. The uncertainty in these predictions must be minimized, as they are the foundation for fast-running engineering models used by the DCiDE tool and JWS to estimate weapon collateral damage and lethality.

In FY24, JTCG/ME conducted multiple tests to further the understanding of munition burial (as shown in Figure 3) and building debris effects on personnel and nearby structures (as shown in Figure 4). These live data supported the evaluation of below-ground detonations beneath a covered surface and two-story structure, along with the mitigation of blast and fragmentation effects and the hazards from secondary debris enhancing the validation of the weaponeering and CDE tools. This test program has also offered collaboration opportunities for multiple organizations to gather data for other modeling and simulation (M&S) and methodology development efforts.

Battle Damage Assessment (BDA)

JTCG/ME continued the multiyear effort of verify, validate, and advance the effectiveness of JMEM weaponeering tools by capturing perishable strike information for future analysis. The goal of the BDA program is to collect all strike information to not only analyze strikes and inform reach-back support, but also to support weaponeering tool verification and validation, training, and expenditure analysis.

In FY24, JTCG/ME used automated data collection tools to collect over 250,000+ strike and 48,000+ mission report products from U.S. Central Command, U.S. Africa Command, and U.S. European Command. The data was integrated in the cloud based Joint Battle Damage Assessment Repository (JBAR) and data views were created to analyze the collected information through spatial and data queries (as shown in Figure 5).

Figure 4. Two-story over-burial building debris test conducted in partnership with the U.S. Army Aberdeen Test Center at Aberdeen Proving Ground, Maryland

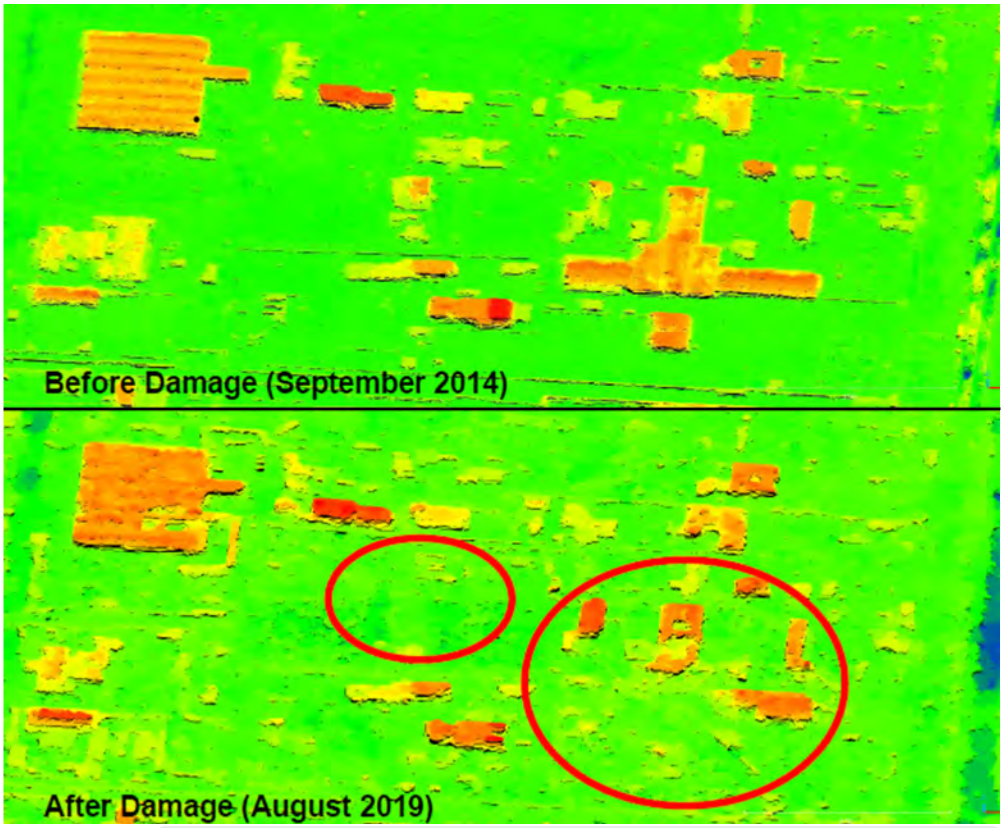


Figure 5. Data collection and analysis of strike event using JBAR

Representational state transfer services are being developed for the hosting of stored data so that strike information can be accessed through an application programming interface (API) with other JTCG/ME.

Lethality/Survivability Improvements

The JLF program continued to improve lethality/survivability assessments and analyses. JLF is uniquely positioned to support DOT&E initiatives and emerging technologies as well as transition the M&S, tools, data, and methods into JTCG/ME operational tools. FY24 JLF efforts included kinetic and non-kinetic lethality improvements. Specifically:

- The Advanced Warhead Characterization, Behind Armor Debris Modernization and Active Protection Systems Enhancements projects improved testing, data collection, and characterization, using advanced analytics and high-fidelity M&S. These improvements were shared throughout the testing, analytic, and operational communities; including the International Test and Evaluation Association, the Test and Resource Management Center, Range Commanders Council, and through international partnerships.
- The Aluminized High Explosives Modeling & Simulation (AHEMS) project dramatically improved the characterization of these unique explosives. Through testing, validated high fidelity M&S, and transitions to fast-running codes, the AHEMS project is bringing accurate predictions of aluminized explosives to warfighter applications, resulting in direct improvements to over 20 existing weapon systems available on current advanced target development tools. AHEMS delivered seventeen technical reports, test data, and improved state-of-the-art high-fidelity codes used by DoD and Department of Energy experts.
- JLF pushed the boundaries of lethality analysis by investing in artificial intelligence (AI)/machine learning (ML). Prototype projects included fitting AI/ML regressions to fragment penetration codes, target vulnerability data, and effectiveness data. AI/ML mathematical fit of effectiveness data have been hosted on a cloud environment to create a first of its kind JTCG/ME Effectiveness as a Service which opens the access to JTCG/ME effectiveness data through computer-to-computer communications via APIs.
- JLF supported DOT&E testing and analysis through improvements to test infrastructure and capabilities. Testing apparatus for multi-shot burst fire were delivered to Aberdeen Test Center. Wireless detonation, which provides reliable and safe detonations for Full Ship Shock Trial, was delivered to Naval Surface Warfare Center. JLF testing and analysis conducted on helmets have shown that obliquity angles of bullets have significant impact on

penetration, and therefore survivability, and will inform future testing requirements.

Lethality of Hypersonic Weapon Systems

In FY24, JTCG/ME and JLF finalized projects addressing the shortfalls related to the evaluation of lethality and associated weaponeering tool capabilities for hypersonic weapons. Hardened autonomous target rafts for Broad Ocean Area testing were delivered to Lawrence Livermore National Laboratories. Autonomous drones with encryption capabilities were delivered and used during recent hypersonic test events. Optical and infrared fragment tracking software has been integrated into the JLF Advanced Warhead Characterization program. Single large mass projectile penetration, cratering, and shock effects were tested, and results have been integrated into high fidelity and fast running codes to improve characterization and effectiveness prediction of hypersonic systems.

Lethal Effect Estimates – Maritime Targets

In FY24, JTCG/ME continues to enhance the ability of weaponeering tools to support the warfighter with credible and timely lethal effects estimates against adversary maritime (surface and subsurface) targets. Within this effort, JTCG/ME has developed the "Maritime Weaponeering Handbook," covering several maritime targets not currently in JTCG/ME inventory. Version 1.0 of the "Target Damage Cards" software, developed by JTCG/ME (shown in Figure 6) will be integrated in the next release of DIEE and enable an interim maritime weaponeering analysis tool for surface and ultimately subsurface targets. JTCG/ME is developing the Maritime Combat Effectiveness (MaCE) operational weaponeering tool, (shown in Figure 7), building on, and adding to, the capabilities of "Target Damage Cards," and integrated into DIEE via plug-in methodology. As indicated in Figure 7 workflow, MaCE will feed CSP data to DIEE.

JTCG/ME continues to execute a collaborative test program that procures data to close knowledge gaps, improve current analytical tools and methods, and

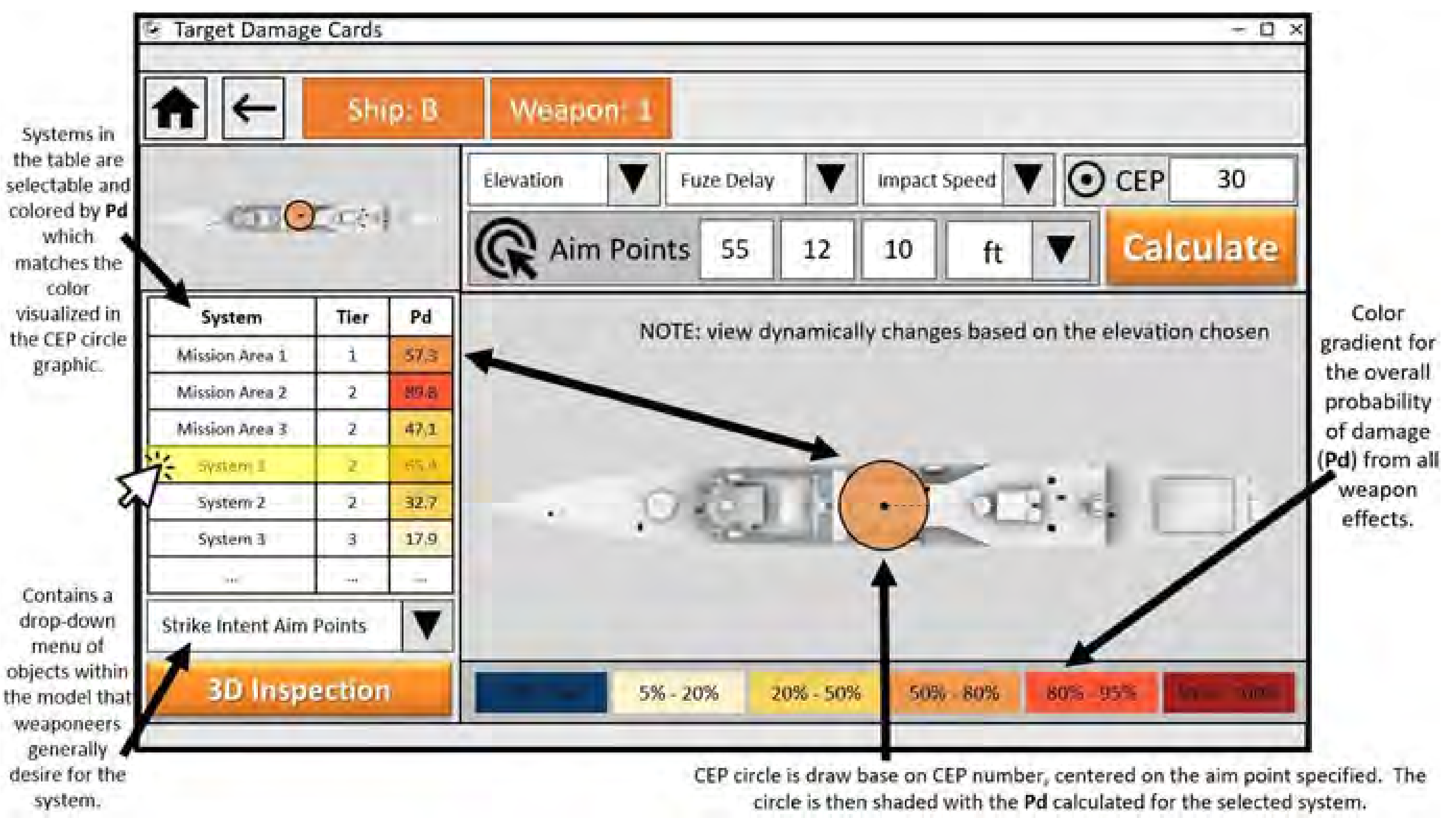


Figure 6. Maritime Target Damage Card visualization tool

develop advanced digital tools required to support the delivery and fielding of weaponeering tools against such targets. This includes the Integrated Naval Simulation for Threat Effects, which will be an engineering level model replacing multiple existing tools and offering best of breed methodologies from those tools for both surface and subsurface targets. Work continues to advance capabilities across the federation of tools, including initiatives related to the Submarine Vulnerable Effects Model, Navy Enhanced Sierra Mechanics, and Dynamic System Mechanics Advanced Simulation. This includes testing and methodology development to predict fire initiation within targets. These efforts increase weapons systems' lethality against foreign maritime threat platforms and will also support more effective and efficient survivability evaluation of U.S. ships and submarines in support of LFT&E objectives.

Aircraft and Weapon Tactics

The JAAM tool is a two-sided operational tool to visualize air-to-air and surface-to-air threat engagements. Prime users of the JAAM application, developed under the Joint Anti-Air Combat Effectiveness Integrated Product Team, are warfighters at test, training, and operational squadrons. Operators are using JAAM daily to support planning, post-mission debriefings with playback, and tactics evaluation with refinement of air combat TTP. JAAM is used across the DoD at 370 sites and 5,600 users. JAAM is used by:

- Operational squadrons
- OT&E ranges
- Mission playback and debriefing applications (government and contractor software)
- Intelligence and acquisition community development of tactics documents
- DoD analysts
- Air, land, sea, space application center fighter interaction team
- Mission planning suites (joint mission planning system - Air Force and Navy)

The JAAM v5.x series is approaching its end of life. The JAAM v5.x series is two-decades old and maintenance is difficult to sustain. The JAAM v6.x series is an entirely new application with a new graphics library and modern architectural design. The JAAM v6.x design includes the following three major components:

- The graphical user interface (GUI)
- The external API
- The Agile Combat Effects Library (ACEL)

The JAAM v6.x GUI (Figure 8) is designed to streamline workflow for the operator. The GUI is designed for three primary use cases: interactive users, virtual range users with event playback to include multiple participants, and iterative studies users supporting few-on-few combat engagements. Specifically:

- Interactive: JAAM v6.x supports one-on-one and few-on-few engagement conditions with detailed aircraft and

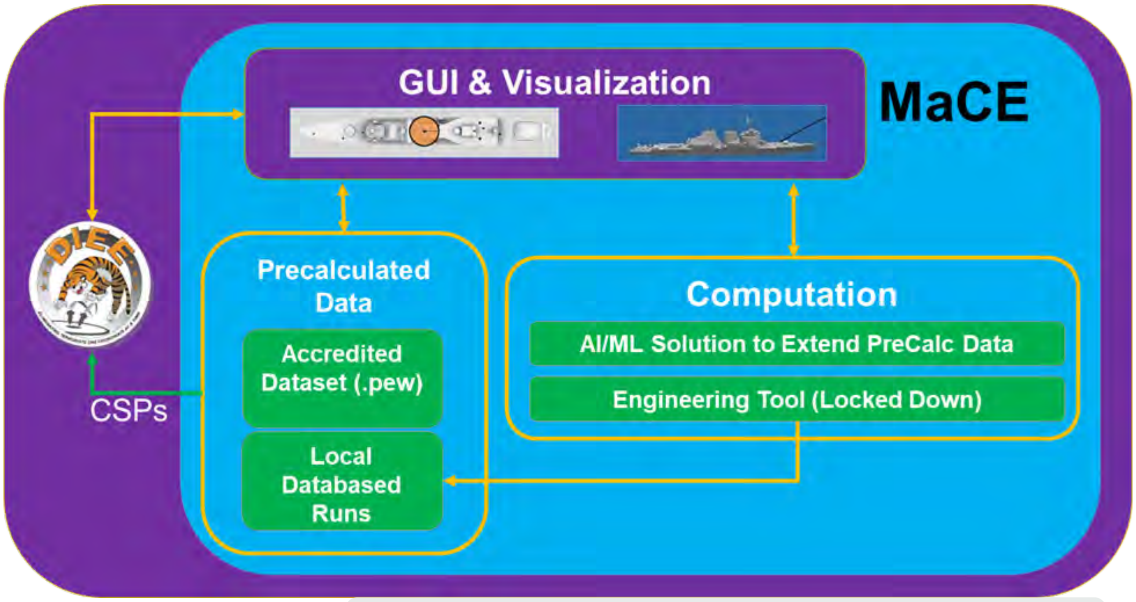


Figure 7. MaCE operational weaponeering tool workflow

weapons metrics and displays. JAAM displays show aircraft and weapon flight paths and key tactical events, such as detection, weapon launch, weapon active, and target killed.

- Virtual Range: JAAM v6.x supports event playback data from Air Ranges (Time-Space-Position Information, aircraft cartridge data, and GPS cartridge data) and injection of weapon shots against targets and evaluation of engagements.
- Iterative Study: JAAM v6.x multi-processors computing to enable multiple aircraft and weapons with hundreds of thousands of parametric engagement conditions. Results are exportable for big data analysis.

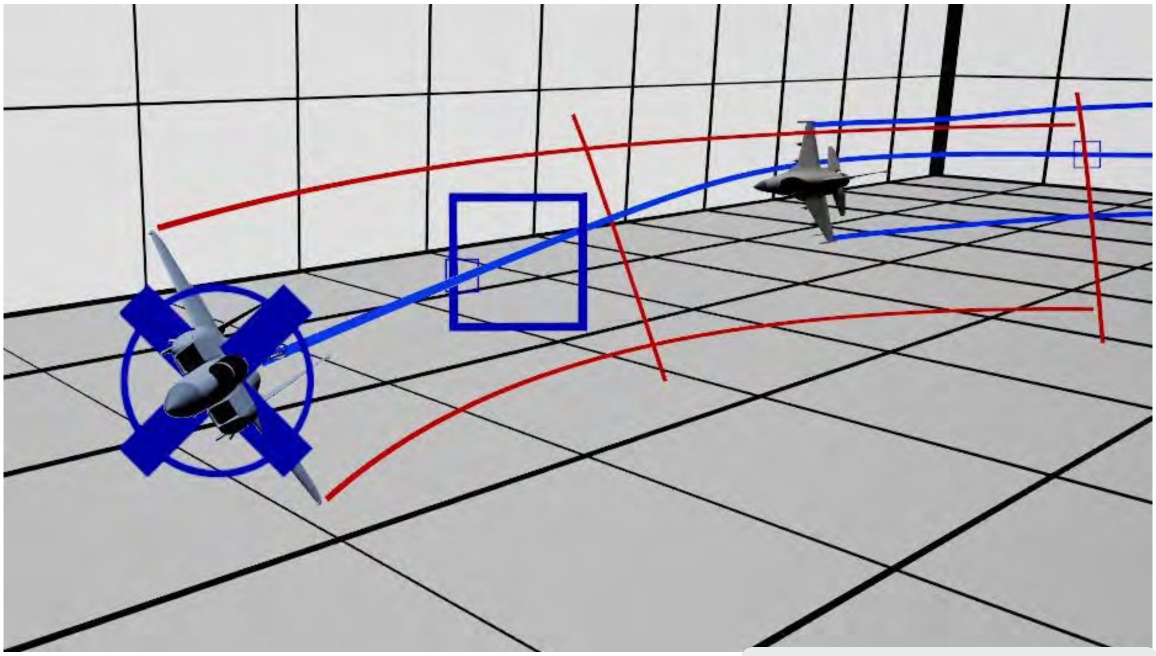


Figure 8. JAAM Interactive GUI

The JAAM v6.x external API is used across the Air Force and Navy Test and Training Ranges which enables authoritative and consistent results within mission playback and debriefing applications. JAAM API is used by:

- Personal Computer Debriefing Systems
- Tactical Combat Training Systems
- Joint Debriefing Subsystems
- Individual Combat Aircrew Display Systems
- Live Mission Operations Capabilities

The numerical engine, ACEL, which includes supplier's simulations and data, are a major component of JAAM v6.x. ACEL is co-developed with the JTCG/ME and the Joint Aircraft Survivability Program (JASP) Office, as discussed in the JASP section of this Annual Report ("SLATE and ACEL Architecture"). The Integrated Product Team manages the collection of simulations and data from multiple suppliers. The suppliers' simulations and data are interfaced into ACEL and ACEL API have evolved to meet JAAM v5.4 capabilities and the initial set of JAAM v6.0 requirements for Medium/High and Low Altitude Multi-Domain two (2)-Sided Air Combat Analysis capabilities (Figure 9). FY24 activities included:

- Signature datasets
- Aircraft and rotary wing datasets
- Weapon lethality and target vulnerability simulations and datasets
- Air-to-Air missile simulations
- Land Surface-to-Air missile simulations
- Early warning and acquisition simulations

JAAM v6.x and ACEL are well suited for addressing the operational needs supporting multi-domain air combat capabilities at an operationally significant pace.

Data Management

To support the implementation of the DoD Data Management Strategy in FY24, JTCG/ME expanded the repositories for archival, review, approval, and access of lethality and vulnerability data, methodology, and documentation. The four following repositories serve multiple user communities with corresponding features and capabilities:

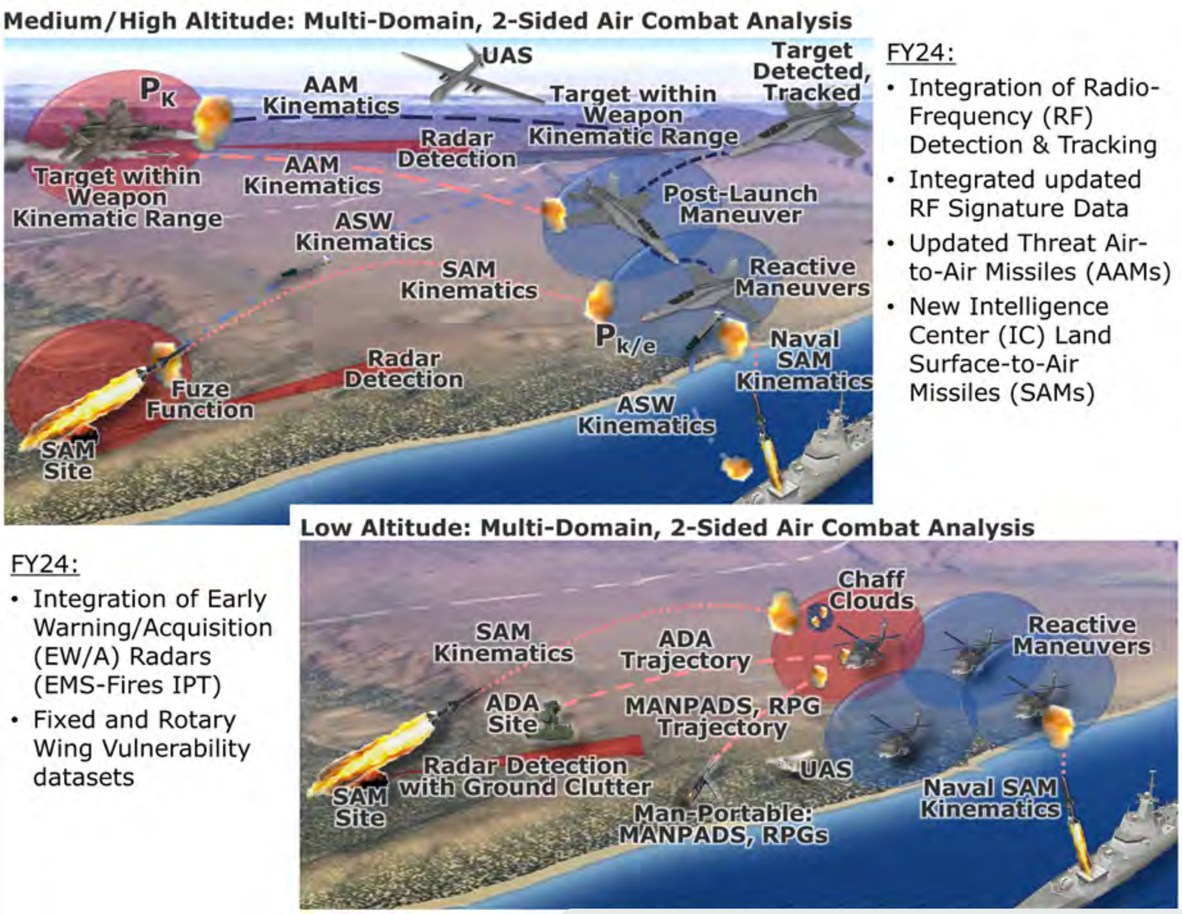


Figure 9. JAAM Operational View 1 (OV-1)

- For data, the Joint Analysis Repository and Visual Interface System (JARVIS) is a web-accessible repository with the authoritative data to support JTCG/ME's portfolio of warfighter applications. A critical requirement is to facilitate the data development and joint-Service review and approval processes. This repository also serves the T&E and acquisition community by providing JTCG/ME approved target vulnerability packages. In FY24, JTCG/ME deployed several updated versions of JARVIS that provided significant enhancements including data management capabilities for weapon characteristics and pre-generated weaponeering results.
- For methodology standards and practices, JTCG/ME created the Joint Effects Library, as the official repository for all implemented methodology and supporting functions that are approved by JTCG/ME and used in weapon effects applications. Not only does it serve as an archive for all JTCG/ME approved modules, but it also enables the incorporation of standard acceptance workflow and supporting material. The intent is to improve quality, increase reusability and reliability, and reduce time to integrate modules into weaponeering applications. In FY24, JTCG/ME incorporated several additional modules into the Joint Effects Library to support penetration effects, cratering, material targets, and blast effects.
- For documentation, the Bugle is a wiki-style website built on Defense Technical Information Center's DoDTechipedia platform. Hosting on DoDTechipedia makes JTCG/ME's technical reports, data requests, and model documentation accessible to the DoD community. In FY24, additional content was added to share information and collaborate on JTCG/ME products, models, and methodologies. In addition, JTCG/ME improved the site navigation and the overall user experience.
- JLF created a Service Specific Repository which serves as a target vulnerability database for the acquisition community. Analysts can use the repository to store, manage, and share target vulnerability data throughout the acquisition

community. This service also has the capability to send target vulnerability data directly to JTCG/ME for use on warfighter tools. The product was deployed in September 2024 and is being used by Army, Navy, and Air Force analytic agencies.

These four repositories work in conjunction to provide joint-Service approved munition effectiveness data, methodology, and documentation within JTCG/ME, JLF, and throughout the DoD.

» ENABLING MULTI-DOMAIN SUPERIORITY WITH DEW, CYBER, INFLUENCE OPERATIONS, AND EMS FIRE WEAPONEERING TOOLS

In FY24, JTCG/ME has made significant progress in multi-domain analysis capabilities and worked in partnership with the Services, Department of Energy's National Laboratories (e.g., Sandia, Lawrence Livermore, Idaho), academia (e.g., Georgia Tech, Johns Hopkins Applied Physics Laboratory), and DOT&E field activities (e.g., Center for Countermeasures, JASP, T&E Threat Resource Activity). JTCG/ME continued support to the warfighter with weaponeering tools intended to integrate kinetic and non-kinetic fires for optimized mission and lethal effects, while mitigating collateral effects to noncombatants, infrastructure, facilities, and equipment. While JTCG/ME has focused on the development and fielding of separate weaponeering tools that can account for DEW, cyber-attacks, and EMS fires, it has also initiated the plans to provide an architecture for a single JWS capable of estimating the appropriate number and type of either kinetic or non-kinetic weapons, and their combined effects, required to achieve superiority in a multi-domain operational environment.

DEW

In FY24, JTCG/ME continued to develop and validate DEW weaponeering tools – Joint Laser Weaponeering Software (JLaWS) and Joint High-Power Microwave (HPM) Applied Weaponeering Knowledge Software (JHAWKS)– to enable the CCMDs to estimate lethal effects using high energy lasers (HEL) and HPMs.

JLaWS

JLaWS uses target vulnerability data, weather effects, and optical risk characteristics to output associated vulnerability result and time to effect for solid state laser weapon systems. JLaWS considers the effect of weather on laser propagation by automatically downloading weather files from established services to account for location dependent weather conditions. JLaWS allows the user to calculate optical risk in the event of HEL reflections from targets using the High Energy Laser Risk Assessment Tool (HELRAT). HELRAT graphically portrays the risk distances around a target that contains reflected laser radiation levels that could cause ocular hazards to friendly forces in the area. Figure 10 shows a JLaWS graphical rendering of a ship-based Laser Weapon System engagement with an unmanned aerial vehicle target

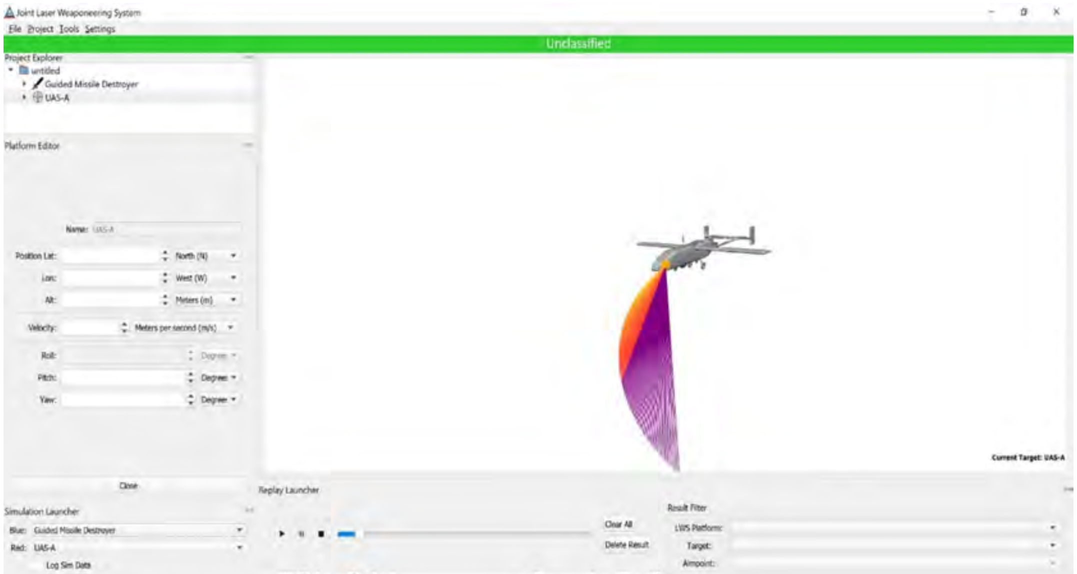


Figure 10. JLaWS Vulnerability Explorer and examples of shot lines

and the spherical zones around the target, as calculated by HELRAT, in which ocular hazards exist.

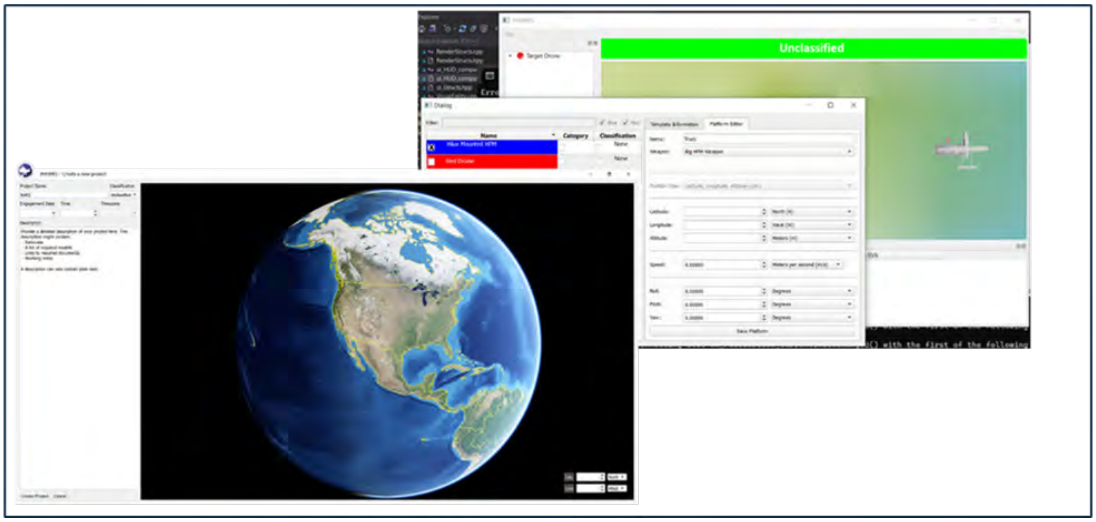


Figure 11. JHAWKS Initialization and Platform Editor

JTCG/ME placed a heavy emphasis on validating and verifying both the underpinning methodology and data that supports JLaWS. A tri-Service Methodology Review Committee made significant strides toward completing accreditation of JLaWS v2.4. The JARVIS repository was updated to include the ability to review and approve HEL target vulnerability packages; as a result, several packages are undergoing joint review. Moreover, multiple LWS characterization packages are nearing tri-Service review completion. The result of these efforts will ensure JLaWS provides the warfighter with a credible means to support weaponeering and CDE for HEL weapon systems.

Further development and validation of the surrogation tool allows for subject matter experts to generate efficient, reliable, and tractable HEL surrogate vulnerability packages from an existing database of completed assessments. Since a full vulnerability assessment is a time-consuming process, quick turnaround HEL analyses and studies can now be performed using the Characteristic-based Laser Objective Surrogate Evaluation tool.

JHAWKS

To advance the development and fielding of HPM weapon systems, JTCG/ME, and JLF partnered to conduct live fire testing, which generated lethality data to verify and validate dynamic engineering-level modeling for effectiveness of HPM weapons against small unmanned aircraft system swarm targets. Moreover, several lethality tests against Service-specific targets were conducted to identify and fill data gaps. Historically, HPM weapon systems testing has focused on effects based on 'back door' attacks where the signal couples to electronic components by entering seams or gaps. Vulnerability tests were conducted to assess damage from a 'front door' attack where the signal can couple into targets via intentional ports such as antennas. These tests aided in the development of new vulnerability methodology for front door target elements.

JTCG/ME made significant progress toward M&S tool development and defining processes that will enable JHAWKS use by the warfighter. A JHAWKS beta version included a GUI for ease of engagement setup (shown in Figure 11) and power-on target determination for free-space wave propagation scenarios. Enhancements were made to the Effectiveness Tool Box, an engineering-level M&S tool, that fills capability gaps for accurately modeling HPM dynamic engagements with multipath considerations. Atmospheric and terrain effects were incorporated into the Effectiveness Tool Box and a major overhaul to the graphics allow for the analyst to visually interpret the complexities of HPM wave propagation (shown in Figure 12). Credible engineering-level M&S outputs are required to provide inputs to JHAWKS. Multiple foundational efforts included generation of a JHAWKS Software Requirements Document, as well as an Interface Control Document, to define the structure and format of the engineering-level M&S tool outputs, thereby ensuring successful future JHAWKS development.

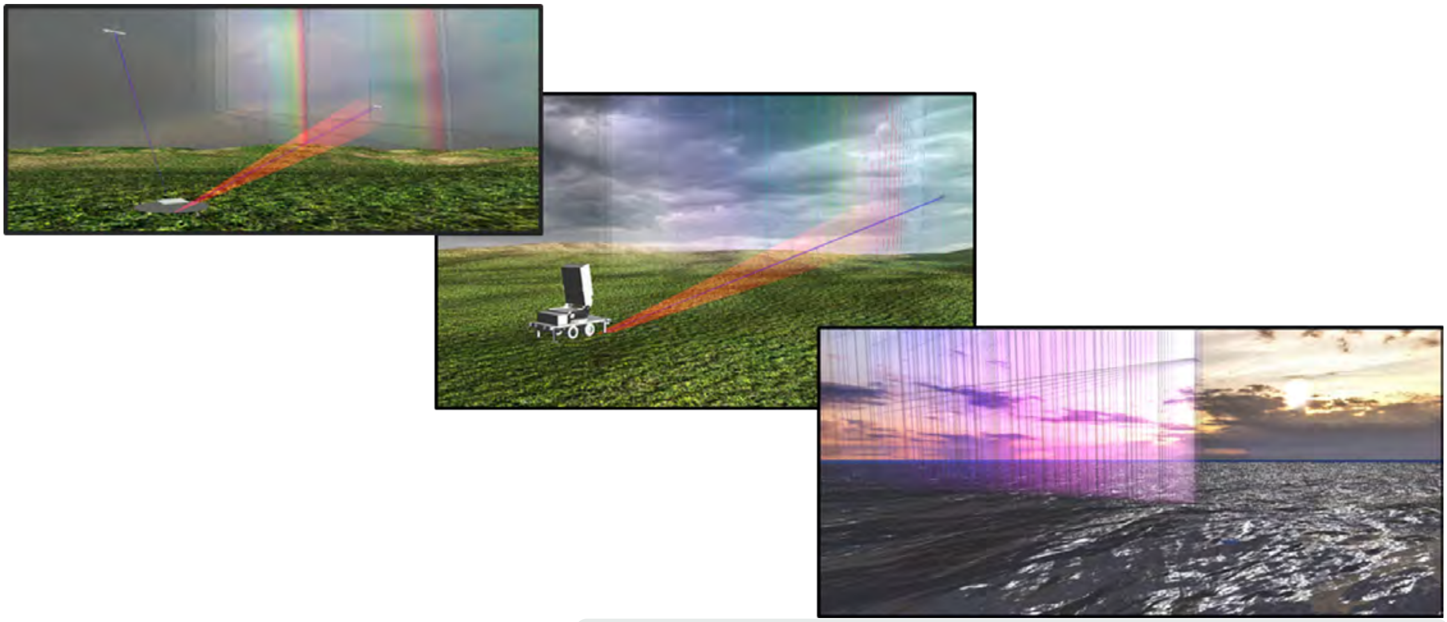


Figure 12. HPM Propagation for Land and Maritime Environments

Cyber Operations Lethality and Effectiveness (COLE)

In FY24, JTCG/ME's Joint Non-Kinetic Effectiveness team continued the development and fielding of cyber JMEM capabilities for the warfighter. The COLE tool is the foundational product, enabling commanders and decision makers at all echelons to generate accredited, quantitative, and predictive effects of cyber operations for combined joint all-domain operations. The COLE software provides the user with a cyber operations planning and analysis capability for; offensive cyber operations, test and evaluation of operational systems, and risk assessments of cyber resilient systems.

JTCG/ME deployed v3.4 of the COLE tool on both classified and unclassified networks, enabling planning elements to model cyber networks, characterize properties, and determine potential network vulnerabilities to cyber capabilities and TTP in various combinations for cyber operations and cyber capability requirement development.

Major FY24 COLE improvements include new automated data ingestion capabilities to accelerate and simplify network characterization and an attack-path optimizer that automatically generates possible courses of action, increasing the thoroughness of options and speeding analytical efforts via automatic generation and tracking of options. A new simultaneous actions capability has also been deployed, enabling planners to consider actions against multiple nodes from a single source. COLE's new functional modeling application allows users to see impacts of cyber operations on cyber-reliant functions. Finally, for COLE users focused on T&E or defensive cyber operations, the COLE team has developed a beta capability to assess risks to a network based on potential adversary courses of action. In addition to cloud-based deployments, in FY24 JTCG/ME initiated deployment of stand-alone COLE instances (known as 'COLE-in-a-Box') to support users who conduct cyber M&S and planning on closed or advanced program networks.

JTCG/ME continues to team with the JASP on the Machine Assisted Exploitability Simulation and Testing for Resilient Operations effort to further develop COLE's ability to assess cyber vulnerabilities of U.S. platforms. COLE for T&E provides a framework of models and tools to aid in examining aircraft cybersecurity.

JLF continues to develop Enhanced Vulnerability Discovery abilities to assist in rapidly and automatically characterizing, discovering, and reporting cyber vulnerabilities within complex software configurations through the Cyber Automated Threat Discovery and Vulnerability Evaluation Reinforcement (CADAVER) program. CADAVER is intended to leverage AI/ML to allow identification of potential vulnerabilities to mitigate cyber-attack access points through automated and semi-automated means. Combined, COLE and CADAVER ensure warfighters have the necessary tools to assess cyber effectiveness/vulnerability using tri-Service-approved data standards and streams.

In FY24, JTCG/ME continued to team with the DoD Test Resource Management Center to create cyberspace effects and enabling Capabilities Cyberspace Live-Fire Evaluation Framework (CLEF) to provide a realistic test environment for cyber capabilities generating accredited performance data. Four CLEF servers have been installed at the 346th Test Squadron at Joint Base-San Antonio, Texas, with initial operating capability expected in September 2024. The CLEF effort will set the standards for rapidly generating and analyzing cyber performance, analogous to kinetic area testing capabilities and standards for fragmentation.

Influence Operations

In FY24, JTCG/ME Joint Non-Kinetic Effectiveness continued its pathfinder effort to develop and influence operations JMEMs, aimed at assessing how an adversary may respond to proposed military courses of action. Behavioral influences analysis can help inform how the U.S. applies military force or other instruments of power and identify what specific adversary elements to attack. Sandia National Laboratories has been developing the Dynamic Multi-Scale Assessment Tool for Integrated Cognitive-behavioral Actions (DYMATICA) tool to assess how various populations and groups perceive U.S. actions. Focusing primarily on aggregating and assessing unclassified, publicly available journals, news media, social media sources and academic papers, DYMATICA leverages AI-engines and subject matter expertise-informed ML models to forecast adversary responses to U.S. or coalition actions across all phases of operations to help influence the decisions of adversary leadership.

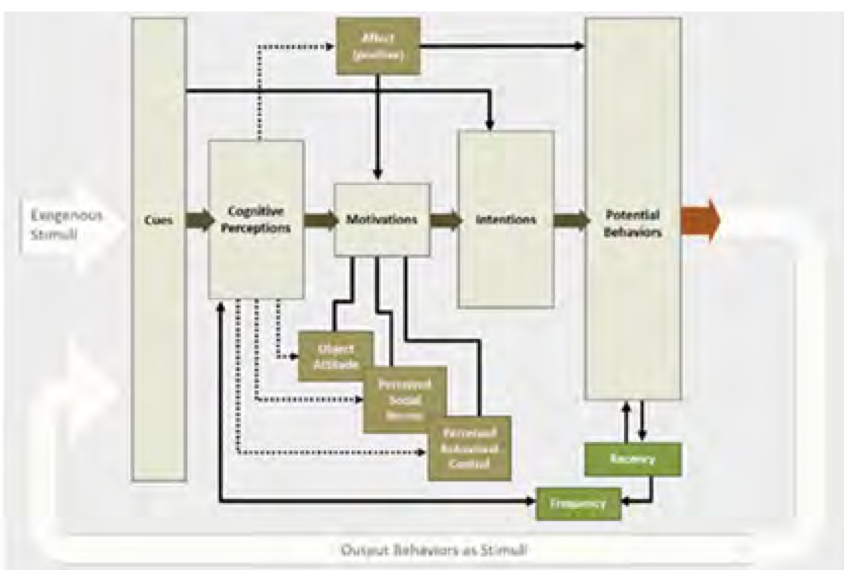


Figure 13. DYMATICA Workflow

EMS Fires

In FY24, JTCG/ME developed an initial set of JMEM capabilities to enable notional mission planning and execution in contested, congested, and constrained EMS environments. Moreover, preliminary modeling of systems across the Services was completed. These tools will estimate electronic attack (EA) effects and the ability of the warfighter to effectively prosecute adversary targets in contested, congested, and constrained EMS operations (shown in Figure 14).

JMEM for EMS fires will allow mission planners and targeteers to assess weapon and combat effectiveness in the presence of adversary EA (e.g., 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), which creates a foundation of joint standard EA effectiveness data and models used across the Joint Targeting Cycle. The objective by 4QFY25 is to expand modeling within an advanced framework that will dynamically depict high fidelity EA interactions to inform future Joint EA Predictive (JEAP) tool development and integration efforts.

JTCG/ME and JLF partnered to execute a full live fire drop of 6 GPS-guided weapons in a heavily denied environment. Testing

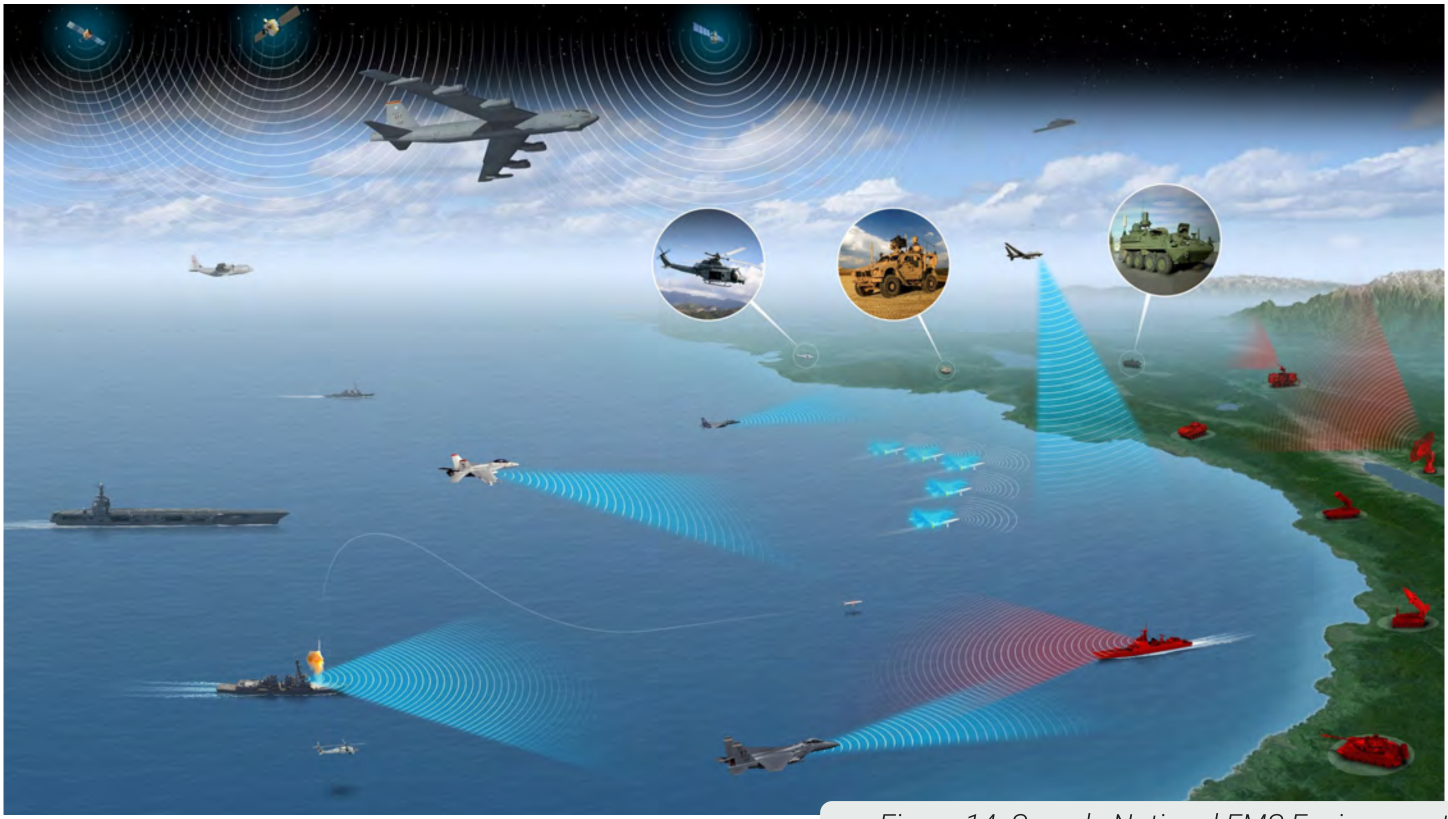


Figure 14. Sample Notional EMS Environment

was conducted in September 2024, leveraging the existing U.S. Army Position, Navigation, and Timing Assessment Experiment. The resulting data will inform current GPS guidance capabilities and improve M&S for predicting GPS guidance performance.

» SUPPLYING WEAPONEERING TOOLS TO SUPPORT INTEROPERABILITY WITH U.S. ALLIES AND PARTNERS

In FY24, JTCG/ME provided weaponeering tools and data sets in support of training to 10 partner countries under Foreign Military Sales agreements. This included the release of weapon effectiveness tables, collateral effects radii tables, and advanced target development capabilities that will help 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 with partners on methodologies and efforts of mutual interest in weapons effectiveness and CDE for both kinetic and non-kinetic weapons. In FY24, JTCG/ME continues to prepare multiple information exchange annexes, to provide weapons effectiveness analytical exchanges and to expand the scope of topics to better represent complex strategic and operational environments.

Joint Test and Evaluation (JT&E)

In FY24, the Joint Test and Evaluation (JT&E) Program advanced a commitment to modernization and innovation to bolster its ongoing support to the joint urgent operational needs (JUONs) of the warfighter. This support included establishing an integration lab to support development of enhanced deliverables and introducing a modern and responsive test process known as an agile reaction test (ART). The JT&E Program managed two joint tests and nine quick reaction tests (QRTs) in addition to starting four ARTs to develop critical solutions to warfighter-identified challenges. FY24 activities enabled National Defense Strategy priorities through the development of concepts of employment (CONEMPs), concepts of operations (CONOPS), and tactics, techniques, and procedures (TTP).

PROGRAM OVERVIEW

The JT&E Program was established in 1972 in response to the 1970 Blue Ribbon Defense Panel Report recommending that responsibility for JUON testing be vested in an OSD staff element. In 2002, management and responsibility for the JT&E Program transferred to DOT&E from the then Under Secretary of Defense for Acquisition, Technology, and Logistics. Today, the JT&E Program considers emerging technologies and the increasingly complex and dynamic, joint, multi-domain operational environment to plan and execute test projects intended to deliver joint warfighter solutions and enhance the lethality, suitability, resilience, survivability, agility, and responsiveness of the joint force.

The Services and combatant commands (CCMDs) 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 OT&E management and expertise to develop, test, and validate joint doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTmLPF-P) solutions, including agile warfighting CONEMPs, CONOPS, and TTP. In turn, the 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 tested within each of the individual Services and CCMDs. Given the increased integration and dependencies of platform, network, and command and control (C2) 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. JT&E's extensive use of OT&E testing techniques, workforce talents, and reach-back are essential to the adequate evaluation of the effectiveness of proposed solutions needed in operational plans across the CCMDs.

The JT&E Program Office (JPO) launched the Integration Lab in March 2024. Its mission is to integrate a modernization framework into JPO programmatic activities to include leveraging digital transformation, digital engineering, artificial intelligence (AI) systems, and other data-driven modeling approaches. JPO's subject matter expertise is provided to enhance the technical excellence of T&E outcomes.

The Integration Lab is focused on leading T&E for the development and application of these digital transformation technologies as trustworthy solutions to the warfighter. This involves a multi-phased approach for establishing trust to include:

- Validation of training data for AI and digital twin systems.
- Verification of AI model selection, architecture, and overall system design.
- Uncertainty quantification of data driven systems.
- Systems security of cyber-physical systems.
- Interpretability and explainability of machine learning-based AI outcomes.

While supporting test projects that involve data-driven methodologies, including AI, the Integration Lab is also evaluating methods to enhance the transition of test products. As of April 2024, the Integration Lab has undertaken an effort to develop a digital twin workflow to digitally engineer project CONOPS. The goal of this initiative is to incorporate validated workflows through a digital multi-domain environment to visualize operational mission threads. This framework will have the potential to expedite the JPO product transition and reduce redundancies across CONEMPs, CONOPS, and TTP by allowing the warfighter to have a streamlined method to test and monitor executional courses of action.

In the second half of FY24, the JPO introduced a newly defined and seamless joint testing integration strategy, known as the ART process, to evolve its business model. This innovation resulted from an internal review to develop a reinvigorated JT&E process built upon the credibility of OT&E methodology with expedited results to solve the modern warfighter's JUONs. During the review, the JPO considered its joint testing procedures, processes, resources, costs, deliverables, timelines, and mission partner support along with lessons learned, stakeholder recommendations, and support of the National Defense Strategy. The resulting ART process stands as the successor of the legacy JT&E processes with cessation of joint tests and QRTs occurring across FY25 and 1QFY26. ART projects test and evaluate CONEMPs, CONOPS, and TTP to provide critical solutions to specific warfighter-identified DOTmLPF-P challenges within one year. The JPO initiated the first round of ART projects in 4QFY24 with the charter of four ARTs set to begin testing in early FY25.

MISSION

The JT&E Program bolsters the warfighter capability by addressing JUON challenges through developing and testing proposed solutions using OT&E methodology synergized with warfighting concept objectives, military exercises, complex mission threads, and kill webs to meet the DoD's strategic objectives.

FY24 KEY ACTIVITIES

» AGILE REACTION TESTS

During FY24, the JT&E Program managed four ART projects addressing challenges identified by Civilian Protection Center of Excellence (CP CoE), U.S. Indo-Pacific Command (USINDOPACOM), North American Aerospace Defense Command (NORAD), and U.S. Northern Command.

Civilian Harm Assessment Cell Training and Operational Integration (CHAC TOI)

In a January 2022 memorandum, the SECDEF directed the development of an action plan to improve the Department's approach to civilian harm mitigation and response (CHMR). Subsequently, the Department established the CP CoE to lead the implementation of CHMR across the DoD enterprise and develop civilian harm assessment cell (CHAC) training certification standards. During FY24, the CP CoE began the process of developing a CHAC training curriculum for operational certification, assessment, and mission integration. This effort included coordination and collaboration with the JT&E Program and key stakeholders from the CCMDs, Office of the Under Secretary of Defense for Policy, Office of the Under Secretary of Defense for Intelligence and Security, Defense Intelligence Agency, and National Geospatial-Intelligence Agency.

To further this SECDEF initiative, the JT&E Program formally chartered CHAC TOI as a JPO-Direct ART in September 2024. The objective is to develop CHMR TTP and an agnostic operational support handbook that enables CHAC operators to assess civilian harm on the modern-day battlefield, support command- or agency-directed investigations into civilian harm, and support civilian harm mitigation efforts. Ultimately, the CP COE plans to leverage this JPO-Direct ART to develop a portal to house all CHMR TTP and training curriculum as well as track CHAC certifications through a fully developed training and certification program by the end of FY25.

Developing Effective CONOPS for Integration of Fires and Effects at RESOLUTE HUNTER (DECIFER)

Operational and tactical commands require the ability to integrate and coordinate employment of organic and inorganic sensors in support of end-to-end kill webs and chains. To address this requirement, the Naval Aviation Warfighting Development Center created the Maritime Intelligence Surveillance and Reconnaissance (MISR) Weapons School to train individuals in all-domain sensor integration necessary to develop accurate target packages and plan, manage, and lead effective kill web execution in the joint environment.

Recent successes of MISR trained personnel have led to a sharp increase in MISR demand across geographic CCMDs. Exercise RESOLUTE HUNTER is a capstone event for the MISR Weapons School program focused on positioning all-domain fires through integration of fires, sensor integration, and battle management/C2 functions. RESOLUTE HUNTER provides a training and innovation environment of sensors from seabed to space to improve interoperability between U.S., joint, and coalition platforms. This environment also facilitates improving how battle management/C2 is delivered to the tactical edge and how information is fused to support timely, well-informed decision-making in large scale combat operations.

The JT&E Program chartered the DECIFER ART in August 2024 to develop, test, and evaluate TTP that standardizes an approach to integrating resilient, all-domain kill webs to maximize the effectiveness of joint fires in the maritime theater of operations. Participating in two RESOLUTE HUNTER events, the DECIFER ART will codify and accelerate use of TTP in all-domain, human- and machine-teamed, end-to-end kill web development. The TTP will improve warfighter confidence in intelligence and promote targeting that is actionable and timely with a low risk of civilian casualties.

Generative Artificial Intelligence Models Integration (GAIMI)

With AI technologies becoming more pervasive in everyday tasks, generative artificial intelligence (GAI) tools, such as large language models (LLMs), have the potential to help staffs become more efficient and effective. LLMs give users unprecedented access to data and the ability to create new content. GAI capabilities and tools have the potential to assist in the development of joint activities and supporting documents. DoD requires formal TTP development for application, governance, and control of GAI to leverage the benefits and mitigate the risks of this new technology.

In August 2024, the JT&E Program chartered the GAIMI ART for NORAD and U.S. Northern Command to develop and test a set of TTP to help capture the use, maintenance, and utility of GAI LLMs. The objective is to leverage GAI to assist staffs with becoming more effective in joint operations by properly prompting GAI to produce products while minimizing risks of hallucinations. The TTP will aid users in preparing a current repository, framing a prompt and grading output to inform the commander's estimate, and developing course of action products created by GAI for operational and planning purposes with the intent of ensuring confidence and reducing risk in the generated information. The GAIMI team plans to conduct two field test events in FY25 to support development and refinement of the TTP.

Joint Sustainment Network (JSN)

CCMDs must plan and manage logistics requirements and capabilities through all phases of operations to support warfighter missions and needs, understand the impact of logistics requirements on operational decisions, and leverage opportunities and resources that can mitigate risks. USINDOPACOM J4 requires a JSN that provides a capability to see, understand, direct, and synchronize theater sustainment operations. The JSN must be dynamic and adaptive to operations plan and operations order development; Service concepts and investments; changing theater infrastructure; shifting permissions for access, basing, and overflight; and evolving defense industrial base capabilities as well as cover a range of environments from competition to conflict in a contested logistics environment. Logistics planners are simply not equipped to manually comprehend and analyze complex logistics challenges in a timely manner, often resulting in oversimplified or late-to-need decisions that are ineffective and not aligned to budgeting cycles.

The JSN ART was initially chartered as the Digital Theater Logistics Plan Joint Feasibility Study in February 2024 to develop a Digital Theater Logistic Plan proof of concept comprised of business rules, data architectures, and data analytics needed to plan, manage, and execute theater logistics operations. With a refocus to meet USINDOPACOM priorities, the JT&E Program chartered the JSN ART in August 2024 to aid in the development of a JSN business intelligence software tool that will enable sustainment decision processes. The JSN ART will support developing, testing, and evaluating TTP that will define JSN requirements and capabilities with procedures, data architecture, and decision processes that specify sustainment requirements, logistics capabilities, and data visualization dashboards. The JSN ART is a one-year project that will develop, test, and evaluate JSN products through several test activities leveraging a CCMD exercise as the culminating event.

» JOINT TESTS

During FY24, the JT&E Program continued two joint tests addressing challenges identified by USINDOPACOM, U.S. Southern Command, and U.S. Strategic Command (USSTRATCOM).

Joint CONUS Directed Over-the-Horizon Radar (J-CONDOR)

Joint forces face challenges in maintaining freedom of maneuver in complex multi-domain anti-access/area denial environments. Adversary and friendly forces have fielded variations of over-the-horizon radar (OTHR) that can detect air and surface targets at long ranges. The OTHR operates by transmitting high frequency radio waves that are reflected off the ionosphere into a surveillance area that can provide target cueing for adversary long-range systems. The JT&E Program chartered the J-CONDOR Joint Test to develop an overarching CONOPS that informs combatant commanders of adversary OTHR capabilities and mitigation strategies. The J-CONDOR CONOPS will include TTP for tactical commanders that synergizes maneuver with electronic systems and capabilities to counter detection and tracking by adversary OTHR. The J-CONDOR Joint Test includes several test events throughout the two-year project utilizing air, maritime, and electromagnetic warfare resources to evaluate the J-CONDOR CONOPS and TTP.

From May to July 2024, J-CONDOR conducted a counter-OTHR field test with maritime surface and air assets and first-of-its-kind electronic warfare (EW) system integrations across multiple test events. The highly successful field test saw participation from multiple commands and activities including U.S. Naval Forces Southern Command, USS *George Washington* Task Group, Center for Naval Analyses, Naval Surface Warfare Center Carderock Division, Battlespace Awareness and Information Operations (PMW 120), and Fleet Surveillance Support Center. The test provided data on the effectiveness of proposed TTP building blocks and effects of EW systems of interest. The analysis of this data will inform CONOPS development and coincidental insights into tactical and operational mission design with regards to counter OTHR in anti-access/area denial environments. An interim CONOPS and TTP will be provided to the warfighter for immediate mission improvements as well as set the stage for a second field test in FY25 with additional EW capabilities.

Joint Conventional Nuclear Integration (J-CNI)

Conventional and nuclear integration is the seamless planning and operation of joint and combined conventional and nuclear forces, in sequence and in parallel, across the competition continuum from force design to planning and execution up to and through a nuclear environment. The scope of planning and execution of such operations encompasses more than conventional support to nuclear operations and requires the complete integration of non-nuclear capabilities to enhance or complement nuclear employment options. The JT&E Program chartered the USSTRATCOM-sponsored J-CNI Joint Test to develop, test, and evaluate a CONOPS for defining integrated conventional and nuclear options that are executable within a pre-synchronized timeline and effectively assign these missions to the responsible organizations.

During FY24, the J-CNI Joint Test team performed research into existing doctrine and planning guidance, conducted a joint warfighter advisory group (JWAG), and executed a risk reduction event in support of GLOBAL LIGHTNING 24 and AUSTERE CHALLENGE 24. These efforts shaped a first draft of the Conventional and Nuclear Integration CONOPS, which received a review by the JWAG in addition to an O-6 level CCMD review. Their warfighter comments are informing the next iteration of the CONOPS before field testing in FY25. The CONOPS will be tested under operational conditions through USSTRATCOM collaboration with U.S. European Command and USINDOPACOM during tier 1 exercises. The J-CNI team will use the results of the field tests to finalize the CONOPS before transition to the Joint Staff for integration throughout DoD. The J-CNI Joint Test will conclude in 1QFY26.

» QUICK REACTION TESTS

During FY24, the JT&E Program managed nine QRT projects addressing challenges identified by U.S. Army, U.S. Air Force, Joint Staff J6, U.S. Coast Guard (USCG), U.S. Space Command, USSTRATCOM, and Missile Defense Agency.

Automated Tactical Targeting and Counterfire Kill-Web System (ATTACKS)

During large-scale combat operations, tactical operators within the U.S. Forces Korea Counterfire Task Force Air Component Command must employ and disseminate counterfire against North Korea's long-range artillery threats efficiently, at scale, and within their vulnerability window. The Tactical Air Control Party and Tactical Command and Control systems have integrated ATTACKS software into current C2 systems with emerging Combined Joint All-Domain C2 platforms including Advanced Battle Management System, Project Convergence, and Project Overmatch. ATTACKS uses joint sensors and the existing Combined Joint All-Domain C2 software to automate data transfer between disparate counterfire systems using machine learning. By automating disparate data links, U.S. forces in South Korea can reduce the total time required to neutralize the long-range artillery threat from minutes to seconds, preventing potential catastrophic loss of life in the Greater Seoul Metropolitan Area. The JT&E Program chartered the ATTACKS QRT to develop and validate TTP to optimize the automation provided by ATTACKS to support the Counterfire Task Force mission.

In June 2024, the QRT conducted the first field test at the 422nd Test and Evaluation Squadron, Nellis AFB, Nevada, to test the initial draft TTP. For the second field test in South Korea, the 607th Air Operations Center, 51st Fighter Wing, 607th Air Support Operations Group, and 621st Air Control Squadron executed with their mobile tactical operations center proving agile combat employment during the exercise. During both events, testing focused on the use of multi-domain counterfire teams, airborne fighter/reconnaissance aircraft, and surface counterfire platforms with the Advanced Field Artillery Tactical Data System. The ATTACKS TTP are Service agnostic and transferrable to other fires platforms and counterfire operations, thus increasing the overall lethality, survivability, and effectiveness of fires in kinetic operations. The TTP transitioned to Seventh Air Force and Eighth United States Army upon completion of the ATTACKS QRT in October 2024. Ultimately, the test showed that commercial off-the-shelf technology can be applied immediately to the battlespace and within established wartime special instructions and operational plans.

Civil Data Link Cyber Awareness and Resiliency (CvDL CAR)

The Aircraft Communication Addressing and Reporting System (ACARS) was developed to enhance the Air Operations Center communications between airline control centers and aircraft. The ACARS network includes a variety of media options to ensure successful air and/or ground data link communications. Civil data link is also used DoD-wide for interoperability with global air traffic safety and control services. U.S. Transportation Command (USTRANSCOM) uses this link as a C2 method for Mobility Air Forces and Civil Reserve Air Fleet aircraft conducting missions globally. Most transport, refueling, and distinguished visitor aircraft are fully equipped with civil data link and use it regularly to gain access to preferred civil airspace routing and for C2 with the USTRANSCOM Air Operations Center. Aircrew and operations centers who rely on aviation civil data links to exchange relevant flight and mission information need the ability to detect, respond, and recover from cyber issues that affect data confidentiality, integrity, and availability.

In September 2023, the JT&E Program chartered the CvDL CAR QRT to develop, test, and validate TTP to address the ability of aircrew and flight managers to detect cyber issues with ACARS data messaging, respond to cyber interference or issues in ACARS message sets, and recover from cyber interference via mitigations to ensure mission assurance. The CvDL CAR test team planned two field test events to observe and collect data to test and validate the TTP. The QRT focused on systems using ACARS such as tanker, transport, and distinguished visitor airlift (C-5, C-17, C-40, C-130, KC-46, KC-135); Air Force and Navy platforms; and operations center C2 nodes. In 3QFY24, the team collected baseline data during Field Test (FT)-1A at Travis AFB, California, and Scott AFB, Illinois, followed by FT-1B conducted in conjunction with exercise VALIANT SHIELD 2024 to leverage Air Mobility Command missions at Scott AFB. FT-2 is planned for October 2024 to continue capturing useful data that test and validate the TTP prior to its transition to Air Mobility Command, USTRANSCOM, and other U.S. Government agencies that depend on ACARS and civil data link. The CvDL CAR QRT is expected to conclude in 2QFY25.

CONOPS for Novel Information Warfare Capabilities (CNIWC)

USSTRATCOM and overall DoD mission success relies on the ability to optimize information warfare capability. The JT&E Program chartered the CNIWC QRT to develop and test a Joint Information Warfare CONOPS to be executed by USSTRATCOM. During 2QFY24, CNIWC conducted a risk reduction event and field test, which supported development, testing, and validation of a stand-alone CONOPS. The QRT concluded in August 2024 and transitioned the CONOPS to USSTRATCOM who will coordinate changes to the joint and Service doctrine.

Joint Aviation Signature Management Analysis, Application and Rehearsals Tool (JA-SMAART)

The U.S. Army Aviation Center of Excellence requires a standardized and repeatable test methodology to evaluate electromagnetic signatures of slow flying, joint tactical aircraft. Anti-aircraft systems exploit specific, and sometimes multiple, electromagnetic spectrum (EMS) signatures to detect, track, and engage their targets. The JT&E Program chartered the JA-SMAART QRT to develop TTP and a series of models to directly improve aircraft survivability in contested, congested, and constrained EMS operations. The objective of the project was to increase aviation combat survivability through a reduction in aircraft susceptibility in multi-domain operations.

In 1QFY24, the JA-SMAART team conducted the first field test with three rotary-wing aircraft to obtain EMS signature data on each airframe. This data was then integrated into the Air Force Improved-Many-on-Many model for mission planning. During the second field test in 3QFY24, Aviation Mission Survivability Officers used the models with a fielded fused mission planning tool to develop mission profiles that would mitigate risk to aircraft. This entire process was captured in the developed Joint Aviation EMS Data Collection and Fused Mission Planning Tool Integration TTP for Low-Level Joint Aircraft (EFI-TTP). In 4QFY24, JT&E completed the JA-SMAART QRT and transitioned the EFI-TTP to U.S. Army Aviation Center of Excellence for future use in the Joint Aviation Survivability Program.

Joint Contaminated Human Remains Storage and Temporary Interment/Disinterment (JCHR-STID)

Joint warfighters lack procedures to identify, store, account for, temporarily inter, and disinter joint contaminated human remains (CHR) for future repatriation to the United States following a chemical, biological, radiological, and nuclear mass fatality incident. The JT&E Program chartered the JCHR-STID QRT in September 2023 to address urgent warfighter requirements pertaining to the disposition and accountability of CHR. The objective is to provide warfighters with the proper procedures for temporary disposition and accountability of CHR that cannot be processed due to the high volume received during large-scale combat operations or in situations where the CHR cannot immediately be repatriated. To develop and test the TTP, the JCHR-STID QRT conducted a field test and preceding risk reduction event at Fort Gregg-Adams, Virginia, in 4QFY24. Headquarters, Department of the Army, G44S, Director of Supply Policy, United States Army G-4, as the QRT sponsor, will facilitate the transition of the JCHR-STID test product to users upon its completion in 2QFY25.

Joint-Global Hypersonic Operational Sensor Tasking (J-GHOST)

The joint warfighter required doctrine to deconflict, coordinate, and integrate attacks that include emerging technologies and newly fielded capabilities within emerging Space Domain Awareness, Missile Defense, and Missile Warning doctrine. The JT&E Program chartered the J-GHOST QRT to develop, test, and deliver refined Space Domain Awareness CONOPS and associated TTP to rapidly task external sensors, international sensors, and internal missile defense sensors in real-time during advanced trans-regional threat events. The goal was to operationally improve responsiveness for no-notice tasking of Missile Warning, Missile Defense, Space Domain Awareness, and other sensors to support detection and improve track custody and reporting of time-sensitive, multi-domain, trans-regional, advanced threats, and high-interest space events.

In March and May 2024, the J-GHOST team conducted field tests to support the Missile Defense Agency and U.S. Space Command in jointly delivering tested and validated CONOPS and TTP to enable warfighters to detect, track, and report on advanced threats. These field test events were coordinated with six CCMDs, the Services, and the Missile Defense Agency and relied on participation from the 18th Space Defense Squadron and National Defense Space Center. Upon test completion in July 2024, the J-GHOST QRT validated the existing CONOPS and delivered a new TTP, via a checklist, to the National Defense Space Center for immediate implementation.

Joint Interface Control Cell Resiliency (JICC-R)

Joint Interface Control Cell personnel require the capability to enable detection, response, and recovery from anomalous data on tactical data link networks through modernized TTP. The JT&E Program chartered the JICC-R QRT to develop and test new TTP to address this need recognized by Air Combat Command. In June and July 2024, the QRT team conducted two field tests at 612th Air Operations Center with eight teams of Joint Interface Control Cell personnel from Air Force, Army, and Navy units to verify the statistical significance of the TTP on operator performance. Supported by 46th Test and Evaluation Squadron, the JICC-R team established a baseline with operators who had not seen the new TTP and compared it to operators who had been trained on the new TTP using identical scenarios. Insights gained during the first field test informed refinement of the TTP prior to the second field test. Based on the results, the TTP proved to be very helpful for improving both speed and accuracy in dealing with anomalous data link conditions in ways that quickly recovered warfighter systems for mission use. Upon completion in October 2024, the QRT delivered the TTP to sponsor Air Combat Command/A3 and the Joint Interoperability Division of the Joint Chiefs of Staff for expected incorporation into Joint Interoperability Data Link Training Center curriculum.

Joint Operation NOBLE EAGLE Link-16 Tactical Data Link (JOLT)

Until recently, USCG Rotary Wing Air Intercept aircraft were not equipped with a tactical data link system and relied only on visual information and aural advisories from the Eastern and Western Air Defense Sectors. The Coast Guard Deputy Commandant for Operations, with advisory direction from NORAD, established a requirement that all USCG MH-65 aircraft participating in Rotary Wing Air Intercept missions have a tactical data link capability to enable real-time visual situational awareness among active air intercept participants. The JT&E Program chartered the JOLT QRT to develop and assess TTP for Rotary Wing Air Intercept missions flown in conjunction with Air Force aircraft and Army Ground Based Air Defenses controlled by the Eastern and Western Air Defense Sectors in the Continental NORAD Region.

The JOLT QRT team jointly developed the TTP with USCG and Joint Staff J6 using a test-fix-test approach during the project execution period from May 2023 to May 2024. The first field test (FT-A) occurred at USCG facilities in Atlantic City, New Jersey, in December 2023. The second field test (FT-B) took place at the National Capital Region Air Defense Facility in Washington, DC, in February 2024, replicating FT-A data collection and its battle rhythm with the addition of a night sortie. The QRT produced the Coast Guard TTP 3-90.8 Rotary Wing Air Intercept Dolphin Link 16 System TTP, which serves to enhance interoperability and USCG Rotary Wing Air Intercept mission execution in support of Operation NOBLE EAGLE. Supplemental test products include a job guide for cryptologic loading and management along with a maintenance procedure card for the installation and removal of the Battlefield Awareness and Targeting System-Dismounted Radio Mount. These test products transitioned to the USCG Aviation Training Center and USCG Aviation Logistics Center when the JOLT QRT concluded in May 2024.

Nuclear Command, Control, and Communications (NC3) Conditions Risk Assessment (NC3CON RA)

USSTRATCOM requires a holistic multi-domain focused risk assessment process with associated indications, warnings, and triggers to enable NC3CON decision-making. The goal is to provide an accurate and comprehensive risk picture of the NC3 Enterprise. In September 2023, the JT&E Program chartered the NC3CON RA QRT to develop and test a CONOPS that codifies a risk assessment process to provide NC3CON decision makers with consistent and reliable information to align high-demand, low-density resources to NC3 missions and systems at greatest risk. During FY24, the QRT team conducted several CONOPS technical exchange working groups, two JWAG CONOPS alignment meetings, and one tabletop exercise to test and evaluate the effectiveness, usability, and utility of the CONOPS in detailing a flexible and reliable risk assessment process in which senior leaders and decision makers can have a high degree of confidence. Upon completion in FY25, the project is expected to deliver a validated CONOPS that codifies the risk assessment process to enable appropriate and responsive NC3 Enterprise risk mitigation activities.

Test and Evaluation Threat Resource Activity (TETRA)

In FY24, the Test and Evaluation Threat Resource Activity (TETRA) continued evaluating the capabilities of current and emerging threat systems critical to OT&E and LFT&E of DoD systems and services. These evaluations included, but were not limited to, the contested electromagnetic spectrum (EMS) environment, the use of artificial intelligence (AI) in adversary systems, and assessments of adversary order-of-battle, capability, concept of operations, and tactics, techniques, and procedures (TTP). For instance, TETRA initiated the development of cognitive, AI-driven, and other high-complexity threat models to facilitate T&E of cognitive and AI-driven electronic warfare (EW) systems. Moreover, TETRA began developing high fidelity space threat models and counterspace threat surrogates to support OT&E and LFT&E of space systems. TETRA managed 129 intelligence authoritative analysis projects and provided threat and target data to support the accreditation of physical surrogates and digital representations of threats and targets for OT&E and LFT&E.

PROGRAM OVERVIEW

TETRA, established in 2000, is a joint duty initiative between DOT&E and the Defense Intelligence Agency (DIA). Its purpose is to ensure that OT&E and LFT&E programs, along with warfighter mission planning and training, are well-informed by emerging intelligence data. TETRA is comprised of DIA analysts, engineers, modelers, and scientists who provide authoritative and timely intelligence assessments of the current and emerging multi-domain threat environment to the OT&E and LFT&E Enterprise. Specifically, TETRA: (1) generates artifacts that include intelligence-based analysis of current and emerging threats and targets; (2) supports the acquisition and utilization of foreign materiel required for testing or developing threat and target surrogates; (3) oversees the verification, validation, and certification of threat and target surrogates, including hardware surrogates and digital representations, such as models, simulations, and digital twins; (4) utilizes emerging science and technologies to anticipate future threat and target capabilities; and (5) investigates, develops, and delivers to the DOT&E and Intelligence Community (IC) novel capabilities required for OT&E of hard problems, such as those required for the analysis of AI human-autonomous teams and Superteams. TETRA's role as a liaison between the acquisition, test, and intelligence communities ensures specialized intelligence support and products tailored to OT&E and LFT&E requirements.

MISSION

In coordination with the DIA and the Services' intelligence production centers (IPCs), TETRA conducts analysis and supports the delivery of capabilities of threat and target digital representations, surrogates, and foreign materiel to meet OT&E and LFT&E requirements.

FY24 KEY ACTIVITIES

» INTELLIGENCE ANALYSIS TO SUPPORT OT&E AND LFT&E

In FY24, TETRA improved the capabilities of over 50 new and emerging threats and targets to support adequate evaluation of the operational effectiveness, suitability, survivability, and lethality of DoD systems and services. Specifically, TETRA:

- Developed DOT&E's Top 50 Foreign Materiel Program (FMP) Priorities list for FY25 to advocate for congressional funding for FMP community efforts to anticipate, prioritize, collect, and manage FMP activities.
- Developed the Threat Annex for the classified DOT&E FY24 Assessment Report of the Missile Defense System, to define the operational threat environment and highlight ballistic missile defense concerns for testers and decision makers.
- Assessed design characteristics, performance capability, and employment tactics for selected foreign torpedo weapon systems, to inform threat surrogate design decisions supporting parameters for OT&E and LFT&E.
- Coordinated with the National Oceanographic Office to develop an assessment of general seabed characteristics, for a defined region, to assess the suitability of potential test sites as realistically challenging environments for operational test (OT) events.
- Coordinated with the Office of Naval Intelligence to assess foreign naval combatants' anti-air warfare capability, to support evaluation of U.S. offensive strike systems.
- Developed a custom product that identifies threat systems and associated threat emulation capabilities, to support operationally realistic adversary threat laydown criteria supporting OT design.
- Scoped the holistic small boat threat including design characteristics, armament, and performance capabilities, to support

characterization of small boat surrogate requirements for OT&E and LFT&E.

- Coordinated with multiple IPCs to identify IC-validated threat missile model emulations, to support missile defense program OT planning.
- Developed a threat intelligence, surveillance, and reconnaissance capability assessment, for a potentially contested region, to provide DOT&E a baseline assessment of adversary capabilities for inclusion in modeling efforts.
- Assessed threat air defense artillery systems, supporting a survivability study for an airborne platform, to support OT and modeling and simulation (M&S) efforts.
- Produced custom intelligence assessments for a foreign anti-ship cruise missile, and a foreign uncrewed surface vessel program to support evaluation of U.S. naval defense capabilities and platform survivability.
- Coordinated with the National Ground Intelligence Center to assess foreign short-range air defense capabilities, technologies, and trends, to support OT&E and LFT&E.
- Briefed stakeholders from NATO, the Space Systems Command, the Air Force, and Center for Countermeasures on directed energy weapons (DEW) threats, capabilities, proliferation, and trends. TETRA also manages and maintains the repository of DEW threat assessments for OT planning.
- Began development of TETRA's Intelligence Digital Ecosystem (TIDE) – an AI/machine learning (ML) customizable web-based interface to support trend analysis of threat intelligence data. TIDE will reduce cognitive load by generating AI summaries for intelligence documents, providing trend analysis of adversarial activity, determine cross- document contradiction detection, and support retrieval-augmented generation summaries for intelligence from multiple sources. TIDE will provide efficiency and trend analysis to better incorporate the threat into OT to increase survivability and effectiveness for DoD acquisition systems.
- Supported the NASA Cyber Threat Working Group by providing vital intelligence on the rapidly adapting adversarial cyber threat.
- Provided DOT&E critical cyber threat assessments for the defense of Guam.
- Delivered mission-critical threat briefings to the U.S. Navy's Conventional Prompt Strike program development team to enhance the team's understanding of current adversary cyber threat capabilities.
- Provided realistic cyber threat intelligence support to Patriot network command and control testing. The TETRA Cyber Threat Intelligence Team assesses real-world active threats to support the DOT&E test community with current cyber intelligence, to maintain realistic testing parameters that mirror adversary TTP.
- Assessed threat intelligence, capability, and EW for OT&E of the Next Generation Jammer, Compass Call, B-21, and multiple other high-priority air warfare platforms.

TETRA contributed to multiple working groups and studies that drive policies and requirements governing intelligence support to DoD acquisition system development. TETRA's contributions ensure intelligence support to acquisition adequately informs T&E threat representations, develops needed M&S, and generates critical intelligence mission data to facilitate realistic, operationally relevant T&E prior to fielding.

» KEEPING PACE WITH EMERGING THREATS AND TARGETS

In FY24, TETRA:

- Developed and managed 38 AI-enabled EW projects in support of: (1) the development of red threat cognitive EW threat models by IPCs; (2) adaptive OT and developmental test (DT) environments; (3) test design, data analysis, and performance metrics; (4) machine learning operations (MLOps) for rapid reprogramming and online learning ; and (5) policies, processes, and guidance for T&E of AI-enabled systems. These efforts identified and evaluated existing tools, processes, and methodologies to address the data, measurement, and analysis challenges faced by the EW OT&E community. By designing and constructing reusable solutions and guidance for establishing a threat environment for cognitive capability test and development, DOT&E is meeting specific goals in its Strategy Implementation Plan including key actions from "3.2 Emphasize cyber and electromagnetic spectrum survivability" and "4.2 Evaluate the operational and ethical performance of AI-Based systems."

- Developed a roadmap to close test capability gaps for the evaluation of U.S. space systems' resiliency against emergent threats. The roadmap led to demonstration of progress on potential counterspace EW threats and radio frequency (RF)-enabled cyber threats to satellite communications and satellite telemetry, tracking, and command. These efforts support the adequacy of T&E against space threats in a representative environment.
- Completed a T&E community survey and provided a detailed assessment on test capabilities and gaps related to the survivability of uplinks for space assets. In collaboration with the Space T&E community, TETRA developed solutions and provided recommendations on investments to close these gaps.
- Coordinated with National Space Test and Training Complex (NSTTC) Digital Range and Intelligence Centers for space threat model development. The developed models will enable resiliency testing of military satellite communications and tracking, telemetry, and control signals which affect all DoD space programs in digital, hardware-in-the-loop, and open-air environments. The model development plan met the requirements identified in the DoD Ranges Workshop; the NSTTC and U.S. Space Force needs; and the 2021 and 2022 National Academies of Sciences, Engineering, and Medicine's "range of the future" reports.
- Collaborated with the Space T&E community to discuss the impact of the RF-enabled cyber threat and its impact to space assets from multiple attack vectors. TETRA began development of new TTP to support the Space T&E community for this emerging threat capability.
- Partnered with National Space Intelligence Center to develop a Space Object Surveillance and Identification architecture for space domain awareness and space debris collision avoidance.

» ACQUIRING ACTUAL FOREIGN THREATS

OT&E and LFT&E programs rely on the availability of actual, foreign materiel threat systems to: (1) test U.S. and allied systems against, or (2) support development of threat or target surrogates (either physical or digital) through reverse engineering. In the absence of the actual threat, TETRA supplies intelligence data on the threat or target characteristics and capabilities critical to the development of threat surrogates.

To secure actual systems for intelligence analysis and use in OT, TETRA works directly with the Joint Foreign Materiel Program Office, overseen by the USD(I&S), as well as other foreign materiel organizations and the IC. 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 IC collection opportunities. The Joint FMP is a critical link between the T&E community, DIA, 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. In FY24, TETRA monitored, developed, and coordinated dozens of acquisition efforts.

For example, foreign man-portable air-defense systems (MANPADS) are in high demand for: (1) the development of MANPADS surrogates to enable adequate testing of countermeasures, (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 antitank 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. Very high frequency radars have been required for programs such as the F-35, to determine how to counter longer acquisition range and low probability of intercept. Decoys of foreign surface-to-air missile systems are in recent demand for threat density and operational realism.

In FY24, TETRA:

- Managed a highly successful foreign materiel acquisition effort essential to delivering threat density and decoys for U.S. and allied OT&E range capability. This effort is critical to F-35, B-21, and over 50 other DoD systems and services acquired via the Defense Acquisition System.
- Led critical foreign materiel acquisition and delivery of essential systems for U.S. support to an ally in a wartime environment.
- Led the reconstituted DoD FMP's Board of Director's T&E Subcommittee ensuring the T&E community stays informed of ongoing foreign materiel acquisitions, foreign materiel exploitations, and requirements tied to specific test events.

» ACCREDITED THREAT AND TARGET MODELS AND SURROGATES

Current and emerging threat weapon systems continue to become more complex, technically sophisticated, and dangerous. Ensuring that U.S. and allied weapons systems can operate and fight amid the modern, multi-domain, contested and congested, battlespace requires close partnership across the IC, weapon system developers, academia, and industry. Threat weapon systems and capabilities leverage technological advances including improved software-defined radios/radars, cloud-based information and big dataflow, AI/ML capabilities, and dispersed and increasingly autonomous operations. These advances in threat weapon systems, require additional focused development and balance of live, virtual, constructive (LVC) capabilities across the U.S. and allied T&E and training communities.

Since 2000, TETRA has served as a bridge between the IC and OT&E community, with a joint mission dating back to 1966. TETRA facilitated pertinent intelligence reports and assessments to weapon system developers and decision makers. TETRA also fostered close partnerships with various T&E facilities and labs helping to ensure that they had adequate capabilities to support T&E events. TETRA supported the development and accreditation of threat and target models and surrogates, either physical or digital twins. In accordance with DoD Instruction 5000.61 and DOT&E policy on M&S verification, validation, and accreditation, TETRA oversaw the threat surrogate verification, validation, and certification process to assess the uncertainties of the threat surrogate compared to the actual threat system that the warfighter would encounter in combat. TETRA served as the DOT&E representative for various Integrated Technical Evaluation and Analysis of Multiple Sources (ITEAMS) projects evaluating options to build threat representative simulators and models that leverage all-intelligence, open source, and industry data. TETRA ensured that threat and target M&S was 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 FY24, TETRA provided threat intelligence, validation, and certification expertise, as well as oversight for 14 joint and Service threat validation efforts, including:

- The Next Generation Jammer to develop a method to validate and certify the radar electronic attack countermeasure tools, models, and simulations.
- M&S gaps and verification, validation, and accreditation in support of Missile Defense System ground testing.
- The Joint Aircraft Mission Survivability Integrated Product Team.

During FY24, TETRA developed, validated, and delivered of 10 RF and 10 infrared (IR)/electro-optical threat models, as well as over 50 high fidelity, closed-loop, EW-capable, emulative threat models using ITEAMS assessments. TETRA is partnering with the IC for the development of additional Laboratory Intelligence Validated

Emulators (LIVEs), Within-Engagement EW (WEEW) system upgrades, and common high-assurance internet protocol encryptor interoperable manager for efficient remote administration (CHIMERA) threat models for 14 additional threats.

In FY24, DOT&E and TETRA delivered 32 new LIVE and WEEW systems and 18 new CHIMERA systems for installation at T&E sites and facilities. Moreover, TETRA provided programmatic oversight for the Missile and Space Intelligence Center's LIVE and WEEW Roadmap, which outlines the current and forecasted deep-dive intelligence assessments, high fidelity model development, and the production and sustainment efforts to field these emulative, closed-loop LIVE threat model systems.

TETRA leads the partnership between the intelligence productions centers and the Space Force to produce counterspace threat models supporting OT&E of space systems in the NSTTC. TETRA also leads a focused model development effort for a high priority counterspace threat to facilitate OT of DoD space systems' defensive measures and operator TTP against a threat that cannot be fully tested in a live environment due to security, safety, and policy constraints. This model, as well as others produced under the partnership, will form the foundation for evaluating the capability and resiliency of U.S. space programs in the contested space domain.

TETRA serves as the DOT&E focal point for T&E sites by organizing and hosting the RF and IR Collaboration Control Boards (CCBs). These RF and IR CCBs brought together leaders, technical representatives and developers, and subject matter experts from across the IC, the T&E community, industry, and academia. The CCBs review and discuss current and emerging RF and IR threats and various roadmaps of effort to understand, detect, test and evaluate and develop countermeasures and associated threat models against these threats. In FY24, TETRA began development of the first iterations of the Space and AI CCBs. TETRA manages and maintains Redmine, the database of IC validated threat models for use by the T&E sites to meet threat modeling requirements.

In FY24, TETRA maintained and updated and/or created 140 records in the Threat Systems Database (TSDB), which contains detailed information on over 2,000 threat representations, targets, M&S, and foreign materiel, and approximately 3,380 threats, including surface-to-air missiles, torpedoes, tanks, anti-ship cruise missiles, airborne systems, and 150 other threat types. The TSDB provides OT agencies with data for planning tests against specific threats.

TETRA leads the Trial Table Mafia to advance the capability to both test EW techniques against IC-validated threat emulators and assess the impact on a digital, threat representative, integrated air defense, via local or distributed assets, in national and multi-national test events.

TETRA participated in the NATO Air Survivability Sub-Group 2 and led an M&S community of interest, along with multiple multinational projects aimed at providing NATO Headquarters with assessments on the joint EW capabilities of NATO countries.

APPENDIX

This page intentionally left blank.

Oversight List

This page intentionally left blank.

DOT&E Oversight List as of September 30, 2024

- .338 Norma Magnum Anti-Materiel, XM1224 (.338 NM AM)
- 120MM Advanced Multi-Purpose (AMP), M1147, High Explosive Multi-Purpose with Tracer (HEMP-T) (M1147 AMP)
- Abrams M1A1 SA; M1A2 SEP; APS
- AC-130J High Energy Laser
- Advanced Airborne Sensor
- Advanced Anti-Radiation Guided Missile - Extended Range
- Advanced Anti-Tank Weapon System - Medium (Javelin)
- Advanced Arresting Gear
- Advanced Battle Management System
- Advanced Reconnaissance Vehicle (ARV)
- AEGIS Modernization (Baseline Upgrades)
- AEHF - Advanced Extremely High Frequency (AEHF) Satellite Program
- Aerosol and Vapor Chemical Agent Detector
- 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 Base Air Defense Battle Management Command and Control
- Air Force Integrated Personnel and Pay System (AF-IPPS)
- Air Force Intercontinental Ballistic Missile Fuze Modernization
- Air Force Maintenance, Repair and Overhaul (MRO)
- 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/APR-39E(V2) Radar Warning Receiver
- AN/TPQ-53 Counterfire Target Acquisition Radar
- Armed Overwatch
- Armored Multipurpose Vehicle (AMPV)
- Autonomous Transport Vehicle - System (ATV-S)
- Auxiliary General Ocean Surveillance Ship (T-AGOS 25)
- B-21 Long Range Strike Bomber
- B-52 Radar Modernization Program (RMP)
- B-52J Commercial Engine Replacement Program (CERP)
- Barracuda Mine Neutralization System
- Bradley ECP; MOD; APS
- Cannon Delivered Area Effects Munitions (C-DAEM) Armor (Inc 1)
- Capability Set 21/23 Integrated Tactical Network - Rapid Fielding
- CH-47F Modernized Cargo Helicopter
- CH-53K King Stallion
- CMV-22 Joint Services Advanced Vertical Lift Aircraft - Osprey -- Carrier Onboard Delivery (COD)
- Cobra Dane Automated Data Processing Equipment Rehost Phase II
- Columbia Class SSBN - including all supporting PARMs
- Command Post Computing Environment/ Tactical Services Infrastructure
- Common Infrared Countermeasures (CIRCM)
- Common Tactical Truck (CTT)
- Conventional Prompt Strike
- Cooperative Engagement Capability (CEC)
- Cooperative Engagement Capability Increment II
- Cross-Domain Solutions

DOT&E Oversight List as of September 30, 2024

- CVN-78 - GERALD R. FORD CLASS Nuclear Aircraft Carrier
- DDG 1000 - ZUMWALT CLASS Destroyer
- DDG 51 Flight III
- Deep Space Advanced Radar Capability
- Defense Enterprise Accounting & Management System
- Defense Enterprise Office Solution (DEOS)
- Deliberate and Crisis Action Planning and Execution System (DCAPES) Inc. 2B
- Digital Modernization Strategy (DMS) – Related Enterprise Information Technology Initiatives
- Directed Energy Maneuver-Short Range Air Defense (DE M-SHORAD)
- Dismounted Assured Positioning, Navigation, and Timing System (DAPS)
- Distributed Common Ground Station - Air Force (DCGS-AF)
- Distributed Common Ground System - Army (DCGS-A)
- Distributed Common Ground System - Navy (DCGS-N)
- DoD Healthcare Management System Modernization (DHMSM)
- Dry Combat Submersible (DCS)
- E-2D Advanced Hawkeye
- E-7A Rapid Prototyping
- EA-18G - Airborne Electronic Attack
- EC-37B Compass Call Rehost
- Electro-Magnetic Aircraft Launching System
- Electronic Warfare Planning and Management Tool (EWPMT)
- Enhanced Polar System
- Enterprise Air Surveillance Radar
- Enterprise Business Systems Convergence
- Enterprise Space-Based Missile Warning
- Evolved Sea Sparrow Missile Block 2
- Evolved Strategic Satellite Communications
- Evolved Strategic Satellite Communications - Cryptologic Segment
- Evolved Strategic Satellite Communications Ground Segment
- EXTRA LARGE UNMANNED UNDERSEA VEHICLE (XLUUV)
- E-XX (Take Charge and Move Out) Recap
- F/A-18E/F Super Hornet Aircraft
- F-15 Eagle Passive Active Warning Survivability System
- F-15EX
- F-16 AN/ALQ-257 Integrated Viper Electronic Warfare Suite
- 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 Tactical Unmanned Aircraft System INC 2 (FTUAS INC 2)
- Future Unmanned Aircraft System-Air Launched Effects (FUAS ALE)
- Future Unmanned Aircraft Systems - Scalable Control Interface (FUAS SCI)
- 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
- Guided Multiple Launch Rocket System/ Guided Multiple Launch Rocket System Alternative Warhead (GMLRS/GMLRS AW)
- Hammerhead Encapsulated Effector Program MOD 1
- Handheld, Manpack, and Small Form Fit Radios (HMS)
- Hercules M88 Upgrade Recapitalization (M88A3)
- HH-60W Jolly Green II
- High Accuracy Detection and Exploitation System (HADES)
- Hypersonic Attack Cruise Missile
- 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)
- Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs – Air Force)
- Improved Threat Detection System
- Improved Turbine Engine Program (ITEP)
- Indirect Fire Protection Capability Increment 2 (IFPC Inc 2)
- Infrared Search and Track
- Integrated Air and Missile Defense
- Integrated Air and Missile Defense of Guam
- Integrated Head Protection System (IHPS)
- Integrated Personnel and Pay System-Army Increment 2
- Integrated Tactical Network - Rapid Prototyping
- Integrated Visual Augmentation System 1.2 Rapid Prototyping (IVAS 1.2 RP)
- Integrated Visual Augmentation System Rapid Fielding
- Joint Air-to-Ground Missile (JAGM)
- Joint Air-to-Surface Standoff Missile Weapon Data Link
- Joint Biological Tactical Detection System
- Joint Cyber Warfighting Architecture - Access Platform
- Joint Cyber Warfighting Architecture - Joint Cyber Command and Control
- Joint Cyber Warfighting Architecture - Persistent Cyber Training Environment
- Joint Cyber Warfighting Architecture - Unified Platform
- Joint Cyber Warfighting Architecture Enterprise
- Joint Light Tactical Vehicle Family of Vehicles
- Joint Operational Medicine Information Systems
- Joint Planning and Execution System
- Joint Regional Security Stack (JRSS)
- Joint Transportation Management System
- KC-46A Tanker Modernization
- Key Management Infrastructure (KMI)
- Large Displacement Unmanned Undersea Vehicle (LDUUV)
- Large Unmanned Surface Vehicle
- LGM-35A Sentinel
- LHA 6 Flt I and associated PARMs
- 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
- Long Endurance Electronic Decoy (LEED)
- Long Range Hypersonic Weapon Ground Support Equipment (LRHW GSE)
- Long Range Stand Off Weapon

- Lower Tier Air and Missile Defense Sensor
- LPD 17 Flt II
- M10 Booker (Booker)
- Maneuver Short Range Air Defense Increment 1 (M-SHORAD Inc 1)
- Marine Air Ground Task Force Unmanned Aircraft System Medium Altitude Long Endurance (MUX MALE) Increment II, SkyTower II MTA (MUX MALE Inc II SkyTower II MTA)
- Massive Ordnance Penetrator Modification
- Medium Landing Ship
- Medium Unmanned Surface Vehicle
- Medium Unmanned Undersea Vehicle (Razorback)
- MH-139A Grey Wolf
- Mid-Range Capability (MRC)
- Military Global Positioning System (GPS) User Equipment Increment 1
- Military GPS User Equipment Increment 2
- Military Personnel Data System
- Mine Countermeasures Unmanned Surface Vehicle and payloads
- Missile Defense System
- Mission Partner Environment (MPE)
- MK 48 ADCAP COMMON BROADBAND ADVANCED SONAR SYSTEM
- Mk 48 Mod 9 Heavyweight Torpedo
- Mk 54 torpedo/MK - 54 VLA/MK 54 Upgrades Including High Altitude ASW Weapon Capability (HAAWC)
- MK 58 Compact Rapid Attack Weapon Very Lightweight Torpedo TI-1
- MK 58 Compact Rapid Attack Weapon Very Lightweight Torpedo TI-2
- Mk21A Reentry Vehicle
- Mobile Advanced Extremely High Frequency Terminal
- Mounted Assured Positioning, Navigation, and Timing System (MAPS)
- Mounted Mission Command - Software
- Mounted Mission Command-Transport (MMC-T)
- MQ-25 Stingray
- MQ-4C Triton
- MQ-8C Fire Scout Unmanned Aircraft System
- M-SHORAD Inc 3 - Next Generation Short Range Interceptor (M-SHORAD Inc 3)
- Multi-Function Electronic Warfare
- National Background Investigation System
- Naval Integrated Fire Control - Counter Air (NIFC-CA) From the Air
- Naval Maintenance, Repair and Overhaul Solution
- Naval Operational Supply System
- Navy Personnel and Pay System
- Next Generation Countermeasure System (NGCM)
- Next Generation Jammer - Mid-Band
- Next Generation Jammer Low Band
- Next Generation Large Surface Combatant
- Next Generation Operational Control System
- Next Generation Overhead Persistent Infrared Space
- Next Generation Squad Weapons Fire Control Rapid Fielding (NGSW FC RF)
- Next Generation Squad Weapons Weapons and Ammunition Rapid Fielding (NGSW W&A RF)
- Nuclear Biological Chemical Reconnaissance Vehicle Sensor Suite Upgrade (NBCRV SSU)
- Offensive Anti-Surface Warfare Increment 1 (Long Range Anti-Ship Missile)
- Offensive Anti-Surface Warfare, Increment 2 (Air and Surface Launch)
- Over The Horizon Weapon System
- Patriot Advanced Capability 3
- Precision Strike Missile
- Presidential and National Voice Conferencing Integrator

- Proliferated Warfighter Satellite Architecture Tranche 1 Transport Layer
- Protected Tactical Enterprise Service
- Protected Tactical SATCOM
- Public Key Infrastructure (PKI) Inc. 2
- Robotic Combat Vehicle (RCV)
- SBIRS - Space-Based Infrared System Program
- Sentinel A4 Mod
- SF - Space Fence
- Ship Self Defense System (SSDS)
- Ship to Shore Connector
- Small Diameter Bomb Increment II
- Small Unmanned Undersea Vehicle - LIONFISH
- Space Based Infrared System (SBIRS) Survivable and Endurable Evolution (S2E2)
- Space Command and Control
- Stand In Attack Weapon
- Standard Missile 2 (SM-2) including all mods
- Standard Missile-6 (SM-6) Air Launched Configuration (ALC)
- Standard Missile-6 Including all mods and variants
- Strategic Mission Planning and Execution System
- Stryker Family of Vehicles (Styker FoV)
- Surface Electronic Warfare Improvement Program AN/SLQ-32C(V)6
- Surface Electronic Warfare Improvement Program Block 2
- Surface Electronic Warfare Improvement Program Block 3
- Surface Mine Countermeasures Unmanned Undersea Vehicle (SMCM UUV)
- Surface Navy Laser Weapon System
- Survivable Airborne Operations Center E-4C
- Synthetic Training Environment - Live Training Systems (STE-LTS)
- T-7 Advanced Pilot Training
- Tactical Intelligence Targeting Access Node
- 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
- Terrestrial Layer System Brigade Combat Team (TLS - BCT)
- Terrestrial Layer System Echelons Above Brigade (TLS - EAB)
- Theater Medical Information Program - Joint Increment 2
- Three-Dimensional Expeditionary Long-Range Radar
- Torso & Extremity Protection (TEP)
- Tranche 1 Tracking Layer
- Tranche 2 Enterprise
- Trident II (D-5) Submarine-Launched Ballistic Missile (SLBM)
- Unified Network Operations (UNO)
- Uniform Integrated Protection Ensemble Family of Systems General Purpose (UIPE FoS GP)
- Upgraded Early Warning Radar
- VC-25B
- VH-92A Presidential Helicopter
- VIRGINIA Class SSN 774
- Vital Torso Protection (VTP)
- Weather Satellite Follow-on (WSF)
- Wideband Communications Services
- XM 250 Top Attack Close Terrain Shaping Obstacle Increment 1 - MTA Rapid Prototyping (XM250 TA CTSO INC 1 - MTA RP)
- XM1170 30x173mm Armor Piercing, Fin Stabilized, Discarding Sabot with Trace
- XM1176 40mm High Velocity (HV) High Explosive Dual Purpose Air Burst (HEDP-AB) (40mm HEDP-AB)

- XM1182 30x173mm High Explosive Air Burst with Trace (HEAB-T) (XM1182 HEAB-T)
- XM1203 50mm Armor Piercing, Fin Stabilized, Discarding Sabot with Trace (XM1203 APFSDS-T)
- XM1204 50mm High Explosive Airburst with Trace (XM1204 HEAB-T)
- XM1223 30x113mm Multi-Mode Proximity Airburst (MMPA) (30mm MMPA)
- XM30 Combat Vehicle (XM30)

DOT&E Activities

This page intentionally left blank.

Table 1. FY24 DOT&E Independent System Evaluation Reports

Program	Date
Early Fielding Reports (EFRs)	
MQ-4C Triton Integrated Functional Capability 4.1.2.4 EFR	January 2024
Small Diameter Bomb Increment II Integration on the F/A-18E/F EFR	February 2024
Mk 48 Mod 7 Heavyweight Torpedo with Shallow Water Urgent Build Software EFR	February 2024
Standard Missile-2 Block III C EFR	March 2024
E-2D Delta System Software Configuration 4 EFR	June 2024
F/A-18 E/F and EA-18G H18 Rel 2 Version 22.4.3 EFR	September 2024
Follow-on Operational Test and Evaluation (FOT&E) Reports	
Family of Medium Tactical Vehicles FOT&E Report	October 2023
AIM-120D Advanced Medium Range Air-to-Air Missile FOT&E Report	January 2024
Javelin Antitank Missile System – Medium FOT&E Report	March 2024
F-22 Raptor Release 2 FOT&E Test Report	March 2024
CMV-22 Joint Services Advanced Vertical Lift Aircraft – Osprey – Carrier Onboard Delivery Combined FOT&E and LFT&E Report	July 2024
AIM-9X Cyber and Lethality Annex to DOT&E FOT&E Report	July 2024
MQ-8C Surface Warfare Increment FOT&E Report	August 2024
Initial Operational Test and Evaluation (IOT&E) Reports	
Dry Combat Submersible IOT&E Report	October 2023
F-15EX Combined IOT&E and LFT&E Report	November 2023
F-16 Radar Modernization Program APG-83 Scalable Agile Beam Radar IOT&E Report	January 2024
F-35 Combined IOT&E and LFT&E Report with Post-IOT&E Block 4 Testing Annex	February 2024
Dismounted Assured Positioning, Navigation, and Timing System Gen II IOT&E Report	May 2024
F-15 Eagle Passive Active Warning and Survivability System IOT&E Report	July 2024
Mounted Assured Positioning, Navigation, and Timing System IOT&E Report	September 2024

Table 1. FY24 DOT&E Independent System Evaluation Reports, continued

Program	Date
Operational Assessment (OA) Reports	
B-21 Milestone C OA Report	October 2023
Three-Dimensional Expeditionary Long-Range Radar OA Interim Observation Memo	March 2024
Air and Missile Defense Radar / AN/SPY-6(V)1 OA Report	March 2024
Long Range Unmanned Surface Vessel Early OA Report	May 2024
Operational Demonstration (Ops Demo) Reports	
Next Generation Squad Weapons, Ammunition, and Fire Control Combined Ops Demo and Limited Lethality Assessment Report	May 2024
Terrestrial Layer System Brigade Combat Team Manpack Ops Demo Report	May 2024
Synthetic Training Environment – Live Training System Increment 1 Ops Demo Report	August 2024
Operational Test and Evaluation (OT&E) Reports	
Patriot Post Deployment Build-8.1 Limited User Test Report	December 2023
Command Post Computing Environment Tactical Service Infrastructure CVPA and AA Report	July 2024
Air Operations Center – Weapon System Cyber Survivability Report	September 2024

Table 2. Other FY24 DOT&E Reports

Program/Topic	Date
Legislative Reports/Responses	
Brief for the HASC on the Development and Testing of Body-Worn Equipment for the USMC and U.S. Army	November 2023
FY23 NDAA Section 242: A Report on the Sufficiency of the Operational Test and Evaluation Resources on Certain Major Defense Acquisition Programs	December 2023
Brief for the HASC on Contractor-Provided T&E Capabilities	December 2023
Brief for the HASC on T&E Equipment Shortfalls	December 2023
FY23 NDAA Section 1656: Persistent Cyberspace Operations (PCO) Report	January 2024
Certification of Appropriateness and Risk Assessment of Services' Planned Test Strategies for Approved Middle Tier of Acquisition (804) and Accelerated Acquisition Programs	March 2024
FY23 NDAA Section 217: Competitively Awarded Demonstrations and Tests of Electromagnetic Warfare Technology	June 2024

Table 2. Other FY24 DOT&E Reports, continued

Program/Topic	Date
Assessment of the DoD's and Services' Funding of Test Infrastructure, Assets, and Personnel to Support Agreed-Upon Test and Evaluation of Programs on the DOT&E Oversight List	July 2024
Battery Testing Infrastructure: HASC Report 117–397 Response	August 2024
Missile Defense System Report	
2023 Assessment of the Missile Defense System	February 2024
Special Reports	
Findings Associated with the Link Monitoring and Management Tools	October 2023
Commercial Cyber Analyses	October 2023
U.S. European Command Cyber Assessment	November 2023
U.S. Navy Cyber Assessment 2023	November 2023
Finding Memorandum: Observations Associated with CSG Assessments	February 2024
DOT&E Cyber Assessment Program Assessment Results and Recommendations for Navy Flank Speed Zero Trust Environment	April 2024
Joint Testing Market Study	June 2024
DOT&E Cyber Assessment Program Assessment Results of Oracle Cloud Infrastructure and Cloud Zero Trust Recommendations	June 2024

Table 3. FY24 DOT&E-Approved TEMPs and Test Strategy Documents

Program Document
AEGIS Cruiser and Destroyer Advanced Capability Build 2016 (ACB 16) TEMP 1669
Amphibious Combat Vehicle Medium Caliber Cannon Variant (ACV-30) TEMP Full Rate Production Update Annex B
CH-53K TEMP 1683 Revision C CH-1
Cloud-Based Command and Control TES
Common Tactical Truck (CTT) Middle Tier of Acquisition Rapid Prototyping Phase TES
Deep Space Advance Radar Capability Site 1 TEMP
Enterprise Business System Convergence (EBS-C) TES

Table 3. FY24 DOT&E-Approved TEMPs and Test Strategy Documents

Program Document
E-XX Take Charge and Move Out (TACAMO) Recapitalization Program Alternate TES
E-XX Take Charge and Move Out (TACAMO) Milestone B (MS B) TEMP
F-16 Active Electronically Scanned Array (AESA) Radar Modernization Program (RMP), TEMP Annex, Version B
F-22 Capabilities Pipeline: Release 3 and 4 Operational Flight Programs (OFPs) TEMP
Future Long Range Assault Aircraft (FLRAA) TEMP
Indirect Fire Protection Capability Increment 2 Middle Tier of Acquisition Rapid Prototyping Pathway TEMP
Integrated Master Test Plan Version 25.1 (IMTP v25.1)
Integrated Master Test Plan Version 26.0 (IMTP v26.0)
Joint Cyber Command and Control (JCC2) TEMP
Lower Tier Air and Missile Defense Sensor (LTAMDS) Program Pre-Major Defense Acquisition Program (MDAP) Middle Tier Acquisition Rapid Prototyping (MTA-RP) TES
Mk21A MS B TEMP
Mobile Protected Firepower (MPF) TEMP
Mounted Assured Positioning, Navigation, and Timing System, Change 1, TEMP
Multi-Function Mmunition (MFM) 30MM: High Explosive Airburst with Trace (HEAB-T), XM1182 TEMP
Sentinel AN/MPQ-64A4 Radar System TEMP
Standard Missile-2 Block IIICU TEMP
Uniform Integrated Protection Ensemble Family of Systems General Purpose (UIPE FoS GP) TEMP

Table 4. FY24 DOT&E-Disapproved TEMPs and Test Strategy Documents

Program Document
Cooperative Engagement Capability (CEC) TEMP REV 6 Change 1

Table 5. FY24 DOT&E-Approved Test Plans

Program Document
AARGM-ER IOT&E Test Plan
Aerosol Vapor Chemical Agent Detector (AVCAD) Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan
Aerosol Vapor Chemical Agent Detector (AVCAD) Integrated Testing Data Collection Plan
Aerosol Vapor Chemical Agent Detector (AVCAD) Low-Rate Initial Production (LRIP) Chemical Test Developmental Test/ Operational Test (DT/OT) Detailed Test Plan
Aerosol Vapor Chemical Agent Detector (AVCAD) Operational Test Data Collection Plan
Aerosol Vapor Chemical Agent Detector Man Portable (AVCAD - MP) Multi-service Operational Test and Evaluation (MOT&E) Operational Test Plan
Aerosol Vapor Chemical Agent Detector Shipboard Fixed (AVCAD-SF) Production and Deployment (P&D) Chemical Chamber Test Plan
AIM-9X Block II Data Collection Plan
Amphibious Combat Vehicle Medium Caliber Cannon (ACV-30) Cooperative Vulnerability and Penetration Assessment Test Plan
AOC-WS i10.1 Adversarial Assessment Test Plan
Automated Security Validation Operational Test Cyber Survivability Test Plan
CH-53K Digital Interoperability Medium System Cyber Survivability Test Plan
Cloud-Based Command and Control Operational Assessment (OA) Test Plan
Command Post Computing Environment (CPCE) Cyber Test Plans
Deliberate and Crisis Action Planning and Execution Segments (DCAPES) IOT&E Test Plan
Dismounted Assured Positioning, Navigation, and Timing System Initial Operational Test (DAPS IOT) Test Plan
Dry Combat Submersible (DCS) FOT&E Test Plan
E/A-18G SCS H18 REL 3 FOT&E Test Plan
E-2D Delta System Software Configuration 4 Operational Test Plan change
E-2D Delta System Software Configuration 4 Operational Test Plan Change
E-7A Alternate Live Fire Test Plan

Table 5. FY24 DOT&E-Approved Test Plans, continued

Program Document
Extended Range Guided Multiple Launch Rocket System Follow-On Test (ER GMLRS FOT) Operational Test Plan
F-15 EPAWSS Cyber Test Plan
F-15 EPAWSS IDAL Test Plan Deviation
F-16 IVEWS OA Test Plan
F-35 2023-2024 Suitability Test Plan
F-35 FY24-25 Overarching Cybersecurity Operational Test Plan
Flight Test Ground-based Midcourse Defense Weapon System-12 Operational Test Plan
Force Element Terminal Operational Assessment Test Plan
Geosynchronous Space Situational Awareness Program (GSSAP) Cyber Follow-On Operational Test and Evaluation (FOT&E) Plan
Gerald R. Ford (CVN 78) Class Nuclear Aircraft Carrier Initial Operational Test and Evaluation Test Plan Update 1
Infrared Search and Track (IRST) Block II
Integrated Fires Test Campaign 2024 (IFTC 24) Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan
Integrated Fires Test Campaign 24 Operational Assessment (IFTC 24 OA) Operational Test Plan
Javelin Light Weight Command Launch Unit (LWCLU) Adversarial Assessment (AA) Operational Test Plan
Joint Biological Tactical Detection System (JBTDS) Limit of Identification (LOID) Environmental Sampling Kit (ESK) and Assay Shelf-Life Production and Deployment (P&D) Test DT/OT Detailed Test Plan
Joint Biological Tactical Detection System Identifier (JBTDS ID) Operational Test Plan
Joint Common Access Platform Operational Assessment Test Plan
Joint Operational Medicine Information Systems, Medical Common Operating Picture Test Plan
Lower Tier Air and Missile Defense Sensor (LTAMDS) Operational Test Plan
M10 Booker Combat Vehicle (BCV) Cooperative Vulnerability and Penetration Assessment (CVPA) Operational Test Plan
M10 Booker Combat Vehicle Initial Operational Test (M10 BCV IOT) Operational Test Plan
Mounted Assured Position, Navigation, Timing System (Maps) Generation (GEN) 2 Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan

Table 5. FY24 DOT&E-Approved Test Plans, continued

Program Document
Mounted Assured Positioning, Navigation, and Timing System Generation II Initial Operational Test Plan
MQ-4C IOT&E Plan Change
Next Generation Jammer Mid-Band IOT&E Test Plan
Next Generation Squad Weapon -- Fire Control (NGSW-FC) Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan
Next Generation Squad Weapon (NGSW) System of Systems (SoS) Limited User Test (LUT) Operational Test Plan
Next Generation Squad Weapon Operational Assessment (NGSW OA) Operational Test Plan
NGAD-P Alternate Live Fire Test Plan
Over The Horizon Weapon System (OTH-WS) Test Plan Change 3
Over The Horizon Weapon System (OTH-WS) Test Plan Change 4
Patriot Communications Obsolescence Upgrade Operational Demonstration Cybersecurity Test Plan
Patriot Post Deployment Build-8.1 Communication Obsolescence Upgrade (COU) and Digital Exciter Radar Set (DEX) Ops Demo Detailed Test Plan
Small Diameter Bomb Increment II (SDB II) on F/A-18E/F Quick Reaction Assessment (QRA) Test Plan Change 3
Small Diameter Bomb Increment II (SDB II) on F/A-18E/F Quick Reaction Assessment (QRA) Test Plan, Change 2
Stryker Double-V Hull Infantry Carrier Vehicle (ICVVA1) 30mm Cooperative Vulnerability and Penetration Assessment (CVPA) II Operational Test Plan
Stryker Infantry Carrier Double V-Hull A1 30mm FOT&E Operational Test Plan
Synthetic Training Environment-Live Training System Increment 1 Operational Demonstration (STE-LTS Inc 1 OD) Operational Test Plan
Terrestrial Layer System-Brigade Combat Team (TLS-BCT) Manpack (MP) System Operational Test Plan
Tomahawk Weapon System (TWS) Cyber Test Plan
Update to the DoD Public Key Infrastructure (PKI) Inc. 2 Cyber Survivability Test Plan Annex A
USS *Gerald R. Ford* (CVN 78) Cyber Survivability Test Plan
Weather System Follow-on Microwave Operational Utility Evaluation Test Plan

This page intentionally left blank.

Service Secretary Comments

This page intentionally left blank.

SECRETARY OF THE ARMY
WASHINGTON

1 7 JAN 2025

MEMORANDUM FOR Director, Operational Test and Evaluation, 1700 Defense Pentagon, Washington, DC 20301-1700

SUBJECT: Department of the Army Response to the Fiscal Year 2024 Director, Operational Test and Evaluation Annual Report

1. Thank you for the opportunity to respond to the Fiscal Year 2024 Director, Operational Test and Evaluation (DOT&E) Annual Report.

2. I appreciate the thoroughness of the report and the coordination between DOT&E and the Army. The Army acknowledges the importance of the oversight role of OSD activities. It is also imperative that 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. In general, this report accurately reflects the status of oversight programs in the Department of the Army.

3. The Army recognizes the challenges identified by DOT&E to test in the ever-evolving threat environment. The Army's research, development, test, and evaluation budget has prioritized funding, as resources permit, to procure representative kinetic and non-kinetic threats for emerging needs. Additionally, the Army continues to develop a live, virtual, constructive capability that connects test ranges enabling the scope, scale, and complexity necessary to create a realistic multi-domain environment at an affordable cost which otherwise would not be possible using current physical ranges and open-air testing.

4. We look forward to working with your office 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

This page intentionally left blank.

THE SECRETARY OF THE NAVY
WASHINGTON DC 20350-1000

JAN 15 2025

MEMORANDUM FOR DIRECTOR, OPERATIONAL TEST AND EVALUATION

SUBJECT: Department of the Navy Comments on the Fiscal Year 2024 Director Operational Test and Evaluation Annual Report

Thank you for the opportunity to review the Fiscal Year (FY) 2024 Director, Operational Test and Evaluation (DOT&E) annual report final draft. I appreciate the collaboration and work your team did with the Systems Commands, Program Executive Offices, and Program Management Offices to ensure the report is technically correct and meets all public releasability requirements.

Upon final review, the Department of the Navy is satisfied that the FY 2024 DOT&E annual report as written meets both of those criteria.

I look forward to continuing and strengthening the collaboration with DOT&E and the Offices of the Under Secretary of Defense for Research and Engineering Acquisition and Sustainment, and the other services as we continue to implement efficient and effective Integrated Test and Evaluation throughout 2025.

Carlos Del Toro

Carlos Del Toro

Copy to:
ASN (RD&A)
PCD/PMD ASN (RD&A)
DASN (RDT&E)

This page intentionally left blank.

SECRETARY OF THE AIR FORCE
WASHINGTON

JAN 31 2025

MEMORANDUM FOR DIRECTOR, OPERATIONAL TEST AND EVALUATION

SUBJECT: Department of the Air Force Response to Fiscal Year (FY) 2024 Director, Operational Test and Evaluation (DOT&E) Annual Report

I appreciate the opportunity to review the FY24 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.

Recognizing the dynamic nature of test and evaluation activities, the DAF submits the following errata to this year's report:

- MH-139A Grey Wolf (pg 339-340): The final decision to base MH-139A aircraft in the Air Force District of Washington has not yet been made in light of ongoing program adjustments and strategic basing considerations.

- Next Generation Operational Control System (OCX) (pg 356): The Space Force is committed to deliver the OCX system to operators in CY2025. In CY2024, the Space Force reassessed the remaining test campaign activities and developed a new plan to deliver the system to operations as soon as possible in 2025, prior to submission of the Defense Department (DD) Form 250. The new test schedule reflects ready to transition to operations (RTO) in June 2025 and operational acceptance in January 2026. The program is able to meet these dates by accelerating the start of Integrated System Test (IST) 3-1 to be performed in parallel with Site Acceptance Test. Furthermore, instead of requiring Government acceptance of the system via a submitted DD Form 250 as a prerequisite to commencing IST 3-1, acceptance will be granted later during RTO when the system is fully delivered. Early start of IST 3-1 testing allows for quicker discovery of system issues by operators and speeds up resolution.

- Military-Code GPS User Equipment (MGUE) Increment 1 (pg 357): The Space Force has mitigated delay impacts by reaching Destroyers (DDG) Program Executive Office (PEO) certification and changing the Aviation Domain lead platform from the B-2 to the Army MQ-1C Gray Eagle. These efforts will expedite Aviation PEO Certification, speed fielding of the Aviation/Maritime Card, and hasten MGUE delivery to the warfighter.

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.

Gary A. Ashworth
Acting Secretary of the Air Force

cc:
AF/CV
AF/TE

Commonly Used Acronyms

This page intentionally left blank.

The following acronyms are used throughout this Annual Report:

- #QFY## — # Quarter Fiscal Year ##
- AFB — Air Force Base
- CONUS — Continental United States
- DoD — Department of Defense
- DOT&E — Director, Operational Test and Evaluation
- FOT&E — Follow-on Operational Test And Evaluation
- FY## — Fiscal Year ##
- GPS — Global Positioning System
- IOT&E — Initial Operational Test and Evaluation
- LFT&E — Live Fire Test and Evaluation
- NATO — North Atlantic Treaty Organization
- NIPRNet — Non-classified Internet Protocol Router Network
- OCONUS — Outside the Continental United States
- OSD — Office of the Secretary of Defense
- OT&E — Operational Test and Evaluation
- OUSD — Office of the Under Secretary of Defense
- SECDEF — Secretary of Defense
- SIPRNet — Secret Internet Protocol Router Network
- T&E — Test and Evaluation
- TEMP — Test and Evaluation Master Plan
- TES — Test and Evaluation Strategy
- URL — Uniform Resource Locator
- USB — Universal Serial Bus
- USD(A&S) — Under Secretary of Defense for Acquisition and Sustainment
- USD(I&S) — Under Secretary of Defense for Intelligence and Security
- USD(P&R) — Under Secretary of Defense for Personnel and Readiness
- USD(R&E) — Under Secretary of Defense for Research and Engineering

Index of Programs

This page intentionally left blank.

E

F

G

H

I

J

T

V

www.dote.osd.mil