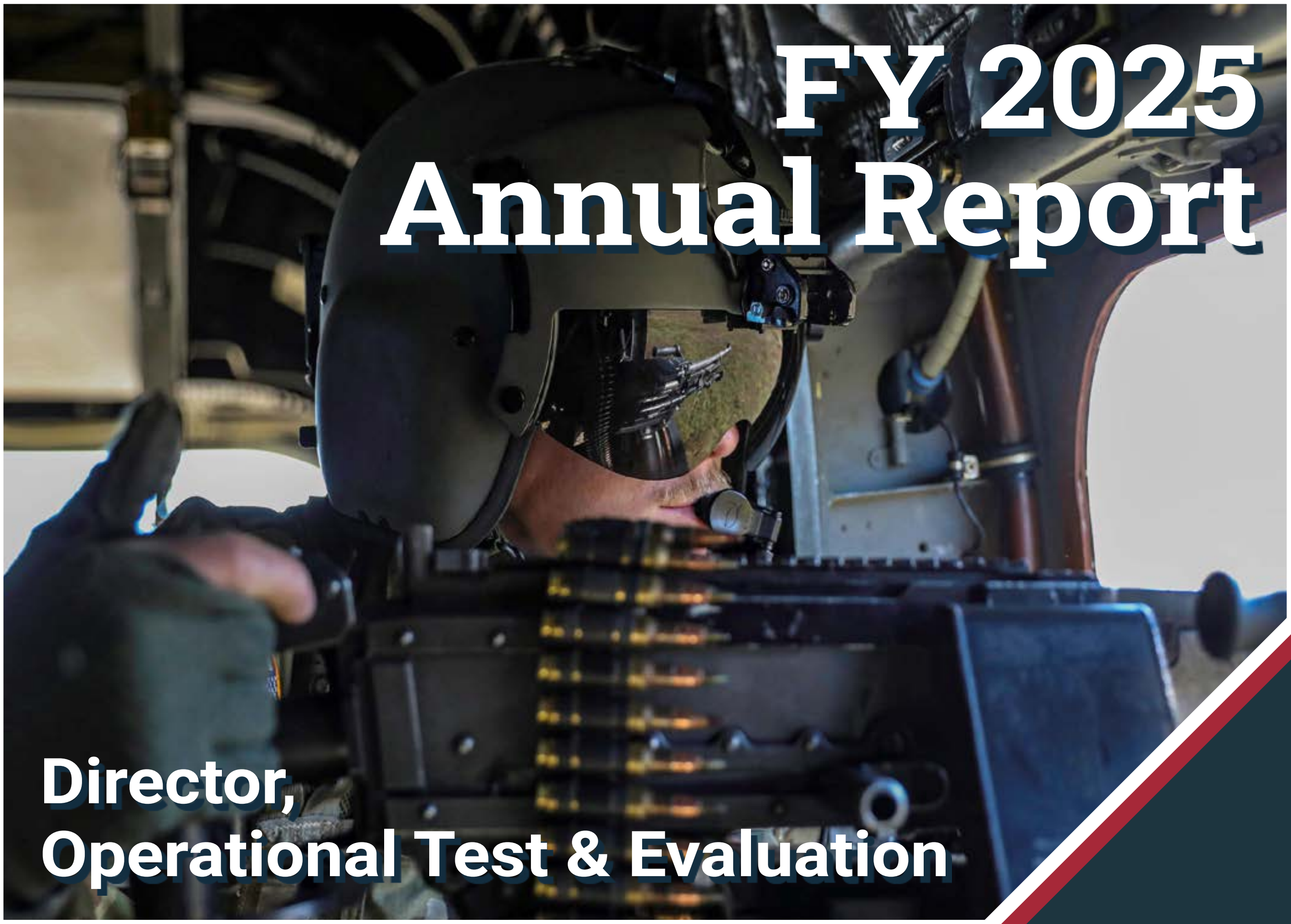


FY 2025 Annual Report

Director, Operational Test & Evaluation

March 2026

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.

Carroll P. Quade
Director (PTDO)

Introduction

It has been a great honor to serve as the senior advisor to the SecWar on the OT&E and LFT&E of the DoW's most critical warfighting capability. In FY25, DOT&E continued its mission to ensure adequate testing and to provide timely, rigorous, and independent evaluations of warfighting systems. Our commitment to ensuring U.S. military Service members receive combat-credible systems has never been more urgent. The threats and challenges to our national security demand that we rapidly and rigorously test and evaluate military platforms and warfighting ecosystems to determine if they are operationally effective, suitable, survivable, and lethal across complex, contested domains.

Throughout my tenure, I have worked with DOT&E staff to focus on the effective and efficient fulfillment of our statutory requirements by resetting priorities, increasing relevancy, and supporting the SecWar's Acquisition Transformation Strategy. In doing so, we have increased collaboration with key partners to align efforts across the DoW to enable the accelerated delivery of capable warfighting systems and ensure the T&E enterprise is ready and able to adapt and evolve at the rate that technological advancement demands.

DOT&E is committed to being more adaptive, timely, and relevant in the development of test plans, strategies, and reports. Because our work informs a number of significant decisions – design, acquisition milestones, Capability Portfolio Management, systems engineering and capability fielding – it is critical that our assessments are contextually relevant and time-phased to inform those decisions that we desire to affect. We have focused on renewing and strengthening partnerships across the OSW and the Services to eliminate duplicative efforts and optimize policy to enable a holistic, integrated approach to T&E. DOT&E has taken a leadership role in facilitating the coordination of operational assessments of multi-Service, warfighting kill chains. These partnerships and new approaches will be critical as the T&E enterprise postures to support the new Portfolio Acquisition Executives.

This report satisfies the provisions of title 10, United States Code, section 139, and summarizes the OT&E activities, including LFT&E activities, of the DoW during FY25.

ENABLING THE DOW'S ACQUISITION TRANSFORMATION STRATEGY

DOT&E is directly supporting initiatives to transform the way the DoW acquires weapons and warfighting capability. For the past several years, DOT&E has reported on the urgent need for the DoW's T&E enterprise to adapt, embrace digital transformation, evolve to adopt novel T&E approaches for complex software-centric systems, and consider performance data from all phases of a warfighting system's life cycle to inform operational evaluation. The SecWar's Acquisition Transformation Strategy presents the T&E enterprise with an unprecedented challenge – and opportunity – to truly adapt by streamlining processes, establishing new policy and plans, partnering with industry, and embracing technological advancements.

DOT&E is working with the Services, Agencies and other key partners in OSW to "prioritize integrated testing to optimize test resources, avoid redundancies, and utilize data-driven decisions to trace programs, performance, and testing." To that end and with our partners, we will reexamine and overhaul T&E policy, guidance, and manuals. To support operational assessments, we will endeavor to collect and use data from across the entire acquisition program's life cycle, including contractor testing, developmental testing, sustainment, operational employment of Minimum Viable Products and early Minimum Viable Capability Releases, and other government certification processes such as the DoW Chief Information Officer (CIO)'s Risk Management Framework. This will require an unprecedented level of collaboration with Developmental Test, Evaluation and Assessments (DTE&A), the Services, and Agencies to plan for combined, integrated T&E. DOT&E will work with industry and programs to embed diagnostics into software-centric capabilities to allow for early identification and mitigation of operational deficiencies and inform future development efforts.

DOT&E has prioritized support to the new Capability Portfolio Management process and cementing the T&E enterprise's role as an integral part of the systems engineering process. This will inform how we test and what we test to support development and acquisition decisions and to inform kill chain analysis. The T&E enterprise must be ready to react to rapidly evolving requirements from both the acquisition community and the warfighter.

EVOLVING THE T&E ENTERPRISE TO DETER, DENY, AND DEFEAT THREATS TO NATIONAL SECURITY

DOT&E continues to champion the key elements of adequate and efficient OT&E, but with a new sense of urgency driven by the SecWar's acquisition transformation initiatives and the rapid pace of emerging technological advancements and threat evolution. The T&E enterprise – test infrastructure, policy and procedures, workforce – must be postured to keep pace with rapid technological advances to characterize the operational performance of systems and kill chains that employ a vast range of new capabilities in hypersonics, directed energy, software, autonomy and artificial intelligence (AI), quantum and cyber realms. Over the next year, DOT&E will continue to work with the Services, Agencies, OSW colleagues, and other partners across academia, the National Laboratories, federally funded research and development centers (FFRDCs), and industry to:

- **Improve T&E Infrastructure:** Technologies that enable warfighting are evolving at an unprecedented pace, as are threats to our military missions. The DoW requires significant and sustained investments in modernizing T&E infrastructure to credibly validate warfighting capability and emulate threat systems enabled by emerging technologies in the software, AI, electromagnetic spectrum operations, hypersonics, and directed energy domains. DOT&E will work with the Services and Agencies to understand and advocate for the mitigation of T&E capability gaps that prevent adequate weapon performance validation and confirmation of resilience against emerging threats likely to be encountered in combat.
- **Maintain Design of Experiments (DOE) and Rigorous Statistical Analysis:** To optimize the use of scarce resources, DOT&E remains an advocate of DOE and corresponding statistical analysis methods to elicit maximum information from constrained resources, combine data across multiple independent test events, and produce defensible rationale for test adequacy

and quantification of risk. DOT&E will continue to partner with OUSW(R&E) and the Scientific Test and Analysis Techniques Center of Excellence (STAT COE) to ensure the T&E enterprise and program managers have access to scientific and statistical expertise to maximize the utility of the T&E data to support key warfighting and acquisition decisions.

- **Verify, Validate, and Accredit Modeling and Simulation (M&S):** M&S is a powerful tool that expands the scope of operational evaluations, because live operational testing across all combat scenarios and warfare domains is simply not feasible. There are undisputable challenges to emulating combat and multi-domain operations on physical ranges using actual systems or across Development Security Operations (DevSevOps) pipelines for software-centric capability. M&S can mitigate some of these limitations, but must be rigorously and continuously verified, validated, and accredited. In partnership with the Services and Agencies, DOT&E will advocate for credible, virtual OT&E of the effectiveness, suitability, lethality, and survivability of weapons systems by ensuring early and frequent collaboration across developers, acquirers, testers, and warfighters and implementation of rigorous statistical and analytical principles to compare M&S predictions with results from physical testing.
- **Characterize Human Systems Integration to Maximize System Usability:** The focus of OT&E will always be the warfighter. Hardware and software alone cannot accomplish missions. As the DoW's digital transformation continues with plans for vast, complex software-centric ecosystems enabling joint warfighting and extensive use of AI, it is more critical than ever to characterize the usability of military systems as well as the workload, fatigue, and frustration that operators experience while employing a system. Surveys are often the only means to evaluate these issues. DOT&E will continue to advocate and enable proper scientific survey design to ensure that the data collected to evaluate the quality of human-system interactions are valid, reliable, and inform meaningful outcomes.
- **Accelerate Digital Transformation to Lay the Groundwork for AI and Enable More Efficient, Timely OT&E:** Data is everything. Collecting the right data, accelerating data analyses, and sharing data-driven outcomes with the right people within operationally relevant timeframes are fundamental to fielding effective warfighting capability at the speed of need. Most of the Services and Agencies have impressive ongoing efforts to manage data and develop digital capability that could facilitate accelerated, more efficient test planning and evaluation in the future. DOT&E and key partners in OUSW(R&E) are leading efforts to enable coordination of those digital transformation activities across the Services and Agencies to maximize cost sharing, enable more powerful kill chain assessments, and effectively support the systems engineering process.
- **Conduct Combined and Integrated Testing to Reduce Test Cycles and Accelerate Fielding:** To support the deployment of combat credible systems at the speed of relevance, the T&E enterprise will need to take more extreme measures to greatly reduce, if not eliminate, the traditional contractor, developmental, and operational test silos. This requires the OT&E community to engage with program managers early in system development to construct testable, operationally relevant requirements; collect operationally relevant test data as early as possible during system development and in early operations; and identify performance shortfalls and cyber vulnerabilities when they are significantly cheaper and easier to mitigate.
- **Ensure the T&E Workforce is Postured to Meet the Warfighting Demands and Objectives of the SecWar's Acquisition Transformation Strategy:** The OT&E of technologically complex warfighting systems requires our T&E workforce to have a tremendous amount of deep and broad cutting-edge expertise. The rapid rate of technological evolution across many technical disciplines requires advanced government workforce training and unparalleled partnerships with academia, National Laboratories, and industry to develop and

validate solutions to the DoW's most immediate warfighting and T&E challenges.

CONCLUSION

The rapid fielding of new capability and integration of advanced technologies remain top priorities for the SecWar. DOT&E plays a key role in realizing this objective. DOT&E will continue to work with and support the T&E enterprise to adapt and accelerate rigorous T&E of combat system operational capability and resilience, so that warfighters are equipped to manage risk on the battlefield and prepared to employ those systems effectively and decisively in combat.

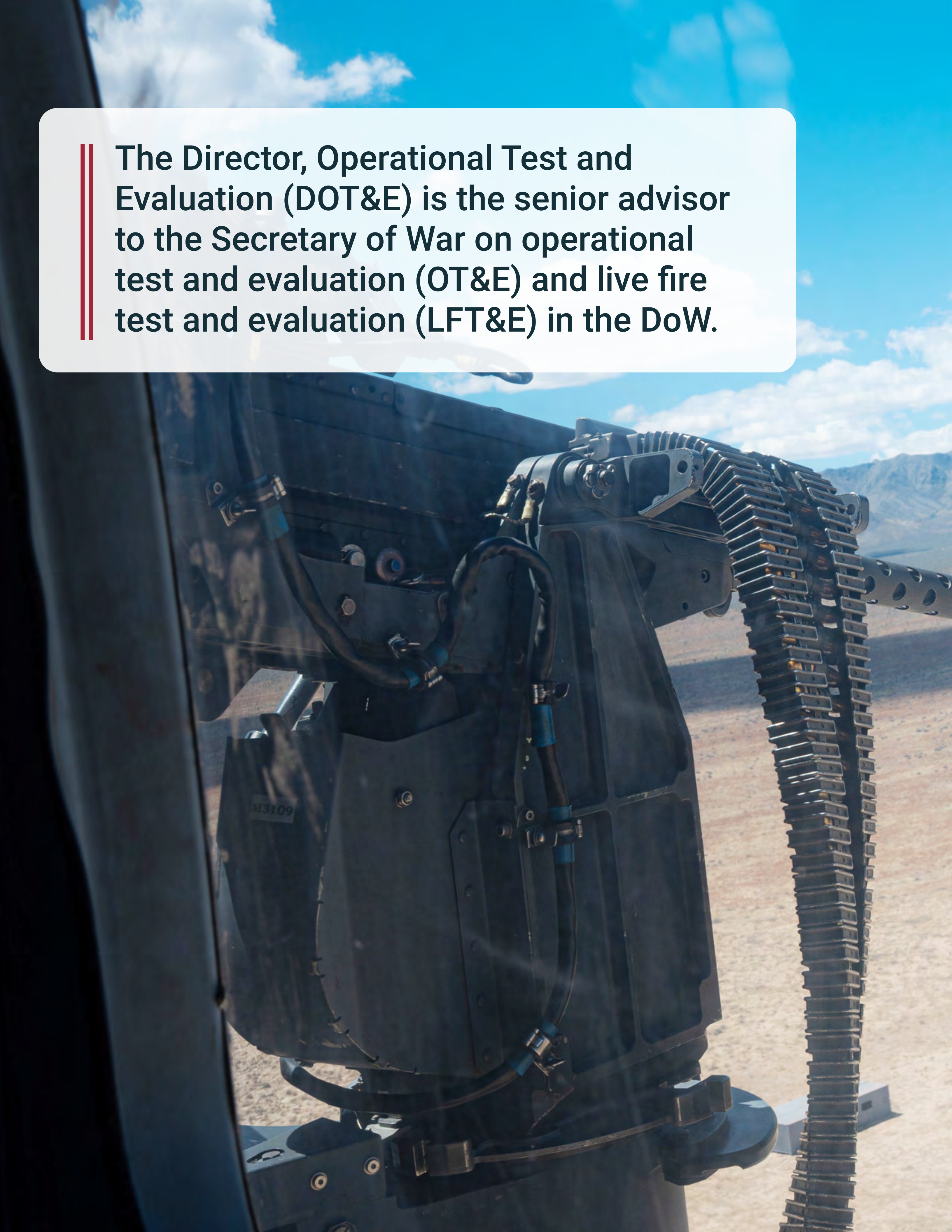
It has been an honor and a privilege to perform the duties of the Director. Consistent with our statutory obligations, DOT&E has maintained its objectivity and independence, continuing the practice of providing factual ground truth to Congress, the SecWar, other DoW leaders, and warfighters. DOT&E is grateful to our partners in the DoW and Congress for their continued support. Finally, I wanted to extend my sincerest thanks to the DOT&E staff for their professionalism and dedication to the mission this past year.

Carroll P. Quade
Director (PTDO)

CONTENTS

CONTENTS

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



DOT&E'S MISSION

- Enable adequate OT&E and LFT&E of DoW weapon systems in operationally representative and relevant conditions to support credible evaluation of the operational effectiveness, suitability, survivability, and lethality of DoW 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 War. 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, DoW Directives, and DoW Instructions.[1] DoDD 5141.02 assigns the following, critical DoW programs and activities to DOT&E:

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

1 Throughout this Annual Report, references to historical decision makers, documents, and programs use the titles from that time, including "DoD."

This page intentionally left blank.

EXECUTIVE SUMMARY

This page intentionally left blank.

MAJOR PRODUCTS

In FY25, DOT&E reviewed the programs on the T&E Oversight List for OT&E and/or LFT&E, using the criteria below, to assess if programs should be removed from oversight. In addition, this review resulted in some programs on the lists being consolidated to more accurately reflect how DOT&E was executing oversight; some programs being removed from OT&E oversight but not LFT&E oversight; and clarification in regard to the specific programs that are on oversight.

Criteria for being on the T&E Oversight List:

- Program exceeds or has the potential to exceed the dollar value threshold for a major program, to include major defense acquisition programs (MDAPs), designated major subprograms, highly classified programs, and pre-MDAPS.
- Program has a high level of congressional or DoW interest.
- Weapons, equipment, or munitions that provide or enable a critical mission warfighting capability or are a militarily significant change to a weapon system.

As of September 30, 2025, DOT&E had 173 DoW 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 FY25, DOT&E:

- Approved 28 T&E Strategies/TEMPs and disapproved 1 TEMP.
- Approved 87 individual test plans.
- Published 43 reports, including 28 reports to the Services, Congress, and/or the SecWar providing system evaluations, a classified annual assessment of the Missile Defense System, and 14 special or legislative reports.

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

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

Source	Title	Status
	FY24 NDAA	
Conference Report Sec. 1507	Review and Plan Relating to Cyber Red Teams of the Department of Defense	Complete
Conference Report Sec. 1686	Actions to Address Serious Deficiencies in Electronic Protection of Systems that Operate in The Radio Frequency Spectrum	Complete
	FY25 NDAA	
JES Page 438	Organization and Codification of Provisions of Law Relating to Missile Defense	Complete
	FY25 Other Legislative Actions	
SASC Report	Testing for Artificial Intelligence System Survivability	Complete
SAC Report	Joint Fires Network (Semi-Annual Submission #1 of 2)	Complete
SAC Report	Joint Fires Network (Semi-Annual Submission #2 of 2)	Complete

Acronyms: JES – Joint Explanatory Statement; NDAA – National Defense Authorization Act; SAC – Senate Appropriations Committee; SASC – Senate Armed Services Committee

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

Source	Title	Status
	FY25 NDAA	
JES Page 844	Pilot Program on Establishment of a Test and Evaluation Cell Within the Defense Innovation Unit (DIU)	In Progress (DIU is OPR; DOT&E reviewed and provided input to DIU's draft report in April 2025)
	FY25 Other Legislative Actions	
SASC Report	Consideration of Installation Infrastructure and Other Supporting Resources by Department of Defense Test Resource Management Center	Completed by OUSW(R&E)
SASC Report	Modeling and Simulation in Relation to the Fragmentation Rapid Analysis Generator Using Computed Tomography	Completed by the Army
HASC Report	Assessing the Army's Capabilities for Automating Data Collection in Arena Testing	Completed by the Army

Acronyms: HASC – House Armed Services Committee; JES – Joint Explanatory Statement; NDAA – National Defense Authorization Act; OUSW(R&E) – Office of the Under Secretary of War for Research and Engineering; SASC – Senate Armed Services Committee

OT&E AND LFT&E OVERSIGHT OF DOW SYSTEMS

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

TEMP, T&E Strategy, and Test Plan Recommendation Trends

In FY25, DOT&E evaluated the adequacy of TEMPs, T&E Strategies, 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, validation, and accreditation (VV&A) of modeling and simulation (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 FY25, DOT&E approved all but one test plan and one TEMP. The disapprovals were the result of insufficient resources available to support M&S VV&A that is required to conduct adequate operational assessment. DOT&E commonly approved documents with caveats. Common DOT&E conditions for document approval include: (1) testing all intended system capabilities, (2) insufficient resources or planned test events, (3) M&S VV&A plans, (4) incomplete survivability plans that cover the full system-of-systems architecture and non-kinetic threat space, and (5) insufficient coverage of the operational environment, to include arctic and tropical environments.

Test Adequacy Recommendation Trends

In FY25 reports, DOT&E assessed the adequacy of OT&E and/or LFT&E performed in 26 system evaluations. DOT&E assessed 62 percent (16 of 26) of testing as adequate, 23 percent (6 of 26) as partially adequate, and 15 percent (4 of 26) as not adequate. As shown in Figure 1, FY25 test adequacy assessments are comparable to the last 9 years (FY16 – 24).

The determinations of inadequacy or partial adequacy of OT&E and LFT&E in FY25 were caused by: (1) lack of operational testing prior to early fielding, (2) tested systems not being representative of fielded systems, (3) execution shortfalls, (4) inadequate M&S, (5) insufficient data to conduct rigorous analysis, and/or (6) lack of operationally realistic testing due to range or instrumentation limitations. DOT&E also highlighted limitations discovered in testing or in post-test analysis, including but not limited to:

- Unrealistic operational conditions due to range or test instrumentation limitations
- Safety restrictions
- Networks or sub-systems off-limits to cyber testing
- Lack of operational context in developmental testing
- Kinetic vulnerability models or inputs do not model some vulnerability modes

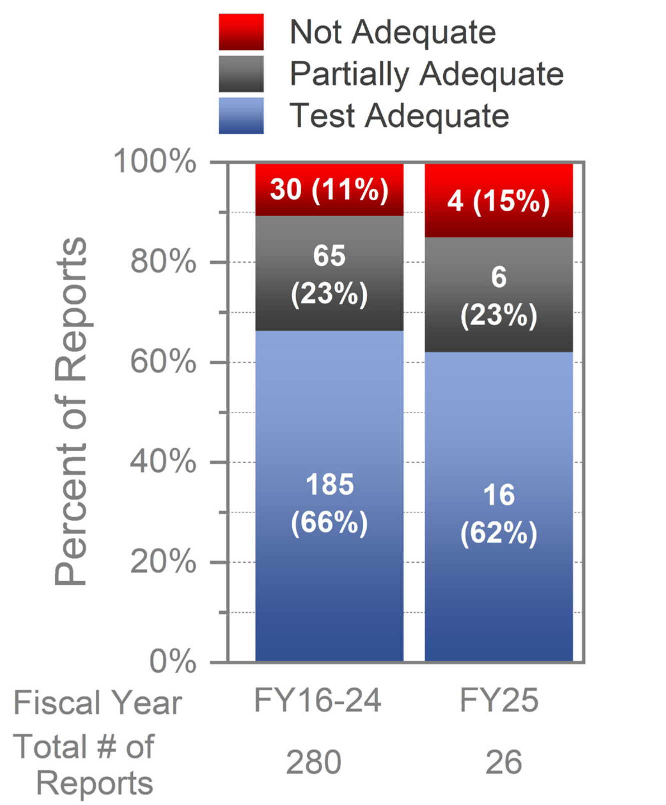


Figure 1. Test Adequacy in FY25 and Prior Years

- Models and model inputs not validated or not operationally realistic
- Insufficient data to conduct a quality evaluation
- Did not test all operational use cases

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

- Completing testing with hardware and software intended for fielding
- Collecting suitability and cyber data during sustainment to monitor changes in suitability and survivability
- Resourcing test ranges to allow execution and data collection of realistic operational missions against realistic threats
- Conducting cyber assessments of software factories and relevant supply-chains
- 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.
- Developing robust and independent VV&A for all M&S for use in OT&E and LFT&E

» PROVIDED INDEPENDENT EVALUATION OF OPERATIONAL PERFORMANCE

In FY25, DOT&E published 28 independent system evaluation reports on the operational performance of the system. In 10 of those reports, DOT&E was unable to assess operational effectiveness, operational suitability, and/or survivability from early fielding and early operational testing because there was not enough data available to make full operational assessments. In those cases, DOT&E's reports comment on progress towards operational effectiveness, operational suitability, and survivability. In eight of the system evaluation reports, DOT&E did not plan on evaluating effectiveness, suitability, and/or survivability because the performance element was evaluated in previous reports or was out of scope. The performance trends, discussed below, are depicted in Figure 2.

Operational Effectiveness Trends

In FY25 system evaluation reports, DOT&E was able to assess operational effectiveness of 11 systems. Of those 11 evaluated systems, DOT&E reported 36 percent (4 of 11) as operationally effective. By comparison, over the last 9 years (FY16 – 24), DOT&E reported 53 percent (89 of 167) as operationally effective. In FY25, DOT&E assessed three programs as not operationally effective and four programs as being partially effective because the system either could not complete one or more of its primary missions, had poor reliability reducing effectiveness, or had poor operational effectiveness in some operationally relevant conditions against intended threats and targets.

Operational Suitability Trends

In FY25, DOT&E was able to assess operational suitability of 13 systems. Of those 13 evaluated systems, DOT&E reported 23 percent (3 of 13) as operationally suitable. By comparison, over the last 9 years, DOT&E reported 48 percent (77 of 159) as operationally suitable. DOT&E assessed eight programs as not operationally suitable and two programs as being partially operationally suitable. These 10 programs experienced shortfalls in hardware and software reliability and availability, safety issues, and training.

Survivability Trends

In FY25, DOT&E assessed survivability for 12 systems reports. Of those 12 evaluated programs, DOT&E reported 50 percent (6 of 12) were survivable. By comparison, over the last 9 years, DOT&E assessed 30 percent (40 of 132) as survivable. DOT&E assessed four programs as not survivable, and two as partially survivable, primarily due to vulnerabilities in contested cyberspace. Cyber threats remain the most common non-kinetic threat type tested against in comparison to testing against electromagnetic spectrum; or chemical, biological, radiological, and nuclear (CBRN) threats in OT&E and LFT&E.

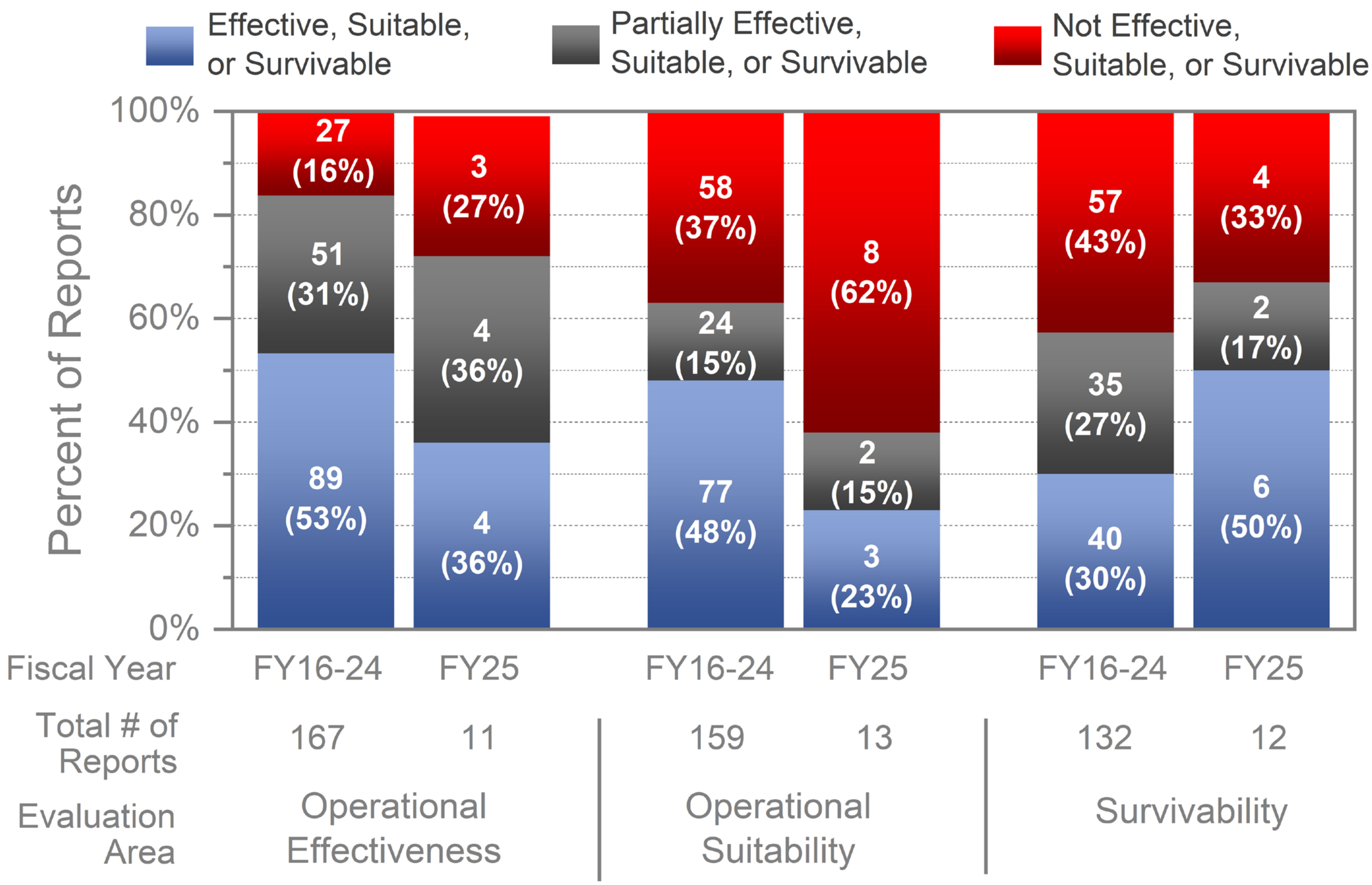


Figure 2. Operational Performance Trends in FY25 and Prior Years

Recommendations Trends

DOT&E reports include practical recommendations to fix the identified deficiencies and improve the operational performance of the DoW 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.

This page intentionally left blank.

TEST AND EVALUATION RESOURCES

This page intentionally left blank.

Test and Evaluation Resources

DOT&E is required to assess the adequacy of operational and live fire testing conducted for programs under oversight, and to include comments and recommendations on resources and facilities (infrastructure) available for OT&E and LFT&E and on levels of funding made available for these activities. DOT&E monitors and reviews T&E strategies, investment programs, and resource management decisions to ensure capabilities necessary for realistic operational tests are supported. This report highlights general areas of concern in testing current systems and discusses significant issues, DOT&E recommendations, and T&E resource and infrastructure needs to support OT&E and LFT&E.

The DoW's T&E infrastructure is an enabler for validating systems in realistic operational environments, strengthening deterrence and supporting a lethal force. Deficiencies in T&E resources compromise the Department's capacity to test and field effective, lethal, and operationally resilient warfighting systems.

In collaboration with the Services, Agencies, and OUSW(R&E), DOT&E is working to modernize T&E infrastructure to ensure ranges, facilities, instrumentation, threat surrogates, and test environments reflect the realities of multi-domain combat against kinetic and non-kinetic threats. Specifically, the DoW must address test capability gaps related to long-range fires, air and missile defense, cyber, electromagnetic spectrum (EMS) warfare, unmanned systems, and space capabilities. And because live testing is constrained by range safety, security, cost, and logistics, those investments must include rigorous verification, validation, and accreditation of modeling, simulation, and digital-test capabilities that can augment live events and deliver credible results.

The T&E workforce must embody the warrior mindset — trained, ready, accountable, and centered on mission success. The Department must invest in recruiting, training, and retaining talented individuals — especially in domains such as space, cyberspace operations, software engineering, data analytics, and artificial intelligence (AI) — and equip them to support a lethal and ready force. A robust T&E enterprise — backed by modern infrastructure and staffed by warrior-minded professionals — is essential to ensuring our systems are proven, resilient, and ready to deter or decisively defeat any adversary.

RANGE INFRASTRUCTURE MODERNIZATION

The statutory T&E mandate to assess system performance requires live, open-air ranges and laboratories that are rapidly configurable to different operational scenarios, support complex multi-domain missions, and connect via secure networks. Test ranges should emulate current and future blue and red system capabilities, tactics, threat laydowns, scenarios, and operating spaces to characterize performance of systems under test. The current open-air range space should be increased and better integrated to support system-of-systems assessments of air, land, and sea combat systems with capability for emerging long-range fires, hypersonic missiles, EMS warfare, unmanned systems, nuclear effects, and directed energy (DE) weapons. Lastly, DOT&E intends to work with the Services, Agencies, and the Test Resource Management Center (TRMC) to resource and develop persistent, scalable enterprise capabilities that can be accredited for use by all stakeholders across the DoW.

» OPEN-AIR RANGES AND CORRIDORS

- To close gaps in the ability to test long-range, network enabled, coordinated kinetic and non-kinetic kill chains, the DoW requires operationally representative command and control networks, to connect blue sensors to shooters across domains, networks, and classifications in any combination of live, recorded, and/or modeling and simulation (M&S) to support complex, coordinated mission scenarios involving air, land, sea, spectrum, cyber, and space systems. DOT&E supports the Joint Mission Environment Test Capability program's work to build out the network infrastructure to support operations across integrated test ranges, and wide area off-range exercises and experimentation events.

- The DoW needs to invest in and coordinate expanding and connecting the airspace available to the open-air ranges enabling testing and training of advanced capabilities. Threat systems and our own capabilities far exceed the current available air space on the open-air ranges. The ranges need support and assistance to coordinate additional airspace and corridors with the FAA and industry. Expanding and connecting range air space is necessary to facilitate testing and training critical long-range capabilities that our warfighters need and to replicate the threats they will face.
- To better understand how unmanned systems affect DoW warfighting missions, DoW ranges – in coordination with the Services and TRMC – should invest in enterprise-level resources that enable persistent and continuously updated surrogates and test environments capable of operating multi-system configurations in safe spaces with spectrum allocation and instrumentation to capture data on mission effects.
- To test missiles with longer ranges and gather data to support simulation validation, including for hypersonic missiles, the DoW should invest in long-range, overland missile flight test corridors with land-based impact areas and mobile hypersonic-specific range instrumentation to produce the required lethality data against threat-representative targets for terminal area assessments.
- To support nuclear modernization programs, the DoW requires upgrades to critical T&E infrastructure with test chambers at proper classification levels to support development and testing of the various nuclear effects as associated with DoD Instruction 3150.09, "Chemical, Biological, Radiological, and Nuclear Survivability."

» ENABLERS AND INSTRUMENTATION

- To improve Open-Air Battle Shaping (OABS) and the ability to provide real-time integration of live aircraft and ground threat systems with modeled weapon performance, the Services and TRMC should continue to invest in improvements to ensure pertinent data across the domain is available to OABS. Specifically, they need to ensure additional aircraft, advanced sensing systems, ground systems, threat systems, surface vessels, and autonomous systems are integrated with their real-time data to enable testing advanced weapon engagements. The Services and TRMC also need to support the procurement of additional weapon models, updates to existing models, and the improvement of virtual threat insertion such as Link-Inject-to-Live (LITL) and Synthetic-Inject-to-Live (SITL). They also must support furthering the modeling of electronic warfare, modeling electronic attack (EA), and advancing kill/survival determination methodologies as weapon capabilities and computer processing power evolves.
- To improve consistent collection of Time, Space, and Position Information and bus data across each mission – regardless of range, platform, or weapon – the DoW should invest in multi-source data collection methods and data collection tools that make it possible to reconstruct ground truth for assessments of operational effectiveness.
- To improve operational testing of EMS-dependent systems on open-air ranges, the DoW should invest in mobile radio frequency (RF) collection instrumentation that can be sited with ground-based radar, communications, and jamming systems to capture truth data for the signals emitted by these systems to reconstruct during analysis the many RF signals present in a test.
- To improve replication of peer radar and threat radar, GPS, and data link jammer capabilities in operational testing of EMS-dependent systems, the DoW should invest in a greater number and variety of RF emitters and surrogate systems to represent a modern threat environment with realistic signal density and congestion.

- To replicate the air defenses of peer-level adversaries that involve kinetic defenses, EA defenses, and DE point defense weapons, the DoW requires additional investment in threat EA and DE systems and radar test assets capable of high-fidelity emulation of signal detection. DoW ranges should invest in high fidelity, rapidly reprogrammable, open-air threat emulation systems; and upgrade current high-fidelity systems, like the Radar Signal Emulator systems, to provide greater flexibility and fidelity. For each threat system, test ranges should have sufficient numbers of moveable high-fidelity surrogate shells to physically represent the threat system vehicle types accurately with reflectivity properties; coatings; and camouflage, concealment, and decoy items typical of those employed by threat operators.
- To safely test high-energy laser (HEL) weapon systems in realistic combat conditions, the DoW must outfit test and training ranges with HEL-specific safety equipment to conduct open-air, self- and area-defense test scenarios. Radar, infrared (IR) and electro-optical (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. DOT&E supports the Army's White Sands Missile Range's requirement to upgrade its HEL Systems Test Facility.
- To assess capabilities for cyberspace operators to monitor activity, issue orders, and engage across the spectrum of friendly, neutral, and adversary cyberspace, including those that are part of the Joint Cyber Warfighting Architecture, the DoW requires ranges with neutral and malicious traffic and scenario generation capabilities. The Department also may consider using digital copies of cyber operational force systems to support OT&E while the primary systems support real-world operations.
- To replace the Pacific Tracker and Pacific Collector missile range instrumentation ships that are nearing end-of-life and essential for flight tests of all Missile Defense Agency (MDA) programs and other missiles, MDA was appropriated $530M in funding in FY25 that will fund a Pacific Collector replacement, and partially fund that ship's radar and a Pacific Tracker replacement. DOT&E is tracking that MDA's current acquisition plan calls for the Pacific Collector replacement to achieve full operational capability in FY30, and for the Pacific Tracker replacement to achieve full operational capability in FY31.

THREAT AND TARGET REPRESENTATION

The T&E community must accurately characterize the performance of systems under test against representative threat scenarios and threat surrogates of representative physical size, quantity, and capability. The DoW requires substantial intelligence and resources to enable the T&E community to keep pace with the rapid development of adversary capabilities and with the increasing numbers and growing variety of weapons systems that adversaries are bringing to bear.

» AIR

- To perform open-air, mission-level operational test trials of aircraft and anti-aircraft systems, the DoW needs a sufficient number of peer-level adversary aggressor aircraft with sufficient active and passive EMS capabilities to represent threat fighter aircraft. These threat 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 EO and IR sensors and communications data links, and data recording instrumentation to satisfy T&E analysis requirements.
- To assess lethality of live weapons and validate models for end-to-end effectiveness, the DoW should invest in threat surrogate full-scale targets. Surrogate targets are required for fourth-, fifth-, and sixth-generation threat fighter aircraft, large bomber and mobility aircraft, helicopters, and others with comparable sizes and signatures to the threat aircraft they need to represent.
- To support T&E of air defense sensors and systems, the Army lacks organic fighter aircraft to serve as threat surrogates for evaluating target tracking, identification, and electronic protection capabilities. Previous assets have been relocated and are no longer available, creating a need for fixed-wing support from the other Services

through agreements and during large test events for Integrated Fires Test Campaigns.

- To address a broader range of hypersonic threat surrogates in OT&E and for verification and validation of M&S, the Navy and MDA will require increasingly sophisticated hypersonic threat surrogates that can represent the full range of hypersonic speeds and cross-range and terminal maneuvers. DOT&E is aware that the MDA is developing Aegis Sea-Based Terminal and Glide Phase Intercept capabilities and, for the first time, flew a hypersonic target in a flight mission in FY25.
- To perform adequate OT&E of supersonic and subsonic missile defense combat systems requires improved aerial targets. The Navy's supersonic aerial target, the GQM-163, requires the ability to fly evasive maneuver flight trajectories representative of supersonic anti-ship cruise missile threats, the aggressive diving profiles of some anti-ship cruise missiles, and the ability to fly greater ranges. The Navy's BQM-177 subsonic aerial target and the GQM-163 require advanced electronic warfare payloads to correctly emulate threats and to induce operationally realistic responses from the combat system. The Navy also requires the ability to test against a threat with flight profiles of hybrid anti-ship cruise missile threats, which transition from subsonic to supersonic flight. DOT&E is aware that for the GQM-163, the Navy is investigating ways to improve the kinematic performance of the vehicle and is working to integrate some improved electronic attack (EA) payloads. DOT&E is also aware that the Navy is working to incorporate the Filthy Buzzard EA payload into the BQM-177 subsonic target which should improve its ability to emulate certain threats.
- To assess Navy shipboard self-defense HEL systems in open-air tests, the Navy will require accredited threat surrogates for anti-ship cruise missiles and swarming unmanned airborne and surface vehicles.

» SEA

- To properly evaluate torpedoes and antisubmarine warfare capabilities, the Navy needs a mobile target that can accurately represent a diesel-electric submarine.
- To accurately determine and maximize torpedo performance against threat submarines, the Navy needs static and mobile submarine-launched countermeasure surrogates that can emulate threat capabilities.
- To execute set-to-hit testing of torpedoes, the Navy needs to evaluate lethality and effectiveness against threat submarines employing full evasion capability. DOT&E is aware that 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.
- To determine the ability of Navy ships and combat systems to defend themselves against anti-ship cruise missile attack, the Navy has traditionally used the unmanned Self-Defense Test Ship (SDTS) for close-in self-defense evaluation. With the current SDTS approaching the end of its service life, the Navy will require a replacement for the SDTS capability to support future test programs, including Aegis Modernization and the Integrated Combat System.

» LAND

- To assess end-to-end effectiveness and vulnerability of airborne platforms to DE threats, the DoW requires test ranges with surrogate systems capable of replicating peer threat capabilities for tactical lasers, high-power microwave, and ultra-wideband DE point defenses.

» SPACE

- To increase resilience of space operations, communication, and missile defense programs, the DoW requires adequate OT&E of satellite systems. High-end advanced training, testing and threat replication activities need high-fidelity space-based threat surrogates in low earth orbit, medium earth orbit, and geo-stationary earth orbit. To collect data on the resilience of space systems, a variety of on-orbit and ground-based sensors are required to feed a range control system that will be used to analyze the data and provide corrective direction for systems going by, through, or to the space domain. In order to maintain the safety of our critical orbits, these sensors should include both on-orbit and ground-based EO radar and

IR systems. This Service-retained orbital range will also require the organic ability to command and control its own assets in order to ensure continued and uninterrupted operations of force-presented assets.

- 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 need mission simulators and simultaneous reproductions of the natural and man-made environments.

» CYBER

- To create operationally realistic attack surfaces for testing cyberspace effects and enabling capabilities per DoD Instruction O-3600.03, "Test and Evaluation of Cyberspace Effects and Enabling Capabilities," additional investments are required in target representative networks, threat surrogates, and opposing force emulation.

MODELING, SIMULATION, AND DIGITAL ENGINEERING

As the capabilities of adversary systems become more complex and systems performance cannot be demonstrated in an open-air environment for operational, cost, or security reasons, the DoW must continue to develop and maintain validated models and environments with the fidelity required for developmental and operational testing. The rate of weapons system development by peer-competitor adversaries is currently faster than the development pace of validated, high-fidelity models. As a complement to live testing of physical systems, there is increased effort in the DoW to pursue digital and laboratory M&S solutions that represent current capabilities of systems under test and of the threats they need to be tested against in joint environments.

» M&S

- To evaluate the effectiveness of integrated air defense systems, the DoW requires an integrated, 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.
- To allow quantitative assessments of the effectiveness of integrated hypersonic and ballistic missile defense system and account for safety and cost limitations, the MDA needs to develop a system-level, high-fidelity digital modeling venue. DOT&E is aware that funding for the End-to-End Digital Integrated System-level Simulation was terminated in FY24 but still supports the need for developing this capability.
- To address limitations in open-air range infrastructure, the Navy and Air Force should update current representations and environments and incorporate additional weapon systems into the Joint Simulation Environment (JSE) to enable testing and training that cannot currently be conducted on the DoW'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. JSE also needs to support representation of advanced cyber threats against the blue force to incorporate cyber effects into its battlespace emulation.
- To accelerate development and assessment of autonomous systems, the DoW should invest in credible synthetic range capability that supports hardware-in-the-loop and software-in-the- loop evaluation within operationally representative conditions.
- To support operational performance assessments for ship combat systems, EW suites, and ship missile systems, the Navy needs validated M&S of anti-ship missile and launch platform radar models. Recent shipboard EW programs had only two intelligence-community validated threat models available for operational test.
- To assess survivability and resilience against cyber, EMS and other non-kinetic effects, these effects must be incorporated into the accredited simulation environments being built for long-range kill chain and other performance evaluation purposes.
- To assess vulnerability and recoverability against multiple effectors, M&S suites should be improved to allow for sequential attacks.

» DIGITAL ENGINEERING AND DATA

- To enable automated and real-time data collection, reduction, and analysis the T&E enterprise will require robust data infrastructure (big data analytics and large knowledge management systems), as well as system and platform agnostic data collection tools to improve the quality, speed, and depth of post-mission data processing.
- To address acquisition reforms requirements to field faster and identify the most pressing operational gaps, the DoW requires the ability to connect mission engineering, systems engineering, and T&E data across program and capability life cycles. DOT&E is collaborating with TRMC to align its reference architecture with OT&E and LFT&E needs.
- To share information and jointly develop tactics, techniques, and procedures at all necessary classification levels, assessment teams require joint digital collaboration environments. DOT&E is aware of work at TRMC and within the Services to build digital ecosystems that make some digital tools available across the T&E enterprise.

WORKFORCE

- To understand the impact of recent T&E workforce reductions, DOT&E plans to study the makeup of the Department's current T&E workforce to understand expertise gaps in high-priority warfighting domains and emerging technology.
- To collect, integrate, store, reduce, and analyze enough data to quantify performance and risk of AI-enabled systems, workforce expertise in software integration and data analytics are needed.
- To meet increasing demand for adversarial cyber testing to assess cyber survivability and resilience, the DoW requires additional trained operational test personnel, DoW Cyber Assessment Teams (DCAT), and DoW Cyber Red Teams (DCRTs) to act as aggressors. DoW cyber teams must be fully staffed and trained on emerging cyber threat tactics, techniques, and procedures.
- To improve the DoW's ability to defend against advanced nation-state cyber threats, cyber test teams require additional expertise in several technology areas, including cloud systems; networks using non-traditional protocols; systems that exchange vital mission data via RF interfaces; and AI and machine learning-based approaches to cyberspace attack and defense.
- To perform adequate OT&E of new space systems and technologies, the Space Force requires experienced T&E personnel and funding to operate test assets, analyze data, conduct tests, and perform accreditation of threat M&S as operationally realistic for its intended purpose.

DOW PROGRAMS

This page intentionally left blank.

Aerosol Vapor Chemical Agent Detector (AVCAD)

The Aerosol Vapor Chemical Agent Detector (AVCAD) program has conducted all testing laid out in the DOT&E-approved Milestone C (MS C) TEMP. Since then, the program has implemented software and hardware changes to improve system performance. The program is conducting appropriate retesting, in accordance with DOT&E-approved test plans and TEMP. In July 2025, DOT&E removed the AVCAD program from oversight, because program development has stabilized and there are no significant upgrade activities remaining.

SYSTEM DESCRIPTION

The AVCAD is an aerosol and vapor chemical warfare agent (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 CWAs 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 OVERSIGHT HISTORY

AVCAD is a joint Acquisition Category III program that DOT&E put on oversight in July 2018. In April 2023, DOT&E published an operational assessment. In May 2023, the AVCAD program was authorized 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. The production and deployment phase of testing began in January 2024, with a full-rate production decision targeted for March 2026. The program completed a multi-Service operational test in August 2024, in accordance with the DOT&E-approved test plan but has yet to complete all retesting of AVCAD software and hardware upgrades necessary to provide an accurate evaluation at this time. DOT&E observed all completed testing, which was conducted in accordance with DOT&E-approved test plans.

To improve system performance and reliability, the program office worked with the vendor to update software algorithms for better detection and fewer false alarms and installed a heat sink with user interface warnings to mitigate overheating. The program office also upgraded hardware for electromagnetic environments; improved cleaning tools, preventative maintenance checks, and services procedures; and documented them in an updated technical manual. The program will conduct a Soldier Touchpoint in 1QFY26 to verify the aforementioned updates. In July 2025, DOT&E removed the AVCAD program from oversight because program development has stabilized and there are no significant upgrade activities remaining.

Digital Modernization (DM)-Related Enterprise Information Technology (IT) Initiatives

The DoW Information Enterprise Portfolio Management, Modernization, and Capabilities (PM2C) Council continues to govern aspects of the Department's information enterprise, including the Joint Warfighting Cloud Capability (JWCC) oversight and cloud rationalization initiative. The DoD Chief Information Officer (CIO) published *Fulcrum: The Department of Defense (DoD) Information Technology (IT) Advancement Strategy*, in June 2024. The Fulcrum Strategy advances Digital Modernization (DM).

The DoW CIO, Defense Information Systems Agency (DISA), and Services have been implementing programs, projects, and initiatives intended to achieve DoW DM objectives. Many DM initiatives lack an overarching systems integration process, test strategy, and program executive organization to manage cost, drive schedules, and monitor performance. Deploying untested programs, projects, and initiatives poses an operational risk to the DoW enterprise, particularly in a cyber-contested environment. Future deployment decisions must be informed by adequate OT&E.

SYSTEM DESCRIPTION

DoW DM 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 DoW DM efforts are intended to:

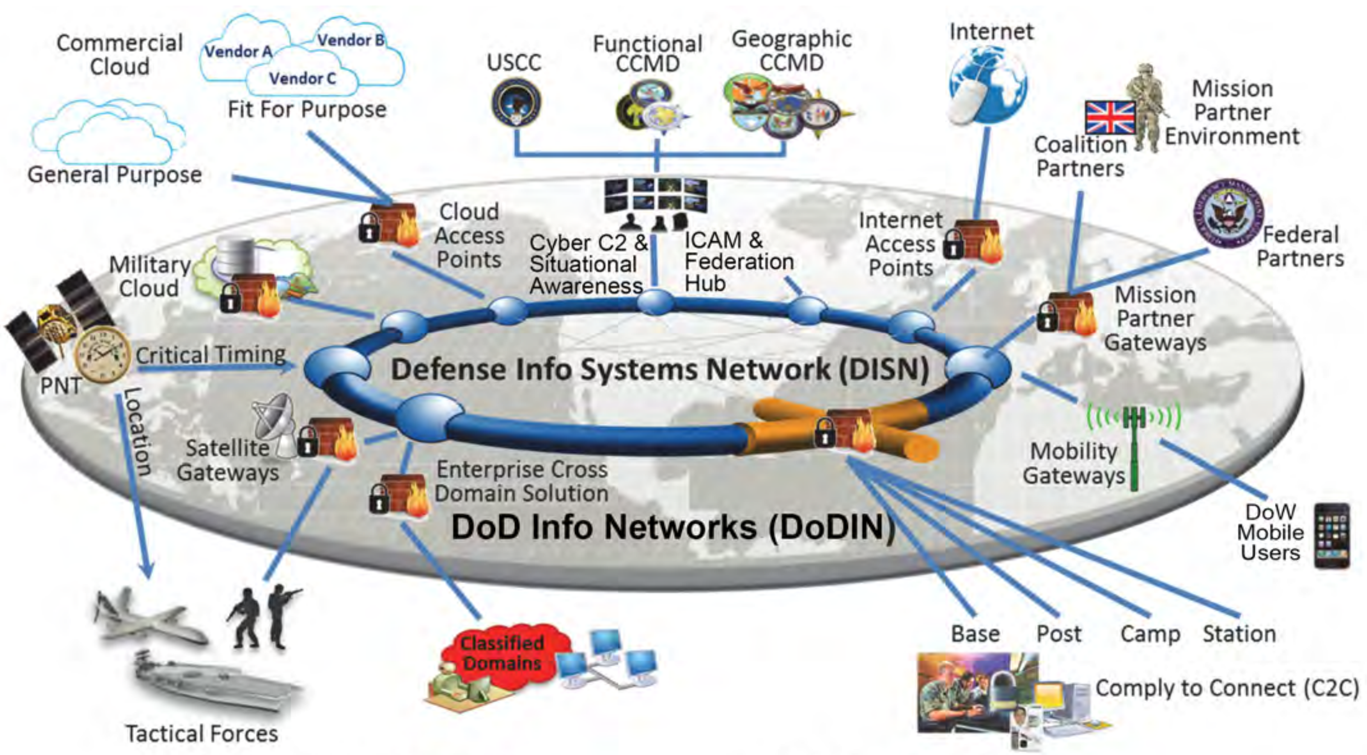
- Optimize DoW office productivity and collaboration capabilities, e.g., Enterprise Collaboration and Productivity Services (ECAPS) Capability Set 1 - Defense Enterprise

Office Solution (DEOS) via Microsoft Office 365 (O365) on NIPRNet, SIPRNet, and tactical (Denied, Disrupted,, Intermittent, and Limited (DDIL)) networks; Capability Set 2 - Business Voice and Video; and Capability Set 3 - Assured Command and Control Voice and Video · Deploy, adopt and integrate Identity, Credential, and Access Management (ICAM) capabilities to support Zero Trust and federated identity services using DoW-approved identity providers (IdPs) with the ICAM Federation Hub

- Transform the DoW cybersecurity architecture to implement Zero Trust throughout the DoW enterprise, including initiatives to provide endpoint security and to implement cyber-risk reporting, scoring standards, and compliance in continuous monitoring as required by law
- Sustain cybersecurity capabilities to protect the DoD Information Networks (DoDIN) and support defensive cyber operations and network operations
- Strengthen collaboration, international partnerships, and allied interoperability through a Mission Partner Environment (MPE)
- Unify DoW with a hybrid Secret ecosystem, underpinned by DISA enterprise IT services, to address the proliferation of independent Secret fabrics

PROGRAMS, PROJECTS, AND INITIATIVES

In June 2024, the DoD CIO published Fulcrum: *The DoD IT Advancement Strategy.* The Fulcrum Strategy advances DM. 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. In 2025, the DoD CIO designated the PM2C Council as the governance forum to manage the priorities outlined in the Fulcrum Strategy, track delivery, and focus on resource needs. By the end of FY27, achieving



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

target level Zero Trust across the DoW is a strategic imperative for Digital Modernization, bolstering data protection, enhancing mission resilience, and establishing a more adaptable and secure environment for future technological advancements.

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

DISA is the principal integrator for DoDIN enterprise capabilities, enabling initiatives, and testing. Many DM 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 DoW CIO, DISA, and Services intend to achieve DM objectives by implementing programs, projects, and initiatives, which currently include:

- **Enterprise Collaboration and Productivity Services (ECAPS):** In FY25, the DEOS Program Management Office (PMO) continued efforts to provide commercial cloud-hosted NIPRNet (known as DoD365-Joint) and SIPRNet office productivity and collaboration capabilities (known as DoD365-Sec) with cyber testing support provided by the Joint Interoperability Test Command (JITC). The DEOS PMO began to develop a classified collaboration capability for Australia, the United Kingdom, and the United States (AUKUS), with testing support provided by JITC.

  In FY25, 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 FY26. In FY25, DISA continued efforts to provide DIPS to OCONUS DoW users with non-U.S. telephone numbers. DISA intends to deploy the OCONUS DIPS in FY26. The DoW has yet to address Next Generation 911 dialing in DIPS, which is dependent on the DISA-led DoW-Emergency Services Internet Protocol Network (D-ESINet) effort to provide location-data transport.

  DISA is providing ECAPS Capability Set 2 (Business Video) on NIPRNet via DoD365 Teams. In FY25, the DoD CIO and DISA worked with the Services to investigate 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 FY25, DISA continued the GVS-C technical refresh, which is projected to complete in FY27.

- **Identity, Credential, and Access Management (ICAM):** The DoW CIO is the lead for ICAM governance for the DoW. The seven DoW CIO-approved NIPRNet ICAM solutions are Army, Navy, Air Force, Defense Logistics Agency (DLA), Defense Health Agency (DHA), National Geospatial Intelligence Agency (NGA), and DISA's DoD Enterprise ICAM (E-ICAM). The DoD CIO, in late September 2025, directed DLA to begin migrating applications to E-ICAM. DISA also has a SIPRNet E-ICAM solution. In FY25, the Department began unification efforts for classified IdPs identities, paired with federation hubs to address mission partner and Federal interoperability. By FY27, the DoW CIO-approved ICAM solutions must support Zero Trust activities and internal control requirements as defined by Federal financial management statutes and guidance. In FY24, DoD CIO and DISA shifted to a Federated approach for IdP, and DISA deployed a NIPRNet Federation Hub that provided identity brokering capabilities in FY25. DISA integrated the NIPRNet Federation Hub with the DoD E-ICAM, and the Army, Navy, and Air Force ICAMs in FY25. DISA intends to integrate the NIPRNet Federation Hub with DLA, DHA, and NGA ICAMs in FY26. Additionally, DISA intends to integrate Defense Human Resources Activity (DHRA) Enterprise Multi-Factor Authentication capability in FY26. DISA plans to deploy a SIPRNet Federation hub in

FY26. The FY24 NDAA required the Department to establish an ICAM acquisition program of record (POR). However, in accordance with the FY24 NDAA waiver process, the DoD CIO and DISA waived the task and did not establish an ICAM POR. In FY25, DISA continued integrating financial and other applications with the ICAM capabilities on NIPRNet that will continue through FY26. In FY26 and FY27, DISA intends to further integrate the NIPRNet and SIPRNet Federation Hubs with the Service and Agency ICAMs. A major part of the ICAM acquisition effort is the Public Key Infrastructure, detailed in a separate section of this Annual Report.

- **Mission Partner Environment (MPE):** In FY26, the Department intends to designate DISA as the lead component for MPE capabilities. The Air Force is working to sunset multiple facets of the Secret and Below Releasable Environment (SABRE) capability, and DISA intends to establish the Joint Operational Edge-Coalition Environment (JOE-CE) in FY26. Future MPE capabilities will leverage the current and next generation of DoW enterprise IT solutions.

TEST ADEQUACY

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

- **ECAPS:** DOT&E published a classified DoD365-Sec cyber test report from previous FY24 testing in December 2024. In August 2025, JITC conducted a cyber assessment of DoD365 Impact Level 5 capability (part of Capability Set 1). DOT&E was unable to observe the cyber assessment due to staffing shortages but will review the JITC report when published in FY26. In June 2025, the DISA PMO postponed the AUKUS early operational assessment (EOA) due to technical issues. In FY26, DISA and JITC intend to conduct the EOA to support an AUKUS minimum viable capability release. Separately, JITC also intends to conduct a cyber assessment of AUKUS in FY26. 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 FY25. DISA plans to deploy the SIPRNet Federation Hub in FY26. DISA does not intend to fund JITC to conduct NIPRNet and SIPRNet Federation Hub operational testing.
- **MPE:** Due to the MPE SABRE PMO transition from the Air Force to DISA, JITC paused all SABRE operational testing efforts in FY25.

PERFORMANCE

In FY25, except for the DoD365 Impact Level 5 cyber assessment, there was no operationally realistic testing performed on DM programs, projects, or initiatives, precluding an evaluation of their operational effectiveness, suitability, or cyber survivability.

RECOMMENDATIONS

As recommended in the FY24 Annual Report, the DoW CIO, Services, Director of DISA, and various DM governance forums should:

1. Manage DM initiatives with trained program managers and supporting offices.
2. Develop a TEMP or T&E Strategy for each funded DM enterprise IT initiative.
3. Fund JITC to fully support DM enterprise IT initiatives, testing, and test-related forums.
4. Perform threat representative cyber survivability testing of all DM enterprise IT programs, projects, and initiatives, in accordance with current DoW and DOT&E cyber survivability T&E guidance and policy, and use operational test data, analyses, and reporting to inform DM governance decisions.

DoD Healthcare Management System Modernization (DHMSM®)

DoD Healthcare Management System Modernization (DHMSM) consists primarily of MHS GENESIS, which is the DoW's electronic health record system that is now fully fielded to all major medical treatment facilities. In February 2025, DOT&E published an FOT&E report on the Revenue Cycle Expansion (RevX) subcomponent of MHS GENESIS based on operational testing conducted by the Joint Interoperability Test Command (JITC) in FY23. In the FOT&E report, DOT&E determined that RevX is partially operationally effective for basic patient registration, clinical documentation, and coding tasks, but is not operationally effective for the end-to-end billing process. DOT&E also determined that RevX is not operationally suitable because of poor usability and insufficient user training. In the period between the test execution and reporting, the DHMSM program management office (PMO) has addressed several of the findings and will execute an FOT&E event in FY26 to validate progress towards operational effectiveness and suitability.

DHMSM® and MHS GENESIS® are registered trademarks of the DHMSM PMO.

SYSTEM DESCRIPTION

MHS GENESIS is a modernized electronic health records system for the DoW, 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 all four organizations can utilize.

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 subcomponent of MHS GENESIS covers all revenue features, to include patient scheduling, registration, preauthorization, medical coding, claims submission, billing, and payment processing. It also introduces new capabilities and workflows to support patient accounting and billing.

MISSION

The DoW and other Federal Government medical staff use MHS GENESIS to manage delivery of healthcare within garrison facilities. DoW 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. The DHMSM PMO began deploying the RevX subcomponent of MHS GENESIS as part of its regular fielding activities for new waves of MHS GENESIS in September 2022. RevX is now operational at all major medical treatment facilities.

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) on MHS GENESIS and associated Defense Health Agency (DHA) infrastructure to help maintain and improve cyber survivability.

» 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

In February 2025, DOT&E published an FOT&E report following the operational test of the RevX subcomponent of MHS GENESIS from FY23. JITC conducted the test in accordance with the DOT&E-approved test plan, and DOT&E observed the test. DOT&E determined that the test was adequate to support its evaluation of the operational effectiveness and suitability of the RevX elements that users actively utilized during the event. JITC could not collect data on claims tasks because users were still clearing a backlog of claims from the legacy system. JITC could also not collect data on dental tasks because users were waiting on guidance from DHA before processing any dental claims. The test was not designed to evaluate cyber survivability because RevX is a subcomponent of MHS GENESIS, and its survivability cannot be evaluated separately.

PERFORMANCE

» EFFECTIVENESS

The RevX subcomponent of MHS GENESIS is partially operationally effective for basic patient registration, clinical documentation, and coding tasks but not operationally effective for the end-to-end billing process. Providers in most clinical areas could document care and medical coders could assign codes to patient encounters. However, the end-to-end billing workflow has systemic problems. Front desk staff could register patients, but they fail to capture some demographics and health plan information required for billing. This missing information creates downstream problems that require time-consuming manual remediation. RevX does not provide enough functionality for users to efficiently manage the claims requiring remediation.

» SUITABILITY

The RevX subcomponent of MHS GENESIS is not operationally suitable because of poor usability and insufficient user training. RevX training does not fully prepare users to accomplish their daily tasks. RevX adds responsibilities to front desk staff that they lacked adequate training on to complete, contributing to the large number of claims with incomplete information. DOT&E did not evaluate reliability, availability, or maintainability data, as RevX is a subcomponent of MHS GENESIS and cannot be evaluated separately.

» SURVIVABILITY

The RevX OT&E did not collect data to 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 to re-evaluate the operational effectiveness and suitability of MHS GENESIS, including RevX, with patient-facing components and performance at OCONUS sites, as recommended in the FY24 Annual Report.
2. Provide training to front desk staff that use RevX on check-in procedures to prevent incomplete or inaccurate data entry during patient registration and reduce the number of claims with errors.
3. Add capabilities to RevX to help users manage the claims requiring remediation.
4. Continue to fund and execute PCO on MHS GENESIS and its components.

The Director, DHA should:

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

F-35 Lightning II

Throughout FY25, the F-35 development effort continued to face challenges in delivering reliable, fully functional software to the operational test (OT) teams. The development teams focused on two software variations, one each for the Technology Refresh (TR)-2 and TR-3 hardware configurations. In spite of the TR-3 capability being a rehost of TR-2, the latest iteration of TR-3 software (40R02) was unsuitable for dedicated OT. Similarly, the latest version of TR-2 software (30R08) – intended to be the last version of software fielded on the TR-2 aircraft – was predominantly unusable for additional OT events during most of FY25, due to stability problems, shortfalls in capability, and on-going discovery of deficiencies. Dedicated OT with 30R08 software began in September 2025 when the OT squadrons participated in a large test exercise, GRAY FLAG 2025 with the latest version of 30R08 software. As such, no new combat capability was fielded in FY25.

The F-35 Joint Program Office (JPO) planned for needed modifications to OT aircraft, but resource shortfalls have not enabled timely delivery of these modifications. Current aircraft forecasts show that there will not be enough OT aircraft available to accomplish dedicated OT in representative formations of aircraft. Concerning the resources necessary to evaluate F-35 capabilities in the Joint Simulation Environment (JSE), the program has only one F-35 In-a-Box (FIAB) delivery contracted for after the 40S03 release next year, which DOT&E considers to be unacceptable. The JPO plans to put more FIABs on contract as the Block 4 configuration plan matures.

SYSTEM DESCRIPTION

The F-35 Lightning II 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, specifies required capabilities and associated capability gaps that drive incremental improvements under what is intended to be 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 Lightning II is an Acquisition Category ID program. IOT&E was completed in September 2023, and DOT&E published a combined IOT&E and LFT&E report in February 2024. The USD(A&S) approved full-rate production in March 2024, and 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.

Block 4 FOT&E is governed by the F-35 Overarching Block 4 TEMP and associated annexes, which are updated incrementally and include developmental testing (DT) and OT with aircraft in the TR-2 and TR-3 configurations. The F-35 Block 4 TEMP Increment 3 annexes were approved in November 2024. They include software upgrades (versions 40R02, 40R03, and 41R01) that add capability, including new Electromagnetic Warfare capability enabled by upgraded hardware on TR-3 aircraft starting in production lot 19. To ensure the program office planned and funded for adequate OT, DOT&E required an addendum to Annex 3, detailing the capabilities and OT requirements for software version 41R01. DOT&E approved the addendum in October 2025.

The TR-3 avionics upgrade, which includes upgraded main mission computers (referred to as integrated core processors), aircraft memory system, and panoramic cockpit displays, is a key enabler for new Block 4 mission systems capabilities. The TR-3 upgrade replaces the corresponding TR-2 components that are currently fielded in nearly the entire fleet of F-35 aircraft.

Problems with the TR-3 hardware and software during DT forced the program to delay delivery of the Lot 15 production aircraft until performance improved, resulting in these aircraft being put into storage. In an effort to stabilize the performance on the new TR-3 hardware, the program developed a truncated version of software by disabling some of the combat capabilities that had already been fielded on the TR-2 aircraft. The JPO, Services, and Lockheed Martin reached an agreement to start accepting TR-3 aircraft with the truncated software. No combat-capable TR-3 aircraft have been delivered to the U.S. Services to date. As of the end of September 2025, 158 F-35s had been delivered in the TR-3 configuration and a total of 812 aircraft (any configuration) have been produced and delivered to the U.S. Services.

» 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

DOT&E continues to have concerns about the ability of the United Operational Test Team (UOTT) – made up of members from the United States, the United Kingdom, and Australia – to conduct adequate testing of the Block 4 capabilities because of the reduced number of OT aircraft with the necessary hardware configurations and the required instrumentation to test mission systems and weapons integration. Effectively managing the multiple aircraft configurations is a challenge that requires a single, integrated master schedule. The program maintains an integrated test aircraft flow that maps software builds to test aircraft configuration, modification schedules and flight test instrumentation, including Open-Air Battle Shaping (OABS). Funding and contracting delays have made it difficult for the OT teams to have eight fully capable aircraft available for dedicated OT trials during the OT periods. Given OT aircraft availability rates, this generally means a total of 12 OT aircraft must be planned and funded to ensure 8 OT aircraft are available for most missions.

Block 4, TR-2 Open-Air Testing

The UOTT 30R08 OT plan, the latest and last planned TR-2 software version, governs the open-air 30R08 OT for all units assigned to the UOTT. The plan covers the open-air test events that can be conducted with various increments or developmental versions of the software. Capability test events (CTEs) in the plan 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 (30R08.XX) 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) in the plan 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. Dedicated OT missions are events that require full mission-level evaluations, assessing F-35 operational effectiveness in terms of lethality and survivability in mission scenarios, similar to 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. Dedicated OT events include variations in operational conditions, such as the number of threat and friendly airborne forces or the number and type of ground threat systems. Finally, dedicated weapon employment events, both captive carry (weapon test article flown, but not released) and live fire events, are included in the 30R08 OT plan.

DOT&E approved the test plan incrementally from February 2023 through August 2025, as the UOTT was able to conduct some portions of the test plan with the version of software delivered to the OT fleet. The UOTT issued a stop test order for OT of the 30R08 software in February 2024, citing critical Category I deficiencies and overall poor software stability. The UOTT issued a limited resume test notification to the program office in October 2024, and completed a GBU-54 weapon employment event, pictured at the beginning of this article. For the remainder of FY25, the UOTT primarily focused on assisting the DT effort by flying CTEs with interim versions of software, identifying and characterizing deficiencies and anomalies, and providing feedback to the contractor software development team. Dedicated OT for the TR-2 configuration began in September 2025 when the OT squadrons participated in a large test exercise, GRAY FLAG 2025.

Block 4, TR-3 Open-Air Testing

The UOTT continues planning for OT of the first TR-3 production configuration, which is now planned to commence with software version 40R03. Although the program developed two earlier versions of software for delivery to the field – 40R01 and 40R02 – the program office designated them as not suitable for conducting OT. The program's DT effort with the TR-3 aircraft and associated software remained significantly behind schedule throughout FY25. Aircraft modifications, flight test instrumentation, OABS capabilities, and stable software will all be required before dedicated OT can begin on TR-3 aircraft. Additionally, program funding constraints will make it difficult to plan for and accomplish adequate weapons testing with 40R03.

» BLOCK 4 – JSE

Following the completion of F-35 IOT&E test trials in the JSE at Patuxent River Naval Air Station, Maryland, in late FY23, program management of the JSE evolved to a larger enterprise to support future OT and training requirements. The organization of the JSE enterprise and the process by which it originates, prioritizes, funds, and implements requirements continue to evolve.

The next iteration of OT of the F-35 in the JSE will be based on the capabilities fielded with 30R08 software. The corresponding aircraft model in the JSE is the 30S08 FIAB. The JPO and the Naval Air Warfare Center Aircraft Division started integration of the 30S08 FIAB in the JSE site at Patuxent River in August 2024. They plan to deliver an initial capability in 1QFY26 that has undergone limited regression testing, but not verification and validation (V&V) needed to accredit for OT. 30S08 V&V activities are planned to continue through FY26, culminating in formal accreditation in early FY27. The UOTT is developing a test plan for conducting 30S08 mission-level trials in the JSE once it is accredited for OT. The UOTT intends to conduct the trials at one or a combination of the JSE sites at Patuxent River and the new Digital Test and Training Range – Nellis (DTTR-N) in Nevada. The Air Force planned to deliver an initial operational capability at the DTTR-N by 1QFY26 with up to 12 F-35 cockpits in the 30S02 configuration (same as that used for IOT&E in FY23) and 4 F-22 cockpits. The Air Force plans to complete 30S08 integration at the DTTR-N in FY26, in parallel with V&V and accreditation (VV&A) activities at Patuxent River, leading to an accreditation at both sites in 4QFY27. After testing in the JSE with 30S08, the program currently has plans to fund only two more FIAB releases during the initial Block 4 contract effort. Additional releases of FIAB will require new funding and additional contracting actions.

» SUITABILITY TESTING

DOT&E approved the latest iteration of the UOTT's F-35 Modernization Block 4 Suitability Test Plan in February 2025, with the caveat that the UOTT address shortfalls in the plan. The UOTT submitted an amendment to the plan in May 2025 to address the shortfalls, which DOT&E approved in July 2025. However, DOT&E remains concerned that no additional dynamic RCS measurement testing has been done on any variant by any of the Services since IOT&E. These measurements are necessary to assess the long-term health and performance of the low observable properties of the aircraft.

In 2026, the program plans to field a ground-based support system that would allow dynamic RCS measurements of operational aircraft by linking with ground station monitors. Without the ground station linkage, only a relatively small number of aircraft equipped with appropriate instrumentation can be measured.

» SURVIVABILITY TESTING

The F-35 Block 4 Cybersecurity Operational Test Plan (COTP) for FY25 included nine scheduled test events, of which only three were conducted. Planned FY25 test events slipped primarily due to attrition of the UOTT cyber survivability test team, which experienced a significant reduction of personnel in FY25. Additionally, funding priorities within the JPO limited testing opportunities. The deferred FY25 test events are being planned for FY26.

In FY25, the UOTT cyber team delivered the report for the FY24 cyber survivability assessment of line-replaceable unit supply chain refurbishment practices, a high interest area for the DoW and the F-35 program. All cyber survivability test activities were conducted in accordance with DOT&E-approved plans, and key events were observed by DOT&E.

Aircraft made available for cyber survivability testing have been permanently grounded assets. These assets are used for software development and thus limit the scope of cyber testing because of the potentially disruptive nature of cyber tests. More robust and representative aircraft cyber tests are needed, which will require Service and JPO investment in hardware- and software-in-the-loop capabilities. To address this need, the JPO designated a retired TR-2 mission systems DT aircraft (AF-3) to be available for dedicated cyber survivability testing. Transfer of the aircraft experienced delays in FY25 and is expected to be available for cyber testing in 1QFY26.

Candidates for cyber survivability testing are continually assessed for inclusion in updates to the COTP. Additionally, once cyber effects are characterized, 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.

PERFORMANCE

» EFFECTIVENESS

Block 4, TR-2 Development

The F-35 program continues to show no improvement in meeting schedule and performance timelines for developing and testing software, failing to deliver on the expectations of its agile development framework. The process of addressing deficiencies and adding new capabilities has stagnated as the current 30-series block of software has been undergoing a fly-fix-fly iterative development cycle for nearly four years, delivering a test-ready version of 30R08 to the UOTT at the end of FY25. Additional challenges added with the TR-3 avionics upgrades, both in development and testing, have caused continued 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 delivered 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.

Block 4, TR-2 Open-Air OT

Due to the lack of adequate testing on the 30R08 software, DOT&E is unable to assess its operational effectiveness. The UOTT has flown with immature versions of the 30R08 software to support DT assessments of capabilities and has participated in large force joint exercises to assess integration and interoperability with other aircraft. However, these tests are not adequate to evaluate effectiveness of the 30R08 capabilities in terms of combat lethality and survivability, in mission-level scenarios. The testing that the UOTT has been able to accomplish continues to lead to discovery of deficiencies. During FY25, the UOTT wrote 17 deficiency reports against

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

Comparison Parameters	Production Software Version		
	30R06	30R07	30R08
Software iterations planned	Four: 30R06.01, .02, .03, .04	Three: 30R07.01, .02, .03	Three: 30R08.01, .02, .03
Software iterations needed	Seven: 30R06.01, .02, .03, .031, .04, .041, .042	Eight: 30R07.01, .02, .03, .031, .033, .04, .041, .045	Thirteen (at least): 30R08.01, .02, .03, .04, .041, .051, .061, .062, .063, .064, .065, .066, .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	> 45 months
All planned capabilities delivered?	Yes	No	No

the performance of capabilities in the 30R08 software, many of which were against capabilities that were working in previous versions of software, an indication of inadequate integration and regression testing. Six of these reports were designated as Category I – the most severe level of deficiency. The program continues to face software stability issues that delay delivery of software needed to accomplish dedicated OT. The OT teams have observed improved stability in the most recent software version provided for testing.

Block 4, TR-3 Development

Although the program and Services have been accepting aircraft off the production line for over a year, including those that were placed in storage waiting for an acceptable version of software, no dedicated OT (i.e., in accordance with a DOT&E approved test plan) had been completed through the end of FY25 on the TR-3 aircraft in a production-representative configuration. DOT&E anticipates that the first iteration of TR-3 software that will undergo dedicated OT missions and weapons testing is 40R03.

» SUITABILITY

The operational suitability of the F-35 fleet continues to fall short of Service expectations and the requirements defined in F-35 Block 4 Modernization Capability Development Document. Historical data show that sustaining improvement in aircraft suitability metrics is difficult, despite reliability improvements initiated by the program. (See the FY24 Annual Report for details on the historical data.) The program continues to prioritize aircraft availability improvement initiatives in order to meet U.S. and partner nation expectations.

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. These resets are poorly recorded – the Autonomic Logistics Information System (ALIS), used to track and manage maintenance issues, does not have the capability to automatically log these events, and pilots have historically underreported the occurrences in post-flight debriefs. As such, mission systems instability is not accurately reflected in reliability metrics. To improve F-35 aircraft mission systems stability, DOT&E recommends that the Operational Data Integrated Network (ODIN) – the system replacing ALIS – include the capability to automatically record and document pilot-initiated resets of mission systems.

» SURVIVABILITY

While the program has made strides to fix many cyber deficiencies and has stated that fixing cyber issues is a priority, additional deficiencies were found during the test events in FY25.

Further insights into prioritizing components of the aircraft for cyber survivability 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, and fund a FIAB for each capability release through the Block 4 program.
2. Ensure programming, funding, and contracting are in place to modify all OT aircraft with the appropriate capabilities, life limit, and instrumentation, including OABS requirements, in time to accomplish dedicated OT of mission and weapons events in the associated OT plans.
3. Conduct more in-depth cyber survivability testing of the air vehicle, ALIS/ODIN, training systems, and eventually JSE; complete the plans for hardware- and software-in-the-loop air vehicle 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, as recommended in the FY22 – 24 Annual Reports.
4. 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, as recommended in the FY22 – 24 Annual Reports.
5. Develop and routinely report software sustainment and

stability metrics that show how well the program's overall software development capability for the air vehicle and logistics sustainment system is progressing. In particular, incorporate the ability of the aircraft's prognostics health management to detect and record pilot-initiated resets of mission critical systems in flight and produce records in the Computerized Maintenance Management System to more accurately track air vehicle system stability, as recommended in the FY22 – 24 Annual Reports.

6. Pursue funding and asset requirements to support testing of weapons being integrated in the 40R03 release, particularly long-range air-to-surface weapons.

The UOTT should:

1. Work with the U.S. Services to resume dynamic RCS measurements of two OT aircraft per variant, in accordance with the TEMP, as recommended in the FY24 Annual Report.

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

In FY25, the Global Command & Control System – Joint (GCCS-J) Program Management Office (PMO) updated the v6.1.x baseline via maintenance releases with improved air, space, ground, and maritime capabilities intended to improve situational awareness. The Joint Interoperability Test Command (JITC) continues to conduct tailored evaluations of each fielded maintenance release. Due to the availability constraints of the combatant command selected to support the GCCS-J cooperative vulnerability and penetration assessment (CVPA) and adversarial assessment (AA), the Defense Information Systems Agency (DISA) postponed the operational cyber survivability testing of v6.1.x baseline until 2Q – 3QFY26.

SYSTEM DESCRIPTION

GCCS-J is the nation's system of record for the command and control of joint and coalition forces. Its common operational picture (COP) correlates and fuses data from multiple sensors and intelligence sources to provide warfighters with situational awareness. It 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 site's 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 COP; and
- Providing a missile warning and tracking capability.

PROGRAM

In FY25, the GCCS-J PMO fielded versions v6.1.0.4 and v.6.1.0.5 and released v6.1.1.0 and v6.1.1.1. These upgrades deliver prioritized air, space, ground, and maritime capabilities and are intended to improve the situational awareness of the warfighter. User sites have the authority to choose when to upgrade GCCS-J.

During operational testing, users identify impactful improvements to add 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.

The GCCS-J integrated test environment includes simulated and live interfaces and operational server configurations; however, it does not capture the mission configurations associated with each combatant command and other critical user sites. In FY25, the GCCS-J team updated their test strategy to encompass the system's agile nature and the varying operational site configurations. The updated strategy includes the incorporation of some operational testing considerations into the PMO's developmental testing and pre-fielding user testing of maintenance releases, and tailored, site-specific operational testing by JITC of releases after their fielding. DOT&E will monitor these smaller test events and report on them as needed, rather than produce an FOT&E report as previously planned in the FY24 Annual Report. This test strategy is reflected in the draft TEMP update, expected to be delivered to DOT&E for approval in FY26.

» MAJOR CONTRACTORS

- Northrop Grumman Systems Corporation – Newport News, Virginia
- BluestoneLogic – Washington, DC
- Data Computer Corporation of America – Ellicott City, Maryland

TEST ADEQUACY

In FY25, JITC completed post-fielding, site-specific operational evaluations of GCCS-J v6.1.0.4 and v6.1.0.5 and monitored the PMO's developmental testing of maintenance releases v6.1.1.0 and v.6.1.1.1. The operational test events were conducted in accordance with DOT&E guidance, which included representative hardware, software, real-world data, and operational end users who performed system administration and COP mission tasks. DOT&E observed the testing, which focused on the capabilities and interfaces available at U.S. Army Pacific and U.S. Marine Corps Forces, Pacific commands. Site-specific test cases were developed with direct input from users at both commands.

In FY25, DISA did not conduct operational cyber survivability testing of the v6.1.x baseline. The CVPA and AA planned for FY25 were postponed to 2Q – 3QFY26, due to site availability constraints.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

DOT&E will continue to monitor testing of upgrades to the GCCS-J v6.1.x baseline to determine operational effectiveness and suitability and report on these upgrades as needed.

» SURVIVABILITY

DOT&E will report on the cyber survivability of the GCCS-J v6.1.x baseline upon completion of the CVPA and AA in FY26.

RECOMMENDATIONS

DISA should:

1. Submit an updated TEMP to DOT&E for approval.
2. Conduct a CVPA and an AA to complete testing necessary to support an evaluation of cyber survivability, as discussed in the FY23 and FY24 Annual Reports.

Joint Biological Tactical Detection System (JBTDS)

The Joint Biological Tactical Detection (JBTDS) program completed all developmental and integrated tests in FY25, in accordance with the DOT&E-approved TEMP, with exception of modeling and simulation, which will now be completed in 1QFY26. The multi-Service operational test and evaluation (MOT&E) is now scheduled for 1QFY26. DOT&E will publish a classified MOT&E report in 3QFY26 to inform the full-rate production (FRP) decision.

SYSTEM DESCRIPTION

The JBTDS consists of an integrated man-portable biological warfare agent (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. U.S. 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 in the production and deployment phase of acquisition. DOT&E approved the Milestone C (MS C) TEMP in September 2023. In July 2025, the program office delivered the identifier component to U.S. Special Operations Command and plans to deliver the identifier component to the National Guard Bureau in 4QFY25. The program completed all developmental and integrated tests in FY25, in accordance with the DOT&E-approved test plans, with exception of modeling and simulation, which will now be completed in 1QFY26. The MOT&E was delayed from 4QFY25 to 1QFY26, due to warfighter availability.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

The program completed multiple laboratory tests in FY25, in accordance with the DOT&E-approved test plans, to demonstrate detector performance across various BWAs.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Rather than submitting a separate MOT&E report on the BWA identifier component, as discussed in the FY24 Annual Report, DOT&E will submit a single classified MOT&E report on the system as a whole. The assessment will use the laboratory test data combined with the future MOT&E data as inputs to a model and simulation to assess the operational effectiveness, suitability, and survivability of the JBTDS system. DOT&E will provide the classified MOT&E report in early 3QFY26 to inform the FRP decision.

RECOMMENDATIONS

The Joint Product Manager should continue to address the following recommendations from the FY23 and FY24 Annual Reports:

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. Improve the identifier assays to meet performance requirements.

Joint Cyber Warfighting Architecture (JCWA)

The U.S. Cyber Command (USCYBERCOM) continues to refine internal processes, roles, and responsibilities as it stands up the Joint Cyber Warfighting Architecture (JCWA) Program Executive Office (PEO). Additionally, USCYBERCOM has established an offensive cyber operations hybrid program management office (PMO) to improve software development efficiencies among multiple critical JCWA components. In 4QFY25, DOT&E approved the T&E Strategy, which represents a coordinated effort to secure the resources required to verify JCWA's ability to successfully enable global resilient cyber operations. No JCWA-level operational testing was conducted in FY25, and individual components continued to field capability following limited operational testing, with most testing focused on cyber resilience.

SYSTEM DESCRIPTION

JCWA is USCYBERCOM's planned system-of-systems architecture that will provide an integrated suite of cyber capabilities and tools to the Cyber Mission Force for rehearsing and conducting offensive and defensive cyber operations. This system of systems is designed to collect, fuse, and process cyber data and intelligence to provide cyber forces with situational awareness and battle management at the strategic, operational, and tactical levels.

JCWA's new capabilities are intended to be adaptable to joint mission needs, operating environments, and evolving threats and technologies. Currently, JCWA includes six foundational components: Unified Platform (UP), Joint Cyber Command and Control (JCC2), Persistent Cyber Training Environment (PCTE), Joint Common Access Platform (JCAP), tools, and sensors.

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 but encompasses the following software acquisition pathway programs:

- UP is a cloud-based set of applications, services, and resources that enable full-spectrum cyberspace operations by integrating USCYBERCOM cyber capabilities and systems. It operates and maintains the Big Data Platform for USCYBERCOM and Service components. UP is a software acquisition program.

- JCC2 is a portfolio of integrated products that provide situational awareness, battle management, and cyber force management for full-spectrum cyber operations.
- PCTE provides a standardized training platform for individuals and teams of cyberspace operators to maintain readiness and rehearse missions for cyber operations. PCTE is an Acquisition Category II program.
- JCAP provides infrastructure for USCYBERCOM and the Services to coordinate and execute cyber operations. JCAP is a software acquisition program.
- Other projects and methodologies are used to develop and deploy tools and sensors to cyber forces.

» MAJOR CONTRACTORS

Each Service uses a multitude of contracts and contractors for the acquisition of JCWA's UP, JCC2, PCTE, JCAP, tools, and sensors.

TEST ADEQUACY

Similar to last year's report, no JCWA-level operational testing was conducted in FY25, and the JCWA components continue to employ Agile methodologies on different development and deployment schedules. However, USCYBERCOM is taking key steps to enable JCWA-level testing by improving the JCWA-level requirements development process and establishing the Joint Interoperability Test Command (JITC) as the lead operational test agency.

In FY25, though some components underwent limited operational testing but was not sufficient to assess operational effectiveness and suitability. PCTE conducted regular operational testing along with cyber resilience testing. JCC2 initiated testing to support an operational utility evaluation. JCAP conducted multiple cyber resilience test events.

Service operational test agencies remain challenged to support the individual component OT&E programs and are unable to react to the constantly evolving demands of Agile software-centric programs. Thus, the Services continue to field multiple capabilities with insufficient testing. DOT&E will continue to work with JITC and USCYBERCOM to address these challenges.

As the JCWA concept matures, the scope of T&E required to support cyber warfighting efforts needs to continuously evolve so that it addresses the entire architecture and the dynamic, operational environment within which JCWA operates. Adequate OT&E of JCWA will require USCYBERCOM to establish a cadence of testing and invest in the development of test infrastructure.

The DOT&E Cyber Assessment Program (CAP) continues to partner with USCYBERCOM to identify ways in which CAP activities can support assessments of USCYBERCOM's global infrastructure for cyber operations.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Insufficient data have been collected to enable a preliminary assessment of the JCWA-level operational effectiveness and suitability.

» 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 and FY24 Annual Reports, USCYBERCOM should:

1. Prioritize and accelerate efforts to finalize JWCA-level requirements.
2. Require OT&E to inform value assessments.
3. Establish a cadence of testing for dedicated OT&E, beginning in FY26, to understand how the capabilities afforded by JCWA evolve over time and to ensure JCWA is an operationally effective, suitable, and survivable enabler of cyber operations.
4. Continue to partner with the DOT&E CAP to characterize the cyber posture of critical infrastructure related to JCWA.

Joint Operational Medicine Information Systems (JOMIS)

In May 2025, DOT&E published a Joint Operational Medicine Information Systems (JOMIS) Medical Common Operating Picture (MedCOP) IOT&E report, based on FY24 testing. In FY25, the Joint Interoperability Test Command (JITC) conducted two operational assessments (OAs), a cyber survivability test, and a large IOT&E event that collectively tested five JOMIS-managed applications, and supporting modernized data backbone. In FY26, DOT&E will report on the JOMIS operational testing conducted in FY25.

SYSTEM DESCRIPTION

The JOMIS Program Management Office (PMO) provides a suite of 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 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 chartered 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.

PROGRAM

JOMIS uses multiple acquisition pathways for its managed applications. MedCOP, OMDS, and TBLD-M are software acquisition pathway programs, while OpMed CDP is a Middle Tier of Acquisition rapid prototyping pathway program. BATDOK-J was previously developed by the Air Force Research Laboratory. MHSG-T is jointly developed with the Defense Healthcare Management System Modernization (DHMSM) PMO as a Business System Category I program with enduring support provided by DHMSM. DOT&E approved the JOMIS T&E Strategy in September 2022.

The JOMIS PMO has fielded the classified variant of MedCOP to most combatant commands and plans to begin fielding the other managed applications in FY26.

» MAJOR CONTRACTORS

A multitude of contracts and contractors support the JOMIS program. Portfolio integration is managed directly by the JOMIS PMO.

TEST ADEQUACY

In FY25, JITC conducted two OAs, a cyber survivability assessment, and an IOT&E of the JOMIS-managed applications

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	

related to the operational medicine healthcare functions of HCD, MedLOG, and MedSA, in accordance with the DOT&E-approved T&E Strategy.

» HCD TESTING

In FY25, JITC conducted the HCD OA and IOT&E to evaluate the HCD applications: BATDOK-J, OpMed CDP, MHSG-T, and OMDS. Together, these systems enable medical personnel to document healthcare in theater. BATDOK-J, OpMed CDP, and MHSG-T support documentation at different types of medical facilities, while OMDS transfers documentation among them and provides the means of injecting operational medicine care documentation into the MHS GENESIS longitudinal record.

JITC conducted a two-part HCD OA in January and October 2024 to inform readiness for IOT&E. In both parts of the OA, medical personnel used the HCD applications to document patient care under simulated scenarios in a laboratory environment.

JITC conducted a cyber survivability test of all JOMIS-managed applications, comprised of a cooperative vulnerability and penetration assessment (CVPA) in April 2025, a cyber tabletop exercise in April 2025, and an adversarial assessment (AA) in June 2025.

In June 2025, JITC conducted the first phase of an IOT&E to inform the initial fielding of the three HCD applications and supporting OMDS backbone. During IOT&E, medical personnel used the JOMIS-managed applications to document simulated patient care on USS *Makin Island* (LHD 8); on USNS *Mercy* (T-AH 19); and at simulated Marine Corps medical facilities at Camp Pendleton, California in July 2025, JITC conducted the second part of IOT&E at simulated Air Force medical facilities at Fort Detrick, Maryland. DOT&E will report on the outcomes of the IOT&E and the cyber survivability testing in FY26.

JITC conducted, and DOT&E observed, the HCD OA and cyber survivability testing in accordance with a DOT&E-approved test plan. DOT&E reviewed and provided feedback on initial drafts of the HCD IOT&E test plan but did not approve the final version of the test plan and did not observe testing, due to personnel constraints following the restructuring of DOT&E during the same timeframe.

» MEDLOG TESTING

In April 2025, JITC conducted the TBLD-M OA to evaluate both TBLD-M and its interoperability with the classified variant of MedCOP, using the OMDS data backbone. The TBLD-M OA evaluated TBLD-M's ability to support a simulated blood distribution system and transfer data to MedCOP. The TBLD-M OA was conducted in accordance with the DOT&E-approved test plan, and DOT&E observed the testing. DOT&E will report on the outcome of the OA in FY26.

» MEDSA TESTING

In May 2025, DOT&E published an IOT&E report following the MedCOP IOT&E conducted in FY24. JITC conducted the IOT&E in accordance with a DOT&E-approved test plan, and DOT&E observed the test. The test was adequate to evaluate the operational effectiveness and suitability of MedCOP. The test was not intended to assess cyber survivability.

PERFORMANCE

» EFFECTIVENESS

HCD Applications

In the HCD OA, JITC found that the JOMIS HCD applications contain deficiencies and lack features medical providers need to document care; such problems could jeopardize patient safety if the applications are used for actual care. Additionally, patient data do not consistently transfer horizontally from one application to another as patients move through the continuum of care, leaving providers with potentially incomplete information about prior medications and treatments. Care documentation is transmitted vertically to OMDS and into the full longitudinal record, requiring a connection with OMDS from all applications in order to be able to successfully access patient care at another location.

In FY26, DOT&E will publish an IOT&E report with operational effectiveness assessments of the suite of HCD applications, based on the testing conducted in FY25.

MedLOG Applications

In FY26, DOT&E will publish an OA report with an operational effectiveness assessment of TBLD-M.

MedSA Applications

At the time of testing, DOT&E determined that MedCOP was not operationally effective. While MedCOP consolidates medical information – such as unit status, medical supply availability, and treatment facility readiness – it does not accurately display data from external sources. Therefore, MedCOP does not provide accurate or complete medical situational awareness, requiring users to access other systems to obtain accurate data and complete their tasks. Multiple improvements to the product have been implemented since the November 2023 IOT&E, including additional automated data sources and rollout of the unclassified MedCOP capability. Additional details are in DOT&E's May 2025 IOT&E report. The JOMIS PMO intends to conduct follow-on testing in FY26 to validate remediations to issues identified in the previous test events.

» SUITABILITY

HCD Applications

In the HCD OA, JITC found that the JOMIS HCD applications do not meet user needs. Users identified usability and training shortfalls that could reduce the system's performance in the deployed environment. Additionally, MHSG-T is difficult for system administrators to install.

In FY26, DOT&E will publish an IOT&E report with operational suitability assessments of the suite of HCD applications, based on the testing conducted in FY25.

MedLOG Applications

In FY26, DOT&E will publish an OA report with an operational suitability assessment of TBLD-M.

MedSA Applications

MedCOP is not operationally suitable. Low user adoption limits its value. Forward units do not consistently report their data in MedCOP, so users at higher echelons do not have all the data they need for medical situational awareness. At the time of the test, forward units without SIPRNet access could not use MedCOP at all. This finding was resolved with the role out of the MedCOP-U product that feeds MedCOP-S. Additional details are in DOT&E's May 2025 IOT&E report.

» SURVIVABILITY

In FY26, DOT&E will publish a cyber survivability report on all JOMIS-managed applications, based on the CVPA and AA conducted in FY25.

RECOMMENDATIONS

The JOMIS PMO should work with the Joint Staff Surgeon and Services to:

1. Define and prioritize the capabilities needed to document patient care in theater, including Service-specific use cases, so that the HCD applications address user expectations.
2. Develop standard operating procedures for MedCOP's use.
3. Issue a mandate for MedCOP's use across all combatant commands and DoW components to ensure forward users are populating MedCOP with actionable data.

The JOMIS PMO should:

1. Implement prioritized fixes for problems identified with the HCD applications to ensure patient safety.
2. Correct data transfer deficiencies to enable the transfer of needed healthcare information from one HCD application to another as patients move through the continuum of care.
3. Ensure MedCOP displays accurate and complete data from external systems by improving its interoperability with those systems.

Key Management Infrastructure (KMI)

In FY25, the Joint Interoperability Test Command (JITC) conducted an operational verification (OV) test of Key Management Infrastructure (KMI) Capability Increment 3 (CI-3) Release 0 (R0). In June 2025, DOT&E published a classified KMI CI-3 R0 OV report. From this test, DOT&E determined that KMI CI-3 R0 is operationally effective with one exception, but not operationally suitable. In July – August 2025, JITC conducted a user acceptance test of Releases 1 through 7. In November 2025, JITC conducted a reduced-scope operational assessment of the combined releases. JITC intends to conduct the Releases 1 through 7 OV in FY26, which DOT&E will report on later in FY26.

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 DoW, 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.

MISSION

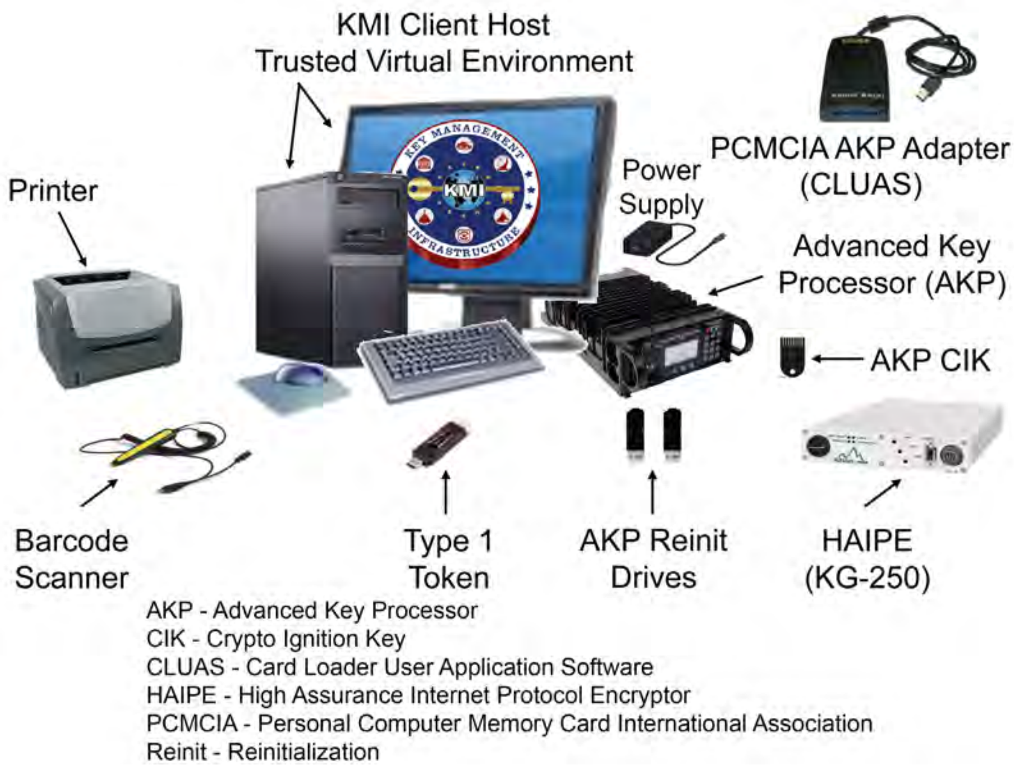
Combatant commands, Services, DoW Agencies, other Federal agencies, coalition partners, and allies will use KMI to provide secure and interoperable cryptographic key generation, distribution, and management capabilities to support mission-critical systems, the DoD Information Network, and initiatives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

PROGRAM

The KMI CI-3 Program Management Office (PMO) began capability development in January 2021. The KMI CI-3 PMO announced a schedule delay in April 2022, due to hardware technical refresh, supply chain delivery delays, system configuration problems, and expanded requirements. The NSA awarded a major contract modification in January 2023 that increased the KMI CI-3 scope to address additional technical requirements packages through 10 Agile releases. The NSA Senior Acquisition Executive re-baselined the KMI CI-3 program in September 2023, and the KMI CI-3 PMO intends to update the KMI CI-3 acquisition strategy to support a full deployment decision in FY27 or later.

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 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 FY26. JITC continues to support development of the operational testing strategy for KMI CI-3.



» MAJOR CONTRACTORS

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

TEST ADEQUACY

JITC conducted the OV test of KMI CI-3 R0 in October 2024 to January 2025. In June 2025, DOT&E published a classified KMI CI-3 R0 OV report. This OV test informed the technical refresh status. DOT&E approved the OV test plan in October 2024 and the cyber survivability plan annex in March 2025. DOT&E observed testing and JITC conducted testing in accordance with the approved test plans. The testing was adequate to evaluate operational effectiveness and suitability; however, JITC has yet to conduct the KMI cyber assessment. JITC conducted a user acceptance test of Releases 1 through 7 in July – August 2025 and conducted a reduced-scope operational assessment of the combined releases in November 2025. JITC intends to conduct the Releases 1 through 7 OV in FY26, which DOT&E will report on later in FY26.

PERFORMANCE

» EFFECTIVENESS

The findings from the KMI CI-3 R0 OV test indicate that the system is operationally effective; however, Over-the-Network-Keying (OTNK) was not effective. KMI users were able to order, generate, and transfer cryptographic products, which are essential KMI functions. OTNK was initially working; however, an upgrade broke the OTNK connections. Additional details are included in the classified KMI CI-3 R0 OV report.

» SUITABILITY

KMI CI-3 R0 is not operationally suitable. JITC and the Services reported numerous suitability problems across a wide range of support, training, and sustainment areas. In particular, users reported issues with trouble ticket tracking and processing. Additional details are included in the classified KMI CI-3 R0 OV report.

» SURVIVABILITY

DOT&E will report on cyber survivability in FY26.

RECOMMENDATIONS

The KMI CI-3 PMO and JITC should:

1. 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 and FY24 Annual Reports.

The KMI CI-3 PMO and NSA should:

1. Fix the OTNK issues. For more details, refer to DOT&E's June 2025 classified KMI CI-3 R0 OV report.
2. Improve processes for managing trouble tickets. For more details, refer to DOT&E's June 2025 classified KMI CI-3 R0 OV report.

Public Key Infrastructure (PKI) Increment 2

In November 2024, DOT&E published the classified Public Key Infrastructure (PKI) Increment 2 FOT&E Report – Suitability and Cyber Survivability Annex Update to inform a full deployment decision (FDD). The NSA Senior Acquisition Executive signed the DoW PKI Increment 2 acquisition decision memorandum in December 2024 and declared full deployment in April 2025.

SYSTEM DESCRIPTION

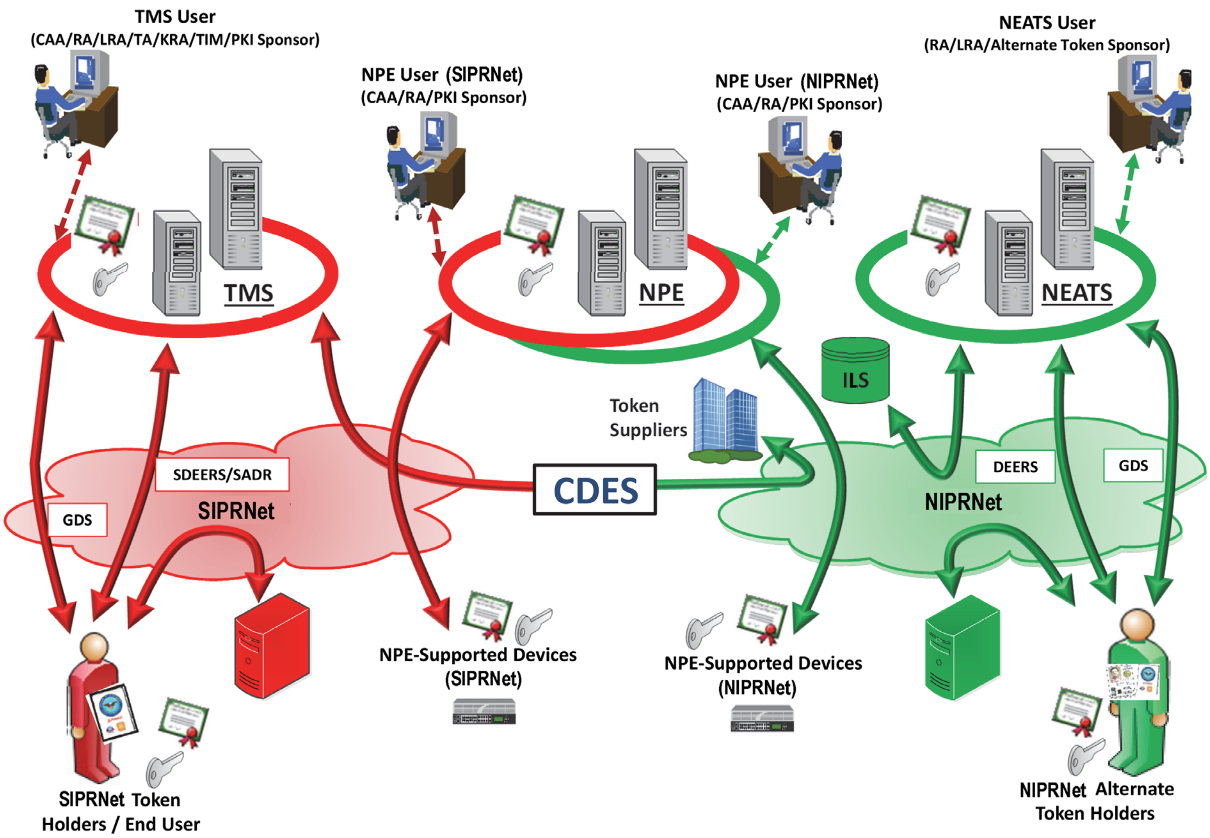
PKI Increment 2 enables the DoW to ensure only authorized individuals and devices have access to networks and data, thereby supporting the secure flow of information across DoD Information Networks and providing secure local storage of information. PKI Increment 2 provides the hardware, software, and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

MISSION

DoW users at all levels use DoW PKI to provide authenticated identity management via personal identification number-protected Common Access Cards, SIPRNet tokens, and NIPRNet Enterprise Alternate Token System (NEATS) tokens to enable DoW 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 DoW Agency operators, communities of interest, and other authorized users use DoW PKI to securely access, process, store, transport, and use information, applications, and networks. Network operators use Non-Person Entity (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.



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

DOT&E approved the PKI Spiral 4 TEMP addendum in October 2017, the PKI Increment 2 FOT&E test plan in October 2020, and the cybersecurity annex in November 2020. The NSA delivered the SIPRNet Token Management System (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 Defense Manpower Data Center (DMDC), and NPE with operational support from the Defense Information Systems Agency (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 memorandum in February 2022, and a classified PKI Increment 2 Cyber Survivability Interim Annex in January 2023. In November 2024, DOT&E published the classified PKI Increment 2 FOT&E Report – Suitability and Cyber Survivability Annex Update to inform the FDD. The NSA Senior Acquisition Executive signed the DoW PKI Increment 2 acquisition decision memorandum in December 2024 and declared full deployment in April 2025.

DMDC began transitioning NEATS authentication from an Alternate Token Issuance and Management System (ATIMS) client to a NIPRNet web service in early 2025. DOT&E attended program management office (PMO)-led test events of the new NIPRNet webservice and browser interface in May 2025. In future years, DMDC intends to migrate many of their capabilities to the Oracle cloud. The ATIMS-to-webservice transition occurred between June 2025 – September 2025.

» 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

In November 2024, DOT&E published the classified PKI Increment 2 FOT&E Report – Suitability and Cyber Survivability Annex Update on FY24 testing. The FY24 events consisted of TMS suitability testing and NEATS cyber survivability testing. These tests were conducted in accordance with DOT&E-approved test plans and provided adequate data to support effectiveness, suitability, and survivability determination. DOT&E observed the testing. The Joint Interoperability Test Command (JITC) did not conduct any operational testing of PKI in FY25.

PERFORMANCE

» EFFECTIVENESS

DOT&E assessed PKI Increment 2 NEATS, NPE, and TMS as 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 and determined that no additional effectiveness testing is required.

» 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. The PKI PMO updated the TMS baseline with improvements in Enterprise Central Management of Tokens (CMT) order tracking to provide 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. In November 2024, DOT&E published an updated assessment of TMS operational suitability in the classified PKI Increment 2 FOT&E Report – Suitability and Cyber Survivability Annex Update, concluding that TMS is operationally suitable with limitations.

» 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 published in January 2023. The PKI PMO mitigated all but one of the NPE problems but did not conduct further NPE operational cyber testing prior to the FDD. The PKI PMO and DMDC mitigated many NEATS findings and other architectural problems found in previous cyber survivability testing. DOT&E published the classified PKI Increment 2 FOT&E Report – Suitability and Cyber Survivability Annex Update in November 2024, which captures the final NEATS operational cyber testing conducted in FY24 at DMDC.

As NSA, DISA, and DMDC migrate PKI capabilities to cloud-hosted environments, operational cyber testing will be needed to maintain and improve survivability. The PKI PMO should conduct periodic operational cyber assessments to evaluate the transition of PKI capabilities to cloud-hosted environments after the FDD.

RECOMMENDATION

The PKI PMO should:

1. Conduct periodic operational cyber survivability assessments of PKI capabilities to evaluate the transition of PKI capabilities to cloud-hosted environments after the FDD.

This page intentionally left blank.

DEPARTMENT OF THE ARMY PROGRAMS

This page intentionally left blank.

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

The AN/APR-39E(V)2 Modernized Radar Warning Receiver (MRWR) began FOT&E in November 2024 and completed all but one FOT&E test event in FY25. The Army conducted operational effectiveness, suitability, and cyber survivability testing in accordance with DOT&E-approved test plans. In FY25, DOT&E observed operational flight testing and intends to publish an FOT&E report in FY26 to inform the Army's full-rate production decision.

SYSTEM DESCRIPTION

The AN/APR-39E(V)2 will replace the more than 30-year-old AN/APR-39A(V)1/4 system on Army rotary-wing and selected fixed-wing aircraft. New electronics and improved antennas will provide aircrew with a fully digital capability to detect current and emerging threats with modern, agile waveforms that operate over an extended frequency range. Cockpit display of a threat's location and operating mode, combined with auditory warnings, will enhance the aircrew's situational awareness and the aircraft's mission survivability. The MRWR includes an open-system architecture and a potential 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 associated with 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 more effectively counter active threats.

PROGRAM

The AN/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 2017, in accordance with a DOT&E-approved test plan and fielded a limited number of D(V)2 as an interim solution to an operational need. MRWR development started in 2019, and DOT&E accepted the Army's existing T&E Strategy when DOT&E placed the program on oversight in December 2022.

DOT&E approved the cooperative vulnerability and penetration assessment (CVPA) cyber test plan in August 2023, and the Army accomplished the CVPA in December 2023. DOT&E approved the adversarial assessment (AA) cyber test plan in January 2024, and the Army accomplished the AA in March 2024 onboard an AH-64E at the Redstone Test Center, Redstone Arsenal, Alabama. The Army also surveyed aircrew during the FOT&E flight testing on how they would potentially identify and respond to cyber-attacks. DOT&E approved the FOT&E test plan in October 2024, and the Army began flight tests in November 2024. The Army began low-rate initial production in December 2023.

» MAJOR CONTRACTOR

- Northrop Grumman – Rolling Meadows, Illinois

TEST ADEQUACY

In November 2024, the Army began conducting FOT&E flight testing and completed all but one FOT&E test event in FY25 at the Naval Air Weapons Station, China Lake's Electronic Combat Range. DOT&E observed the testing. The Army conducted the testing in accordance with the DOT&E-approved test plan, employing two operationally representative AH-64Ev6 Apache helicopters equipped with the MRWR. Operational aircrew flew against the range's surface threats, as well as in proximity to the city of Los Angeles, to assess the MRWR's performance in a complex electromagnetic environment. The Army collected data to quantify the time it took pilots to respond to an alert from the APR-39E(V)2 angle-of-arrival-accuracy of signals, and other effectiveness metrics. The Army also collected system reliability and other suitability data during the FOT&E flight tests. Long-term reliability metrics require data harvested over a large amount of flight time. Since the number of operational flight test hours flown was insufficient to assess system reliability with statistical confidence for longer-duration Apache missions, or using data from missions performed by other Army aircraft, such as the CH-47 and UH-60, DOT&E will not be able to fully assess system reliability.

The last remaining FOT&E test event the Army plans to complete is a maintenance demonstration, scheduled for 1QFY26. The maintenance demonstration will verify the effectiveness of design changes the Army implemented to improve maintainability relative to AN/APR-39D(V)2. The Army also collected human-systems interaction data, such as pilot workload and system usability in actual flight operations, using surveys administered during FOT&E flight testing. Following completion of the maintenance demonstration and data analysis, DOT&E will publish a classified FOT&E report in FY26 to inform the Army's full-rate production decision.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E will assess MRWR operational effectiveness, suitability, and cyber survivability in a classified FOT&E report in FY26.

RECOMMENDATION

The Army should:

1. Continue to collect and analyze failure data after the AN/APR-39E(V)2 is fielded, to assess and improve system reliability and built-in test performance, particularly for longer mission durations (up to 11 hours), to support future CH-47 and UH-60 operations.

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

In February 2025, the Army conducted a Soldier Touchpoint (STP) to observe soldiers' performance installing and removing a composite rubber track (CRT) on the Armored Multi-Purpose Vehicle (AMPV) Medical Treatment (MT) variant. The Army also collected soldier feedback on ride quality and track maintenance during preventive maintenance checks and services.

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), MT, Medical Evacuation (ME), and Mortar Carrier (MC). Variants are equipped with tailored mission equipment packages to support units' tasks.

MISSION

ABCTs employ the AMPV Family of Vehicles to accomplish required operational support missions across the range of military operations. ABCT units 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. DOT&E published a combined IOT&E and LFT&E report with a classified annex in January 2023 to inform the full-rate production decision in June 2023. In July 2023, the Army completed baseline testing of the CRT on an AMPV MT to inform the characterization and durability of the CRT, and the automotive performance and ride quality.

The Army intends to submit an updated TEMP and LFT&E test plan to DOT&E for approval in 2QFY26. Live fire testing is scheduled to commence in 3QFY26 to collect data on the survivability and repairability of the CRT, and to assess post-threat impact on the AMPV's mobility. As part of live fire testing, the Army intends to conduct a STP to collect soldier feedback on installing and operating a damaged track with a battlefield damage repair kit. DOT&E intends to observe the live fire testing and to publish a classified LFT&E report in 1QFY27 to inform the Army's engineering change proposal production cut-in decision scheduled for 2QFY27.

» MAJOR CONTRACTOR

- BAE Systems – York, Pennsylvania

TEST ADEQUACY

In February 2025, the Army conducted an STP at Aberdeen Test Center, Maryland, to observe soldiers' performance conducting a full-track removal and installation of the CRT on an AMPV MT with support from a M88A2 recovery vehicle. The Army also collected soldier feedback on ride quality and track maintenance during preventive maintenance checks and services. DOT&E observed the testing.

PERFORMANCE

» EFFECTIVENESS

There are no updates to DOT&E's operational effectiveness evaluation from the January 2023 combined IOT&E and LFT&E report.

» SUTIABILITY AND SURVIVABILITY

DOT&E intends to use the STP observations and the 3QFY26 LFT&E data to publish a classified LFT&E report in 1QFY27, assessing suitability and survivability.

RECOMMENDATION

The Program Executive Office should:

1. Provide to DOT&E for approval LFT&E test plans for assessing suitability and survivability once the plans are finalized.

Army Integrated Air and Missile Defense (AIAMD)

In February 2025, DOT&E approved an updated Army Integrated Air and Missile Defense (AIAMD) T&E Strategy Annex that details testing to be completed in FY25. In June 2025, the Army Test and Evaluation Command (ATEC) started the AIAMD FOT&E and expects to complete testing in 2QFY26. DOT&E will publish an updated assessment of AIAMD operational effectiveness, suitability, and survivability in a classified FOT&E report upon completion of testing in 2QFY26.

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. Additional sensors and weapons, such as Lower-Tier Air and Missile Defense Sensor (LTAMDS) and the Indirect Fire Protection Capability Increment 2 (IFPC Inc 2), have also been integrated through the IBCS agile software development process.

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. In June 2024, the program received the first low-rate initial production units, which included upgrades to much of the AIAMD system's hardware to address obsolescence issues, system limitations, corrective actions, and support integration with new systems. The Army intends to continue to integrate new and existing sensors and weapons through a series of future software increments.

In February 2025, DOT&E approved the AIAMD 2025 T&E Strategy Annex. The annex covers dedicated AIAMD FOT&E, conducted as part of the Integrated Fires Test Campaign 2025 (IFTC 25). The AIAMD FOT&E is intended to support a full materiel release decision to field AIAMD equipment to operational Patriot Air and Missile Defense Battalions. The FOT&E will also inform a Chief of Staff of the Army decision to field AIAMD in the U.S. Indo-Pacific Command and U.S. European Command theaters of operations. The Army plans to continue to submit annual T&E Strategy annexes for DOT&E approval in support of future test objectives.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

ATEC started FOT&E in June 2025 at White Sands Missile Range, New Mexico, and expects to complete testing in 2QFY26. The DOT&E-approved test plan includes software/hardware-in-the-loop operations using accredited modeling and simulation (M&S) tools; sustained live air operations; and a missile flight test. Additional test phases include a cooperative vulnerability and penetration assessment and an adversarial assessment in the software/hardware-in-the-loop environment. A separate cyber and electronic warfare convergence test is also planned to occur in the live air environment. DOT&E is observing the FOT&E.

The beginning of the AIAMD FOT&E was delayed due to issues with the M&S tools intended to provide an operationally realistic threat environment in the software/hardware-in-the-loop phase of testing. The program worked to improve the M&S tools to receive an ATEC accreditation prior to the start of test; however, the program was unable to fully resolve some of the M&S issues, which will delay DOT&E's assessment of operational effectiveness until at least 2QFY26, when retesting in the software/hardware-in-the-loop environment is scheduled to be completed.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E will publish an updated assessment of AIAMD operational effectiveness, suitability, and survivability in a classified FOT&E report upon completion of testing in 2QFY26. DOT&E's ability to provide an assessment of AIAMD operational effectiveness, suitability, and survivability will be dependent on the potential impacts of M&S issues as mentioned above.

RECOMMENDATIONS

The Army should:

1. 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 – 24 Annual Reports.
2. Continue development of the AIAMD 2026 T&E Strategy Annex to support future test of AIAMD capabilities and IFTC events.

CH-47F Block II Chinook

In April 2025, the CH-47F Block II Chinook program began LFT&E, which will continue through FY26. In July 2025, DOT&E approved the program's Milestone C TEMP. On September 12, 2025, the Army transitioned the program from the major capability acquisition pathway to the Middle Tier of Acquisition (MTA) rapid fielding pathway. The newly approved TEMP will support the testing scheduled for the MTA pathway.

SYSTEM DESCRIPTION

The CH-47F is the Army's heavy-lift helicopter that provides combat and combat service support capability to the Army, with a capacity to transport 31 combat-loaded troops. The CH-47F Block II increases performance to offset the performance lost due to mission equipment package weight growth on the legacy aircraft. The CH-47F Block II establishes a framework for future block upgrades to accomplish recapitalization of the fielded fleet. CH-47F Block II improvements include, but are not limited to, an improved drive train, improved rotor system, lithium-ion battery emergency power system, lightweight fuel system, and airframe strengthening modifications.

MISSION

Units equipped with the CH-47F Block II will support the Army's heavy-lift mission in execution of full-spectrum operations. The Chinook allows the Army to accomplish critical tasks across the operational environment including air assault, air movement, causality evacuation, aerial recovery, and area resupply. The Chinook's range, speed, and lift capacity allow for operational flexibility. Depending on mission requirements, the CH-47F can be employed individually, in multi-ship formations, or as a company.

PROGRAM

The CH-47F Block II started on the major capability acquisition pathway as an Acquisition Category IC program led by the Army's Program Executive Office Aviation at Redstone Arsenal, Alabama. However, in September 2025, the Army transitioned the program from the major capability acquisition pathway to the MTA rapid fielding pathway.

Shortly before the change in the program's acquisition strategy, the Army updated the program's TEMP, which DOT&E approved in July 2025, to inform the Milestone C decision. The newly approved TEMP will support the testing scheduled for the MTA pathway and does not require an update. Additionally, DOT&E approved the Alternate LFT&E Strategy in October 2015 and supports both the major capability acquisition pathway and the MTA rapid fielding pathway.

Additionally, the Product Manager provided DOT&E with the MTA rapid fielding acquisition strategy in September 2025 to inform recommendations for the operational demonstration (Ops Demo) scheduled for 2QFY27.

» MAJOR CONTRACTOR

- The Boeing Company – Ridley Park, Pennsylvania

TEST ADEQUACY

Since FY24, the program has conducted a series of special user demonstrations using the aviation unit assigned to Fort Campbell, Kentucky. These user demonstrations are not operational tests and thus do not have DOT&E-approved test plans. However, the events have demonstrated CH-47F Block II's ability to meet several of the program's requirements. There are plans to conduct another special user demonstration in FY26 with operational users at Fort Bragg, North Carolina, which will be incorporated into company-level training events.

Despite the special user demonstrations not being official operational tests, the special user demonstrations have included data collectors from Army Test and Evaluation Command (ATEC) and DOT&E. DOT&E will use the data in a combined Ops Demo and LFT&E report, following the Ops Demo planned in 2QFY27.

Simultaneously, the Army began conducting live fire tests at Aberdeen Proving Ground, Maryland, in April 2025, in accordance with the DOT&E-approved Alternate LFT&E Strategy. DOT&E has been present at all live fire tests conducted at Aberdeen Proving Ground, Maryland. The tests are still ongoing, and DOT&E will address the findings in the combined Ops Demo and LFT&E report in 3QFY27.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

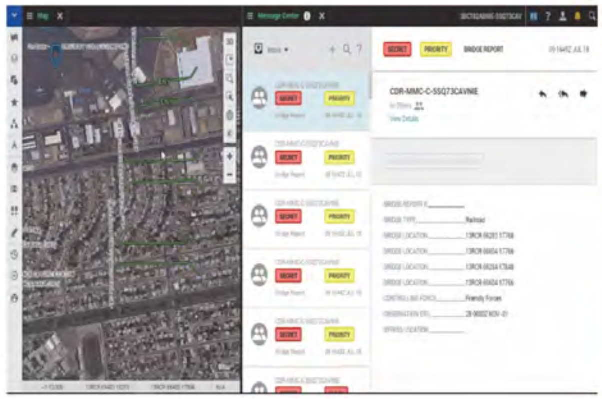
Insufficient data are available at this time to evaluate the operational effectiveness, suitability, and survivability of the CH-47F Block II. DOT&E will publish a classified combined Ops Demo and LFT&E report in 3QFY27, following completion of the scheduled Ops Demo.

RECOMMENDATIONS

The Army should:

1. Continue investment in the program's live fire testing to ensure the survivability of the aircraft and its warfighters.
2. Ensure there are adequate resources, including troops, vehicles, refueling points, ground force, opposing force, etc., needed to conduct the OT&E missions and provide that detail in an operational test plan.
3. Continue to capitalize on special user demonstrations by ensuring adequate data collectors participate, to reduce data requirements during future Ops Demos and to inform operational test reports.

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




In FY25, Command Post Computing Environment/Tactical Server Infrastructure (CPCE/TSI) continued the development of the Increment 2 software delivery. CPCE did not conduct any test events in FY25 and will transition to sustainment in FY26. In July 2025, DOT&E removed the CPCE/TSI program from oversight due to IOT&E, FOT&E, and associated reporting to inform full deployment decisions being complete. Future efforts will continue in separate programs.

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. 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 OVERSIGHT HISTORY

CPCE is an Acquisition Category II major capability acquisition pathway program. In July 2016, DOT&E added CPCE to DOT&E oversight. In May 2020, DOT&E updated oversight of CPCE to include TSI. A full deployment decision for Increment 0 occurred in FY19, and a full deployment decision for Increment 1 occurred in FY22. DOT&E published FOT&E reports in June 2019 and December 2021 to inform those decisions.

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 another full deployment decision. This resulted in a down-scope of the originally planned FOT&E to focus on cyber testing the software to support a software release.

In July 2024, DOT&E published a classified CPCE cyber survivability report that found the Increment 2 performed the same against nearsiders and outsiders compared to CPCE Increment 1. CPCE did not conduct any test events in FY25. The last version of CPCE software will transition to sustainment in FY26. In July 2025, DOT&E removed the CPCE/TSI program from oversight due to IOT&E, FOT&E, and associated reporting to inform full deployment decisions being complete.

Common Tactical Truck (CTT)

The Vice Chief of Staff of the Army concurred with the Common Tactical Truck (CTT) Capability Development Document (CDD) utilizing performance test data from the Middle Tier of Acquisition (MTA) rapid prototyping phase. This new CDD will serve as the basis for a follow-on full and open competition if the Army transitions the program to the major capability acquisition pathway in the future. In July 2025, DOT&E removed the CTT program from oversight because the program is not conducting further testing to inform a fielding decision or full-rate production decision.

SYSTEM DESCRIPTION

CTT is a Family of Vehicles (FoV) modernization effort to replace the Heavy Expanded Mobility Tactical Truck, Palletized Load System, and Line Haul Tractor, 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 may be selected as the base platform to modernize the cargo and load handling system, off-road tractor, line-haul tractor, and tanker, as well as air defense, missile systems, radar systems, bridging systems, and boat systems. These concepts will be further refined as the Army develops requirements in the CDD.

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. The CTT FoV 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 OVERSIGHT HISTORY

DOT&E placed the CTT program on oversight in January 2023 and approved the CTT T&E Strategy in April 2024. The Army conducted an operational demonstration in August and September 2024. All test prototypes were returned to the vendor. The Army utilized performance test data from the event to inform the CDD for the CTT. In July 2025, DOT&E removed the CTT program from oversight because the program is not doing further testing to inform fielding or full-rate production decisions. Should the Army transition CTT to an Acquisition Category I program in FY28 based on the new CDD, DOT&E will put it back on oversight for operational and live fire testing, in accordance with statutory requirements.

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

In June 2025, three Directed Energy Maneuver-Short Range Air Defense (DE M-SHORAD) prototypes participated in a 4th Battalion, 60th Air Defense Artillery Regiment-led training and live fire exercise at Fort Sill, Oklahoma, meant to develop tactics, techniques, and procedures for directed energy and kinetic effector systems. DE M-SHORAD is a prototyping effort led by the Army's Rapid Capabilities and Critical Technologies Office (RCCTO) under its Other Transaction Authority. RCCTO will take lessons learned from DE M-SHORAD prototypes to inform a 4QFY26 Enduring High Energy Laser (E-HEL) system procurement decision. In June 2025, RCCTO demilitarized DE M-SHORAD prototypes and inducted one into the U.S. Army Air Defense Artillery Training Support Facility. In July 2025, DOT&E removed DE M-SHORAD from oversight as the Army is no longer pursuing it as a program of record.

SYSTEM DESCRIPTION

The DE M-SHORAD integrated 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 included a 50-kilowatt spectral beam combined laser, powered by lithium nickel cobalt aluminum oxides (Li-NCA) batteries that were recharged by diesel generators onboard the vehicle.

DE M-SHORAD briefly augmented 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

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

PROGRAM OVERSIGHT HISTORY

DE M-SHORAD is a prototyping effort led by RCCTO under its Other Transaction Authority. The program did not have an acquisition strategy. The Army procured a total of six DE M-SHORAD prototype vehicles.

- In May 2019, the Secretary of the Army initiated the DE M-SHORAD program, approving the initial Directed Energy Strategy and directing 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 Air Defense Artillery Regiment 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 Activity awarded C-17 transportability certification in January 2024. In February 2024, the Army deployed the four DE M-SHORAD prototype vehicles to support OCONUS operations. DOT&E placed the DE M-SHORAD program on oversight in March 2024. By November 2024, all four DE M-SHORADs redeployed to the CONUS.
- In June 2025, three DE M-SHORAD prototypes participated in a 4-60th Air Defense Artillery Regiment-led training and live fire exercise of at Fort Sill, Oklahoma, meant to develop tactics, techniques, and procedures for directed energy and kinetic effector systems. At the conclusion of the live fire exercise, the Army demilitarized DE M-SHORAD prototypes one through four and inducted one of the prototypes into the U.S. Army Air Defense Artillery Training Support Facility. DOT&E intended to publish an early fielding report in FY25 but no longer will, as the Army is no longer pursuing the program.

DE M-SHORAD prototypes five and six are additional test articles that provide alternative technical and competitive laser weapon solutions. RCCTO plans to execute government acceptance testing for prototype five in 2QFY26. RCCTO will transition prototype six to support Science and Technology efforts. RCCTO is using the DE M-SHORAD prototypes to inform a 4QFY26 E-HEL system procurement decision. E-HEL is a RCCTO prototyping effort for a modular, open-interface air defense high energy laser weapon system. In July 2025, DOT&E removed DE M-SHORAD from oversight as the Army is no longer pursuing it as a program of record.

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

Dismounted Assured Positioning, Navigation, and Timing System (DAPS) is a handheld GPS receiver that provides Army forces with trusted position, navigation, and timing (PNT) information in degraded and denied GPS environments. The Army completed DAPS GEN II IOT&E in November 2023, in accordance with a DOT&E-approved test plan. DOT&E published a classified DAPS GEN II IOT&E report in May 2024 to inform the full-rate production (FRP) decision in August 2024. DOT&E removed DAPS from oversight in July 2025 as the IOT&E and associated reporting were complete.

SYSTEM DESCRIPTION

DAPS is a handheld Military Code (M-Code) GPS receiver that integrates multiple 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 currently used by Nett Warrior equipped soldiers.

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 electromagnetic 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 OVERSIGHT HISTORY

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 Category III program at Milestone C with a DOT&E-approved TEMP. In November 2023, the Army conducted the DAPS GEN II IOT&E. In May 2024, DOT&E published a classified DAPS GEN II IOT&E report, which informed the Army's FRP decision in August 2024. DOT&E removed the DAPS program from oversight in July 2025 because the IOT&E and associated reporting were complete.

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

In FY25, the Army worked with the prime contractor to develop and test a redesigned side-mounted proximity sensor (SMPS) for the Extended Range Guided Multiple Launch Rocket System (ER GMLRS). The Army plans to restart the remaining three system qualification test (SQT) shots in 1QFY26 and complete operational testing in 1QFY27. In September 2025, DOT&E approved the ER GMLRS Milestone C (MS C) TEMP annex. DOT&E will publish an ER GMLRS operational assessment report in 3QFY26 and an IOT&E report that encompasses all production-representative testing of ER GMLRS to inform the full-rate production (FRP) decision in 2QFY27.

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 height of burst (HOB) for both the ER GMLRS Unitary and Alternative Warhead (AW) rocket variants.

Both the ER GMLRS Unitary and AW variants have a 200-pound 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 submunitions.

PROGRAM

In June 2017, the Army initiated the ER GMLRS program as an engineering change proposal (ECP) to the ER GMLRS Unitary and AW 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 AW variant. In November 2023, the Army delayed additional testing of the AW variant, pending development of a redesigned SMPS. All testing was conducted in accordance with the DOT&E-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 Milestone C (MS C) planned for 3QFY25. In 1QFY25, the Army shifted the MS C decision to 3QFY26, to allow for the ongoing redesign of the SMPS and to complete the remaining integrated test shots in FY26, which will use the redesigned SMPS.

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 HOB and the AW variant were not part of the operational test due to SMPS' early detonation anomaly reliability failures.

In July 2025, the Army submitted the ER GMLRS MS C TEMP annex, in response to DOT&E's recommendation. In September 2025, DOT&E approved the ER GMLRS MS C TEMP annex with a caveat that the program, to mitigate risk, should resource additional rockets to increase the confidence and likelihood that the number of rockets tested will be adequate to allow for DOT&E to conduct an integrated operational effectiveness and suitability evaluation; inform the Army's tactics, techniques, and procedures; and inform multiyear procurement quantities.

Following integration of the redesigned SMPS into the ER GMLRS, the Army plans to conduct one additional SQT shot with the AW variant in 1QFY26 and two additional SQT shots with the AW variant rocket in 2QFY26. The Army will continue operational testing of two multiple-rocket missions with both variants until 1QFY27, 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 in 2QFY27.

» 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 insufficient to assess, with statistical confidence, operational effectiveness, lethality, suitability, and survivability. The first 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 variant in delay mode, because the necessary hardware modifications to the ER GMLRS to integrate the flight termination system creates an increased risk to warhead initiation when engaging a target in delay mode. This in turn introducing an undesirable unexploded ordnance hazard to range personnel. The Army does not currently plan to test ER GMLRS Unitary variant 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.

The Army did not conduct any operational or live fire testing in FY25. In 3QFY26, following completion of ER GMLRS testing with both the old SMPS design and the redesigned SMPS, DOT&E will publish an operational assessment report to inform the Army's MS C decision in 3QFY26.

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

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

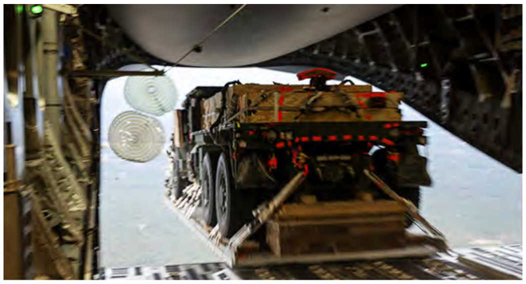
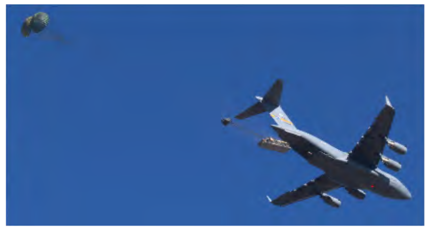
Insufficient data are available to evaluate the operational effectiveness, lethality, suitability, and survivability of the ER GMLRS. DOT&E will provide these assessments following the scheduled completion of operational test in 1QFY27, in an IOT&E report in 2QFY27.

RECOMMENDATIONS

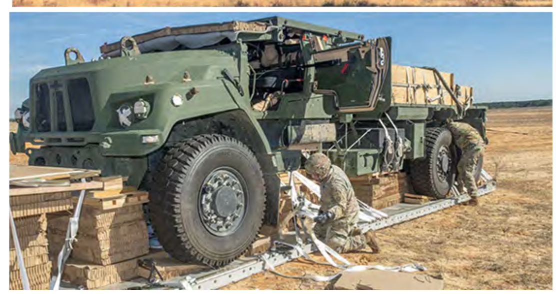
As recommended in the FY24 Annual Report, the Army should:

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. Continue to develop a plan to demonstrate the key performance parameter reliability requirement with statistical confidence.
4. Consider testing ER GMLRS Unitary rockets in delay mode.

Family of Medium Tactical Vehicles A2 (FMTV A2)



In March 2025, DOT&E published a classified Family of Medium Tactical Vehicles A2 (FMTV A2) Low-Velocity Airdrop (LVAD) LFT&E report covering a series of live fire tests conducted in 2023 and 2024. The report supports the Army's full materiel release decision projected for 3QFY26. In March 2025, DOT&E removed the FMTV A2 program from oversight due to completion of operational and live fire testing and associated reporting requirements.

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.

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 upgrades to expand truck capabilities, such as increased cargo carrying capacity, improved mobility, improved onboard diagnostic capabilities, increased electric power capacity, and increased safety and survivability features.

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 material handling crane and a self-recovery winch. The following variants are available on each FMTV chassis:

- Light Medium Tactical Vehicle (LMTV) chassis – a 3-ton cargo truck, a 2.5-ton van, and a 3-ton LVAD cargo truck.
- Medium Tactical Vehicle (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.

The Army modifies the standard variants for specific mission equipment packages, such as transport for air defense radar and High-Mobility Artillery Rocket System rocket launchers.

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

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. In 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 (IED) threats and exploitation testing. The FMTV LVAD MTV cargo truck airdrop testing was conducted from November 2023 through February 2024, and the LVAD LMTV cargo truck variant was airdrop tested December 2024 through April 2025. DOT&E personnel observed airdrop testing of the FMTV A2 LVAD MTV and LMTV cargo trucks and supported the assessment that the FMTV A2 is operationally effective and suitable.In March 2025, DOT&E published a classified LFT&E report with the results of the live fire testing and survivability assessment to inform the Army's full materiel release decision in FY27. DOT&E removed FMTV A2 from oversight later that month due to completion of operational and live fire testing and associated reporting requirements.

» MAJOR CONTRACTOR

- Oshkosh Defense, LLC – Oshkosh, Wisconsin

TEST ADEQUACY

From December 2023 through June 2024, the Army conducted LFT&E at Aberdeen Proving Ground, Maryland, to confirm the LVAD cab did 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 IEDs, and one under-vehicle blast mine test of the MTV LVAD cargo truck. The Army executed the LFT&E in accordance with DOT&E-approved test plans. DOT&E observed these tests, which were adequate to assess the vehicle's survivability. DOT&E published a classified LFT&E report with the results of this testing in March 2025.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

DOT&E has no changes to the assessment in the FY24 Annual Report for operational effectiveness and suitability.

» SURVIVABILITY

DOT&E's assessment of the LVAD variant's survivability is classified and can be found in the LFT&E report published in March 2025.

RECOMMENDATIONS

The Army should:

1. Continue to address DOT&E's recommendations from the October 2023 FMTV A2 combined FOT&E and LFT&E report and the March 2025 FMTV A2 LVAD LFT&E report.
2. Notify DOT&E if the Army decides to recompete the production contract, changes the manufacturing process, or changes the production facility, so DOT&E can assess impacts.

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

In July 2025, the Launched Effects (LE) Product Office earned Army Acquisition Executive concurrence to proceed with the Air Launched Effects (ALE) program on the urgent capability acquisition pathway for FY25 – FY27. This acquisition strategy enables the LE Product Office to issue, iterate, and reissue LE systems in a way that is not only consistent with technology maturation but also meets the operational needs of Army warfighters. Due to the change in acquisition strategy, DOT&E removed the Future Unmanned Aircraft System – Air Launched Effects (FUAS ALE) program from oversight.

SYSTEM DESCRIPTION

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 OVERSIGHT HISTORY

FUAS ALE was a Middle Tier of Acquisition (MTA) program on the rapid prototyping pathway. DOT&E placed FUAS ALE on oversight in February 2023. An operational demonstration had been scheduled for 4QFY24, but the Army canceled it due to technology immaturity. The Army's replacement to ALE – now known as LE to cover both ground and air launched effects – was placed on the urgent capability acquisition pathway for FY25 – FY27. In July 2025, DOT&E removed the FUAS ALE program from oversight, because the Army has transitioned to the new acquisition approach.

HERCULES M88 Upgrade Recapitalization (M88A3)

In March 2025, the Army completed live fire testing to compare crew survivability, system survivability, and system functionality restoration of a combat-loaded M88A3 against the current model, M88A2, using realistic threats to support a production decision in June 2025. In July 2025, the Army canceled the M88A3 Upgrade Recapitalization effort and associated testing, so DOT&E did not publish an LFT&E report. As the Army is considering making upgrades to the M88A2 to improve vehicle reliability and maintainability, DOT&E intends to maintain oversight to monitor the potential upgrades.

SYSTEM DESCRIPTION

The Army had intended for the M88A3 to fill the capability gap of single-vehicle recovery of 80-ton vehicles by upgrading the M88A2's powerpack, suspension, hoist, and winch. The upgrades were intended to increase mobility, survivability, lift, winch, and tow capabilities necessary to recover the heaviest tracked vehicles in the Army.

MISSION

The Army intended for commanders to employ the M88A3 to provide single vehicle towing, winching, hoisting and evacuation of heavy tanks and other tracked combat vehicles. The Army intended to field M88A3 vehicles to brigade support battalions to perform recovery operations in support of combat-equipped M1, M1A1, and M1A2 Abrams Main Battle Tank platforms and future heavy combat vehicles, as well as lighter systems across the armored brigade combat team.

PROGRAM

The M88A3 was an Acquisition Category IC program using an Other Transaction Authority to complete the recapitalization effort. DOT&E originally put the M88A2 on oversight in June 2016 and has since transferred oversight focus to the M88A3 model. DOT&E approved the M88A3 TEMP in September 2023. The Army began developmental testing of the M88A3 in February 2024, and LFT&E in August 2024.

The Army had planned to conduct an FOT&E in 2QFY27 and to begin fielding the M88A3 in 1QFY28, but in July 2025, the Army canceled the M88A3 Upgrade Recapitalization program and all planned testing. The Army is considering making upgrades to the M88A2 to improve vehicle reliability and maintainability. DOT&E intends to maintain oversight to monitor potential upgrades and will update future annual reports as necessary.

» MAJOR CONTRACTOR

- BAE Systems, Inc. – Anniston, Alabama

TEST ADEQUACY

In March 2025, the Army completed live fire testing of the M88A3 at the Aberdeen Test Center, Maryland, in accordance with the DOT&E-approved LFT&E test plan, to inform a production decision in June 2025. DOT&E observed the testing. As the Army has since canceled the M88A3 Upgrade Recapitalization program, DOT&E did not report on test adequacy or survivability assessments.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

As the Army has canceled the program, DOT&E did not assess the M88A3's operational effectiveness, suitability, or survivability. DOT&E will maintain oversight of the M88A2's potential upgrades and will report on relevant testing and performance assessments as appropriate.

RECOMMENDATION

The Army should:

1. Provide to DOT&E for approval a T&E plan for assessing upgrades to the M88A2 once the plan for upgrades is finalized.

Indirect Fire Protection Capability Increment 2 (IFPC Inc 2)

From July to November 2024, the Army conducted an operational demonstration (Ops Demo) of the Indirect Fire Protection Capability Increment 2 (IFPC Inc 2) prototype system, which demonstrated some capability against its intended threat set. DOT&E published a classified IFPC Inc 2 Ops Demo report in April 2025. Additional testing is required to fully characterize the operational effectiveness, suitability, and survivability of IFPC Inc 2 prior to its combined Milestone C/full-rate production decision planned for 2QFY27.

SYSTEM DESCRIPTION

The IFPC Inc 2 system of systems is comprised of multiple subsystems and integrates with other existing systems to provide intended air defense capability.

The Army intends to employ IFPC Inc 2 as a platoon equipped with four IFPC launchers, an Army Integrated Air and Missile Defense (AIAMD) Engagement Operations Center (EOC), a Sentinel radar, and at least one AIAMD network relay. The Integrated Air and Missile Defense (IAMD) Battle Command System (IBCS) software provides command and control through the EOC, communicating across an IAMD Fire Control Network (IFCN).

The IFPC launcher is a palletized platform that includes up to three All-Up-Round Magazines (AUR-Ms), a generator, a user interface for launcher emplacement and initialization, and networking equipment to connect to an EOC. The IFPC launcher has an embedded GPS that provides positioning, navigation, and timing information to the launcher.

The launcher is in a container roll-out platform weapon system that enables it to be loaded, transported, and unloaded by the M-1075 Palletized Load System (PLS). The M-1076 PLS trailer/M-1074 PLS Crane are used to transport additional AUR-Ms and conduct magazine reloads. The AUR-M is intended to be self-contained and replaceable; AUR-Ms will not be reloaded with individual interceptors in the field.

The AIM-9X Block 2 Sidewinder is the first interceptor that will be integrated into the IFPC Inc 2 system. The AIM-9X is a supersonic guided missile that uses a passive infrared seeker for target acquisition and is currently employed by the Navy and Air Force as an air-to-air intercept capability. A missile data link provides target track updates to the IFPC Inc 2 interceptor while in flight.

The AN/MPQ-64 Sentinel is a rotating, X-band radar and is the primary fire control radar for the IFPC Inc 2 system. The Sentinel is designed to detect, track, identify, and classify air objects and provide radar track data to IBCS over the IFCN. The Sentinel A3 – a passive electronically scanned array radar – is currently the main fire control radar for the IFPC Inc 2 system of systems. However, the Sentinel A4 – an active electronically scanned array radar – is intended to replace the Sentinel A3 prior to IFPC Inc 2 IOT&E.

MISSION

The IFPC Inc 2 system is intended to provide 360-degree air and missile defense protection of fixed and semi-fixed assets at the corps and division levels, bridging the gap between tactical and strategic air and missile defense capabilities. IFPC Inc 2 is part of the AIAMD system-of-systems architecture and will contribute to the Army's layered air defense strategy. IFPC Inc 2 can be employed as an IFPC platoon or as part of a larger AIAMD task force that includes additional sensors and shooters, such as Patriot, operating on a single IFCN. IFPC Inc 2 is part of the Army's planned initial capability for the IAMD of Guam.

PROGRAM

In August 2021, the Army Acquisition Executive approved IFPC Inc 2 to proceed under the Middle Tier of Acquisition (MTA) rapid prototyping (RP) pathway. From July to November 2024, the Army conducted an Ops Demo of the IFPC Inc 2 system in order to fulfill the program's MTA RP operational testing requirement and to inform the program's transition to the MTA rapid fielding pathway in April 2025. The Army deployed IFPC Inc 2 prototypes to South Korea in FY25. IOT&E is planned for FY26, with a full-rate production decision planned for 2QFY27.

The Army has yet to determine the final IFPC Inc 2 configuration. As a result, the Ops Demo platoon configuration may not be representative of the configuration that is ultimately fielded.

» MAJOR CONTRACTORS

- Dynetics, a subsidiary of Leidos – Huntsville, Alabama (launcher)
- Raytheon, a subsidiary of RTX – Tucson, Arizona (AIM-9X Sidewinder missile)

TEST ADEQUACY

The Army Test and Evaluation Command (ATEC) conducted the IFPC Inc 2 Ops Demo at White Sands Missile Range, New Mexico, from July to November 2024. The unit under test was an IFPC platoon comprised of soldiers from the 1-51 Air Defense Artillery (ADA) battalion and the 3-43 ADA battalion. The Ops Demo was not fully conducted in accordance with the DOT&E-approved test plan; ATEC coordinated the deviations with DOT&E, who observed the testing. Consequently, the Ops Demo did not generate the expected operational effectiveness data but did provide some insight into suitability and survivability. DOT&E published a classified IFPC Inc 2 Ops Demo report in April 2025.

The hardware- and software-in-the-loop phase of test was intended to provide a large set of simulated IFPC engagements, but the AIM-9X flyout modeling and simulation used during the Ops Demo was not accredited for its intended use prior to test execution and failed to simulate a missile flyout for most of the commanded engagements. As a result, DOT&E did not analyze performance from the hardware- and software-in-the-loop phase, and DOT&E's basis for assessment of operational effectiveness during the Ops Demo is limited to the two live missile flight tests.

All missile flight tests conducted during the Ops Demo were modified from the DOT&E-approved test plan, and one missile flight test with multiple targets was cancelled altogether. The unit executed only 22 of 52 planned launcher reload iterations due to the low reliability of the M-1074 reload vehicles. The Army assessed the cyber survivability of the launcher and AUR-M but did not assess cyber survivability of the system-of-systems for the IFPC platoon. The Army plans to conduct additional cyber testing during IOT&E.

PERFORMANCE

» EFFECTIVENESS

Soldiers operating the IFPC Inc 2 launcher demonstrated the ability to defeat a subset of threats the system is intended to protect against. Additional live testing is required to determine IFPC Inc 2 operational effectiveness against its complete threat set, including multiple threats, in an operationally realistic environment, including in a cyber- and electromagnetic-contested environment. Additional details can be found in the classified Ops Demo report published in April 2025.

» SUITABILITY

The IFPC Inc 2 launcher and AIAMD EOC experienced frequent communications faults during simulated missions, which impacted execution. Launcher reloads and preparations for movement and emplacement drills were conducted throughout the Ops Demo using weight-representative inert magazines. M-1074 reload vehicles experienced two hydraulic leaks, rendering the cranes non-mission capable. The reload vehicle failures prevented the execution of 30 of the planned 52 reload drills. Additional details can be found in the classified Ops Demo report published in April 2025.

» SURVIVABILITY

DOT&E is unable to determine the survivability of IFPC Inc 2 in a cyber- and electromagnetic-contested environment, as the cyber testing conducted during the Ops Demo was not executed in a system-of-system construct and lacked operational realism. Additional details can be found in the classified Ops Demo report published in April 2025.

RECOMMENDATIONS

The Army should:

1. Conduct future live tests to characterize system performance against multiple threats in a cyber- and electromagnetic-contested environment.
2. Conduct cyber survivability testing in a system-of-systems construct.
3. Verify, validate, and accredit all relevant modeling and simulation tools before IFPC Inc 2 IOT&E begins.

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

In 1Q – 3QFY25, the Army conducted the Integrated Personnel and Pay System – Army (IPPS-A) Increment II Release 3 verification of fixes test (VFT) to evaluate remaining findings from the limited user test (LUT) that completed in February 2024. The VFT showed that the system no longer requires most of the workarounds needed during the LUT. In July 2025, DOT&E removed IPPS-A Increment II from oversight because testing to inform formal acquisition decisions is complete.

SYSTEM DESCRIPTION

IPPS-A is the Army's 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 program management office plans to continue to develop IPPS-A to deliver a full set of 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 Increment II is a Business Systems Category I program using the Scaled Agile Framework (SAFe®) development method to continue development and deployment of additional capabilities beyond the IPPS-A Increment II Release 3, which subsumed the majority of personnel systems across the Army Active Duty, Reserve, and National Guard components. DOT&E placed IPPS-A on oversight in 2010. IPPS-A continues to develop the IPPS-A Army Military Payroll capability to provide full pay functionality for all three Army components.

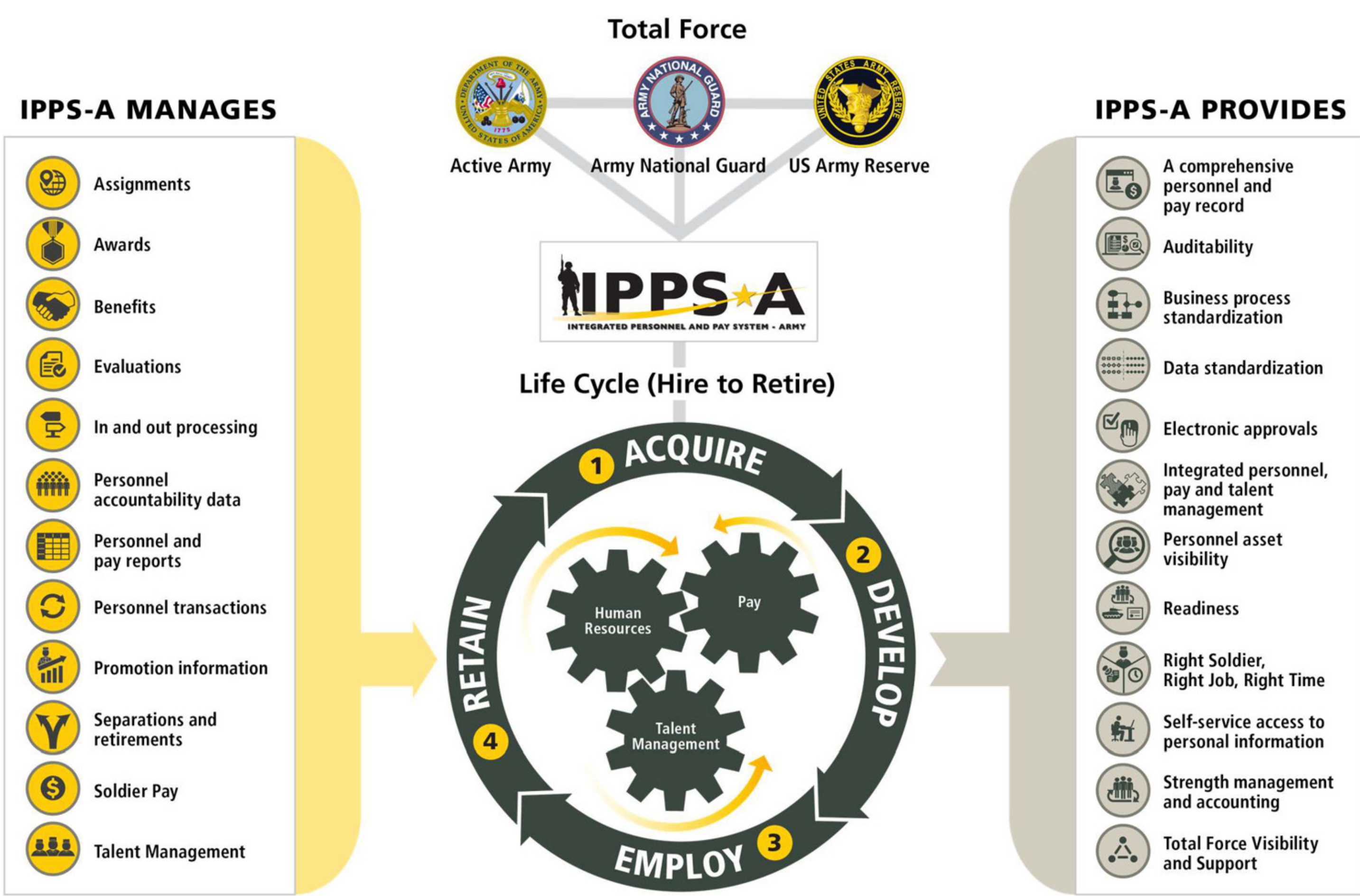
In July 2025, DOT&E removed IPPS-A Increment II from oversight because testing to inform formal acquisition decisions is complete.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

The Army Test and Evaluation Command (ATEC) conducted a LUT for IPPS-A Increment II Release 2 in 2019, focusing



on the Army National Guard deployment. ATEC then conducted the IPPS-A Increment II Release 3 LUT in two phases between 2022 and 2023, to evaluate the system as released to all three Army components. DOT&E identified deficiencies in IPPS-A Increment II Release 3, and the Army then conducted a VFT between 1Q – 3QFY25 to address the outstanding problems, in accordance with a DOT&E-approved test plan. During the VFT, ATEC gathered data from vendor testing and operations, and solicited user feedback in the form of structured interviews and surveys. The VFT included members of all three Army components (Active Duty, Reserve, and National Guard). In parallel, the Threat Systems Management Office executed a portion of the VFT to evaluate cyber fixes implemented since the LUT. DOT&E monitored the data collection during the VFT.

PERFORMANCE

» EFFECTIVENESS

IPPS-A Increment II Release 3 is operationally effective for most of its personnel tasks. During the VFT, ATEC found that users no longer needed to utilize the unsustainable workarounds required during the LUT, because the functionality was now operational in IPPS-A. Inbound interfaces still have intermittent problems, but ATEC has estimated such problems have minimal operational impact.

The two main functionalities that IPPS-A Increment II has yet to fully subsume are: (1) talent management and (2) readiness and manning. For readiness and manning functions, the Active Duty component uses the Service for the Analytics and Business Intelligence Reports tool. As planned, the Active Duty component had not fully transitioned to the IPPS-A talent management tool as of the VFT, limiting the evaluation of that area.

The Army Human Resources Command (HRC) service center and over 10,000 customer relationship management groups around the world provide support for IPPS-A users. The HRC uses a help desk ticket system to track and resolve problems. The number of open pay-impacting tickets remained consistent from February 2024 through May 2025, with between 4,000 and 5,000 pay-impacting tickets open at any given time.

» SUITABILITY

IPPS-A Increment II Release 3 is operationally suitable for most of its personnel tasks. During the VFT, HR professional users rated the usability of IPPS-A slightly higher than during the second phase of the LUT, though the usability rating is “marginal.” Leaders and self-service users also rated usability as marginal on average, with no significant changes in rating compared to the ratings during the second phase of the LUT. Users reported inconsistencies in terminology across the system. They also reported they had difficulty navigating to certain functions and often required help, either from the documentation or by consulting other users. The backlog of HR tickets remains at similar levels as when DOT&E reported last year, but the backlog of IT tickets has decreased.

» SURVIVABILITY

ATEC found during the VFT that the previously identified cyber survivability findings have been remediated.

RECOMMENDATION

The Army should:

1. Continue to iteratively test IPPS-A Increment II, including operational testing, through the full release of the Army Military Payroll capability. Testing should be conducted in an operationally realistic environment with all representative interfaces.

Integrated Visual Augmentation System (IVAS)

In February 2025, Microsoft submitted a request for Army approval to novate the Integrated Visual Augmentation System (IVAS) contract to Anduril. The Army approved the novation in April 2025, recognizing Anduril as the IVAS prime contractor. The Army canceled the IVAS 1.2 variant operational assessment (OA) that was scheduled for April 2025. The Army does not intend to test, produce, or field any IVAS variant systems in the future. Also in April 2025, the Army designated the next generation of IVAS as Soldier Borne Mission Command (SBMC) and released a Request for Solution to industry. The Army is scheduled to approve the SBMC program to use the Middle Tier of Acquisition (MTA) rapid prototyping (RP) pathway in December 2025. In future Annual Reports, DOT&E will report on SBMC systems as the replacement program to IVAS.

SYSTEM DESCRIPTION

The Army intended IVAS to function as a soldier-worn system to increase soldier lethality in all environments and battlefield conditions at the battalion-level and below. IVAS included a heads-up display (HUD), a body-worn computer known as a puck, a networked data radio, and three conformal batteries per soldier. IVAS was designed to provide 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-wideband network was intended to enable passive targeting capabilities by connecting the Family of Weapon Sights – Individual, mounted on a soldier's weapon, to the sight picture in the HUD. The IVAS radio enabled IVAS-equipped soldiers to transmit data within the company.

MISSION

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

PROGRAM OVERSIGHT HISTORY

In December 2022, the Army approved the IVAS 1.2 variant to use as the MTA RP pathway, and the technological insertion was awarded to Microsoft under the existing IVAS production Other Transaction Authority. The Army planned to conduct an IVAS 1.2 variant OA in April 2025 to inform a production decision and support the transition from the MTA RP pathway to a new acquisition pathway in August 2025. Fielding of the IVAS 1.2 variant was planned to begin in 1QFY26.

In February 2025, Microsoft submitted a request for Army approval to novate the Integrated Visual Augmentation System (IVAS) contract to Anduril. The Army approved the contract novation in April 2025 and canceled the IVAS OA.

In April 2025, the Army ceased testing. production and future fielding of IVAS 1.2 systems and announced that the follow-on effort to the IVAS 1.2, previously referred to as IVAS-Next, had been rebranded as the SBMC. The Army is scheduled to approve the SBMC program for use of the MTA RP pathway in December 2025. In future Annual Reports, DOT&E will report on SBMC systems as the replacement program to IVAS.

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). From July to August 2025, the Army conducted a cyber adversarial assessment on the LW CLU. DOT&E will publish an addendum to the classified FOT&E report in 2QFY26, once data analysis is complete. 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 into FY26.

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 and the Javelin Force-on-Force (FoF) Tactical Trainer (JTT) 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, informing a LW CLU production decision in October 2024. Urgent fielding of the LW CLU is expected to begin in 2QFY26.

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 is still ongoing. 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. 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.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

From July to August 2025, the Army conducted a cyber adversarial assessment on the LW CLU, in accordance with the DOT&E-approved test plan. DOT&E will publish an addendum to the classified FOT&E report with a cyber survivability assessment in 1QFY26, once data analysis is complete.

As discussed in the FY24 Annual Report, the Javelin Program Office identified the root cause of a software fault and developed LW CLU software update 4.1 and 4.1.1 to address the issue. The software updates have not yet undergone integrated testing with soldier operators. This should be completed prior to equipping the first unit with the LW CLU.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

DOT&E has no changes to the assessments in the FY24 Annual Report. DOT&E will publish an addendum to the classified FOT&E report in 1QFY26 to assess cyber survivability, once adversarial assessment data analysis is complete.

RECOMMENDATIONS

The Army should:

1. Conduct integrated testing of LW CLU software updates 4.1 and 4.1.1 with soldier operators prior to equipping the first unit.
2. 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,

as recommended in the FY23 and FY24 Annual Reports.

3. Investigate a long-term replacement strategy for the existing LW CLU battery to improve cold weather performance, as recommended in the FY23 and FY24 Annual Reports.
4. Develop the JTT to allow soldiers to conduct FoF exercises to support unit readiness.

Long Range Hypersonic Weapon (LRHW) – Dark Eagle

In December 2024, the Army and Navy completed the first successful end-to-end flight test for the Long Range Hypersonic Weapon (LRHW) (Dark Eagle) using a battery operations center (BOC) and a transporter-erector-launcher (TEL). In October 2025, DOT&E approved the Army's LRHW (Dark Eagle) Master Test Strategy. The Army intends to field two additional batteries of LRHW to complete the Middle Tier of Acquisition (MTA) rapid fielding phase by FY28. The Army also intends to complete an operational assessment (OA) in 4QFY26. DOT&E will publish a classified OA report once analysis is complete.

SYSTEM DESCRIPTION

The LRHW (Dark Eagle) is a prototype surface-to-surface long range strategic fires system composed of Army ground support equipment and eight All-Up-Round (AUR) missiles (designed by the Navy) packaged in Army AUR canisters (AUR+C). The Army ground support equipment is comprised of a BOC, a BOC Support Vehicle (BSV) and four TELs. The MTA rapid fielding effort only consists of the BOC, BSV, 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, theater and national strategic targets in support of multi-domain operations. Theater combatant commands, in coordination with U.S. Strategic Command, will execute mission planning and target engagement at the theater-level through the joint targeting cycle.

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 would use the MTA rapid fielding pathway and transferred the program, consisting of the Army ground support equipment, to Program Executive Office Missiles and Space.

The Army developed the LRHW Master Test Strategy and submitted it for DOT&E approval in August 2025, addressing a longstanding DOT&E recommendation. In October 2025, DOT&E approved the LRHW Master Test Strategy. The Army intends to field two additional batteries of LRHW to complete the MTA rapid fielding phase by 4QFY28.

The LFT&E Strategy, written by the Navy and addressing hypersonic targets, is captured in the Navy's current draft TEMP and is expected to be submitted for DOT&E approval in FY26.

The Navy's CPS program is the design authority for the common AUR, which will be employed by Navy *Zumwalt*-class destroyers and *Virginia*-class submarines, and will be employed by the Army's Dark Eagle system. The Army integrated AUR+C into LRHW in 3QFY25.

» 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

The first successful end-to-end flight test for the LRHW (Dark Eagle) using a BOC and a TEL was conducted in December 2024. As it was not an operational test, it did not require a DOT&E-approved test plan. However, the flight test data will help inform future operational test plan development.

The Army continues to collaborate with the Navy in their development of the Navy's LFT&E strategy for the AUR that will support the Army's program. The Navy's LFT&E Strategy includes representative targets. However, it is understood that the Army's threat environment is different than that of the Navy. 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 modeling and simulation (M&S) capability across the family of hypersonic weapon systems.

The initial CPS sled and flight tests the Navy conducted in FY24 did not include operationally representative targets and consequently provided no direct validation of the weapon's lethal effects. The Navy continues to investigate methods to obtain effectiveness and lethality data by incorporating representative targets into the CPS flight tests. Until the Navy characterizes 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, electromagnetic, cyber) threat-contested environment on the performance of the AUR, TEL, or BOC. This should include an end-to-end cyber survivability testing with both a cooperative vulnerability and penetration assessment and an adversarial assessment. The Army intends to conduct this testing from 1QFY26 to 2QFY27. 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.

The Army plans to conduct an OA beginning in 4QFY26. Upon completion of the OA, DOT&E will publish a classified OA report.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Insufficient data are available at this time to evaluate the operational effectiveness, suitability, and survivability of the LRHW system. Sufficient data for a full evaluation are not expected until completion of operational tests in 2QFY27. Following the completion of the OA, DOT&E will publish a classified report to assess LRHW progress toward operational effectiveness, suitability, and survivability.

RECOMMENDATIONS

The Army should:

1. Continue collaboration with the Navy on the LFT&E Strategy and ensure that it captures adequately verifying and validating the required M&S tools to create credible weaponeering and mission planning tools in support of the proposed operational fielding dates.
2. Test for full-spectrum survivability in a contested environment during the OA.
3. Conduct end-to-end cyber survivability testing to include a cooperative vulnerability and penetration assessment and adversarial assessment.
4. Coordinate with the Navy to ensure M&S outputs have been validated and combine with ground test data to support design of experiments and evaluation of operational effectiveness and survivability.
5. 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.

Lower Tier Air and Missile Defense Sensor (LTAMDS)

In December 2024, the Army Test and Evaluation Command (ATEC) completed an operational assessment (OA) of Lower Tier Air and Missile Defense Sensor (LTAMDS) prototypes. In April 2025, the LTAMDS program achieved Milestone C and officially transitioned to the major capability acquisition pathway. DOT&E approved the TEMP in March 2025. In April 2025, DOT&E published a classified OA report. The Army plans to execute additional operational testing in FY26 during the Integrated Fires Test Campaign 26 (IFTC 26). After the completion of LTAMDS IFTC 26 testing, DOT&E will publish a classified early fielding report to inform the issuance of systems to Guam.

SYSTEM DESCRIPTION

LTAMDS is intended to be a multi-function, multi-mission C-band, three-faced, fixed active electronically scanned array radar. It will provide simultaneous 360-degree coverage while dynamically adapting to the evolving threat environment. The radar will integrate with the Army's Integrated Air and Missile Defense (IAMD) Battle Command System (IBCS), to share information and support a common view of the battlespace for the warfighter. The Army plans for LTAMDS to support the full capability of the Patriot Advanced Capability (PAC)-2 and

PAC-3 family of interceptors and address capability gaps.

MISSION

Combatant commanders intend to deploy LTAMDS as part of: (1) a surveillance package with no weapons to support joint IAMD capability and (2) an IBCS-enabled Patriot Engagement Package with at least two Patriot launching stations for point defense of deployed forces and critical assets from missile and aircraft attacks in all weather conditions.

PROGRAM

LTAMDS is an Acquisition Category IC program that exited the Middle Tier of Acquisition (MTA) rapid prototyping pathway in October 2023. During the MTA rapid prototyping phase, the Army built eight prototypes. The LTAMDS program achieved Milestone C and major capability acquisition program designation in April 2025. DOT&E approved the TEMP in March 2025.

The LTAMDS schedule has shifted to the right since DOT&E approved the TEMP in March 2025. The TEMP reflected a full-rate production (FRP) decision in 1QFY28, with IOT&E planned during IFTC 26, approximately one year prior to the FRP decision. The Army has since moved the FRP date almost one year later, to the end of 4QFY28.

The Army has stated that the purpose of LTAMDS IFTC 26 testing is to support an evaluation of two specially configured LTAMDS intended for urgent materiel release (UMR) and limited initial fielding to Guam in FY27. That testing will not include cybersecurity or cyber/electronic warfare convergence testing, among other omissions. The documentation the Army provided indicates that the assets intended for testing during IFTC 26 are not representative of the LTAMDS low-rate initial production (LRIP) configuration. Therefore, after the completion of LTAMDS IFTC 26 testing, DOT&E intends to publish a classified early fielding report to inform the issuance of the two LTAMDS UMR prototypes to Guam.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX – Andover, Massachusetts

TEST ADEQUACY

ATEC conducted an eight-phased OA from July to December 2024 with three LTAMDS prototypes. Testing was not conducted in accordance with the DOT&E-approved test plan due to system and range limitations discovered during the OA. ATEC coordinated the necessary changes to the test with DOT&E. DOT&E observed the test and published a classified OA report in April 2025.

During the OA, LTAMDS participated in a missile flight test and other live events to demonstrate its capability against surrogate short-range ballistic missiles and air-breathing threats and its survivability against electronic attack. The OA included LTAMDS emplacement, displacement, and maintenance demonstrations to evaluate LTAMDS suitability. The OA also included a cooperative vulnerability and penetration assessment and an adversarial assessment to evaluate LTAMDS cyber survivability.

The OA yielded sufficient data to provide insight into LTAMDS effectiveness against air-breathing threats and into its suitability and survivability. Because DOT&E determined the modeling and simulation accreditation was not valid for the test, the OA did not provide insight into LTAMDS effectiveness against tactical ballistic missiles or survivability against anti-radiation missiles.

LTAMDS also participated in four developmental missile flight tests in FY25. These events demonstrated the system's capability in a non-operational setting and thus were not used for DOT&E's operational effectiveness assessment.

PERFORMANCE

» EFFECTIVENESS

DOT&E's April 2025 classified OA report provides an assessment of LTAMDS operational effectiveness against air-breathing threats. Insufficient data are available to assess LTAMDS operational effectiveness against tactical ballistic missiles at this time.

» SUITABILITY

LTAMDS is not currently suitable. During the OA, LTAMDS had low reliability and demonstrated unacceptably long emplacement and displacement times. LTAMDS also failed to meet some natural environmental qualifications and transportability requirements. Additional details are in the April 2025 classified OA report.

» SURVIVABILITY

DOT&E's April 2025 classified OA report provides an assessment of LTAMDS cyber survivability. Insufficient data are available to assess LTAMDS survivability against anti-radiation missiles at this time. Additional details are in the April 2025 classified OA report.

RECOMMENDATIONS

The Army should:

1. Update the LTAMDS program schedule to reflect IFTC 26 testing as an operational assessment supporting issuance of two UMR prototypes to Guam in 1QFY27.
2. Conduct IOT&E on LRIP-configured assets to support the FRP decision in 4QFY28.
3. Ensure the modeling and simulation tools required for LTAMDS performance evaluations are verified, validated, and fully accredited for their intended uses, prior to IOT&E.
4. Address the recommendations in the April 2025 classified OA report.

M10 Booker

The Army completed LFT&E at Aberdeen Proving Ground, Maryland, in March 2025 and IOT&E at Fort Stewart, Georgia, in April 2025. In June 2025, the Army Acquisition Executive published a directive cancelling the M10 Booker program. The Army has ceased production and canceled fielding. Due to the cancellation of the program, DOT&E removed the program from oversight in July 2025.

SYSTEM DESCRIPTION

The Army intended for the M10 Booker to provide infantry brigade combat teams (IBCTs) with a mobile, protected, direct fire capability against light armored vehicles, hardened enemy fortifications, and dismounted personnel. The M10 Booker was designed as a fully tracked armored combat assault vehicle, transportable on C-17 aircraft, and manned by a crew of four soldiers capable of firing a broad spectrum of munitions through use of its 105mm main gun and 7.62mm coaxial machine gun. The M10 Booker design included 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 intended 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. The Army envisioned IBCTs using the 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 OVERSIGHT HISTORY

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 as M10 Booker. DOT&E approved the IOT&E and the Live Fire Test Design Plan in August 2024 and observed all test events. The Army completed IOT&E in February 2025 and LFT&E in March 2025. Due to the cancellation of the M10 Booker program in June 2025, DOT&E removed the program from oversight in July 2025.

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

In February 2025, the Army approved Mounted Assured Positioning, Navigation, and Timing System (MAPS) Generation II (Gen II) for full-rate production (FRP). The Army completed fielding MAPS Gen II to Stryker brigade combat teams (SBCTs) in July 2025. The Army scheduled an FOT&E with armored brigade combat team (ABCT) vehicles in 2QFY26 to support a separate ABCT fielding decision in 4QFY26. In July 2025, DOT&E removed MAPS from oversight because program development has stabilized and there are no significant upgrade activities.

SYSTEM DESCRIPTION

MAPS Gen II 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 Gen II does not have an integrated screen and relies on other client systems to display PNT information to vehicle crews. MAPS Gen II 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 vehicles.

MISSION

A unit equipped with MAPS Gen II 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 Gen II 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 OVERSIGHT HISTORY

MAPS Gen II is an Acquisition Category II major capability acquisition program. It was part of the Army's Assured Positioning, Navigation, and Timing (A-PNT) Program, which DOT&E placed on oversight in 2015. DOT&E approved the Milestone C (MS C) TEMP in April 2022, as part of the oversight of A-PNT. DOT&E placed MAPS Gen II itself on oversight in July 2022.

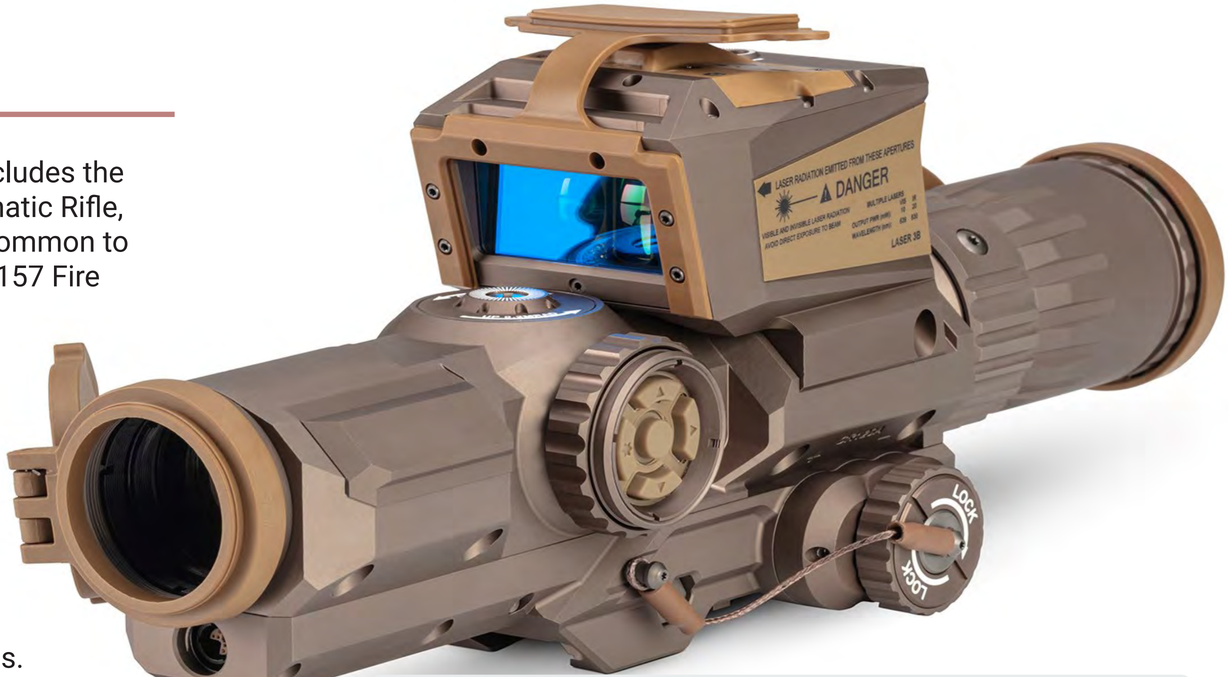
In January 2024, DOT&E approved the MAPS Gen II IOT&E test plan. The Army subsequently conducted the IOT&E in February 2024. In September 2024, DOT&E published a classified MAPS Gen II IOT&E report. The IOT&E report supported the February 2025 FRP decision and the fielding of MAPS Gen II to the SBCTs, completed in July 2025. The Army plans to conduct FOT&E focusing on ABCT vehicles in 2QFY26 to support a separate ABCT fielding decision. In July 2025, DOT&E removed MAPS from oversight because program development has stabilized and there are no significant upgrade activities.

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

Top: Next Generation Squad Weapon (NGSW) M7 Rifle
Bottom: NGSW M250 Automatic Rifle

The Army completed natural environment testing on the Next Generation Squad Weapon (NGSW) at the Arctic Regions Test Center in Fort Greely, Alaska, in February 2024; airborne and military free-fall testing at Fort Bragg, North Carolina, in August 2024; an operational assessment (OA) at Fort Campbell, Kentucky, in October 2024; and limited lethality testing of the 6.8mm Special Purpose (SP) ammunition at Aberdeen Proving Ground, Maryland, in December 2024. The Army anticipates completing LFT&E of the 6.8mm General Purpose (GP) ammunition by 2QFY26. DOT&E published an early fielding report (EFR) with a classified limited lethality annex on the 6.8mm SP ammunition in June 2025. DOT&E will report on the 6.8mm GP ammunition LFT&E results in a classified lethality report by 3QFY26. Due to the completion of operational testing (OT) and associated reporting to inform fielding and full-rate production (FRP) decisions, DOT&E removed NGSW Weapons and Ammunition (W&A) and Fire Control (NGSW-FC) from OT oversight in July 2025. NGSW W&A remains on live fire (LF) oversight.

SYSTEM DESCRIPTION



Next Generation Squad Weapon Fire Control (NGSW M157 FC)

The NGSW system includes the M7 Rifle, M250 Automatic Rifle, 6.8mm ammunition common to both weapons, and M157 Fire Control mounted on each weapon. The M7 and the M250 are replacements for the M4/M4A1 carbine and M249 Squad Automatic Weapon used in the close combat force (CCF), and special operations forces units. The M7 is fielded with seven 20-round magazines and has selectable safe, semi-automatic, and automatic firing modes. The M250 is fielded with two 50-round fabric ammunition pouches and three 100-round fabric ammo pouches, and has selectable safe, semi-automatic, and automatic firing modes. The M157 is a variable magnification direct view optic with laser range finder, aiming lasers, environmental sensors, ballistic solver, compass, wireless communication, and display overlay. The M157 replaces the current optics used by the CCF when issued NGSW systems.

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

MISSION

Units 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 conduct the following combat operations:

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

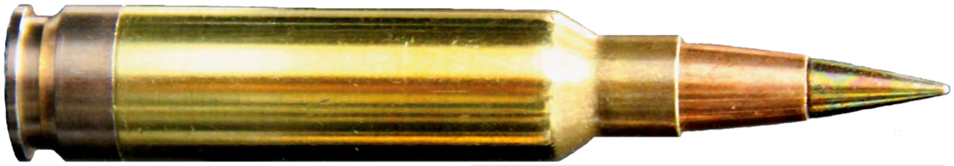
PROGRAM

The NGSW system consists of two distinct Middle Tier of Acquisition (MTA) programs: the NGSW W&A rapid fielding program and the NGSW-FC rapid fielding program.

The NGSW W&A program consists of the following components: M7, M250, and a common family of 6.8mm ammunition. NGSW W&A was approved as an MTA rapid fielding program in March 2022. In March 2024, the Army approved an urgent materiel release for the weapons and initiated fielding. In April 2024, the Army approved an urgent materiel release for the ammunition and issued it to units for use in new equipment training.

The NGSW-FC program consists of the M157 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 and began fielding that same month.

The Army completed an OA of the NGSW system in October 2024 and limited lethality testing of the 6.8mm SP ammunition in



6.8 x 51mm M1186 GP Ammunition

December 2024 to support the planned transition of both the NGSW W&A and NGSW-FC programs from the MTA rapid fielding pathway to separate major capability acquisition programs in 3QFY26. The Army anticipates completing LFT&E of the 6.8mm GP ammunition by 2QFY26.

DOT&E approved the TEMP for both the NGSW W&A and NGSW-FC programs in August 2023, the OT test plan in August 2024, and the LFT&E plan in September 2024. Due to the completion of OT and associated reporting to inform fielding and FRP decisions, DOT&E removed NGSW W&A and NGSW-FC from OT oversight in July 2025. NGSW W&A remains on LF oversight.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

The Army completed natural environment testing at the Arctic Regional Test Center in Fort Greely, Alaska, in February 2024; airborne and military free-fall testing at Fort Bragg, North Carolina, in August 2024; an OA at Fort Campbell, Kentucky, in October 2024; and limited lethality testing of the 6.8mm SP Ammunition at Aberdeen Proving Ground, Maryland, in December 2024. The operational and lethality testing was conducted in accordance with DOT&E-approved test plans, observed by DOT&E personnel, and was adequate to assess the operational effectiveness, lethality, suitability, and cyber survivability of a unit equipped with the NGSW. DOT&E published an NGSW W&A and NFSW-FC EFR, with a classified limited lethality annex on the 6.8mm SP ammunition, in June 2025.

The Army anticipates completing LFT&E of the 6.8mm GP ammunition at Aberdeen Proving Ground by 2QFY26. DOT&E will report on the 6.8mm GP ammunition LFT&E results in a classified lethality report in 3QFY26.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

DOT&E's assessment of M7, M250, M157's operational effectiveness, suitability, and cyber survivability, and the lethality of the 6.8mm SP ammunition are provided in the June 2025 EFR and classified limited lethality annex, respectively. The EFR assesses individual soldier and squad performance using the NGSW system on static and maneuver ranges; highlights the weapons' suitability and soldiers' safety concerns; and compares performance of the SP ammunition to that of current ammunition against specific types of targets. Assessments in the report include:

- Individual soldiers consistently qualified with their NGSW and, when firing on the variable distance range, demonstrated the ability to engage targets at extended distances.
- The 6.8mm SP ammunition generally provides increased lethality over the M855A1 (i.e., the SP ammunition for the legacy M4A1 weapon) against the tested targets.
- Improvements to system reliability, safety, human-systems integration, and compatibility with cold weather operations are needed.
- During the OA, soldiers reported negative physiological effects caused by the noxious off-gassing from their weapons, as well as concerns about the extreme heat from the weapons' suppressors after firing.
- Most M250s equipped with M157s did not retain zero during the OA or the airborne test.
- Ergonomic complaints about the M157 persisted.
- The NGSW is compatible and safe for use during static line and military free-fall airborne operations.

RECOMMENDATION

The Army should:

1. Address the recommendations in the June 2025 EFR and classified limited lethality annex.

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

In FY25, the Army decided that no new investment will go into the Stryker platform after FY26. The Nuclear Biological Chemical Reconnaissance Vehicle Sensor Suite Upgrade (NBCRV SSU) had been intended as a NBCRV Stryker-specific upgrade, but the program office is currently developing a testing strategy for a platform-agnostic SSU, which will leverage the sensors that would have gone into the NBCRV SSU Capability Set (CS) 2.2 upgrade. In July 2025, DOT&E removed NBCRV SSU from oversight because the Army is no longer investing in the Stryker platform.

SYSTEM DESCRIPTION

The NBCRV is the Army's mounted chemical, biological, radiological, and nuclear (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 agent vapors at standoff.
- The Joint Chemical Agent Detector allows the operators to detect and identify chemical agent vapors 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 Imaging 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 OVERSIGHT HISTORY

The NBCRV SSU is an Acquisition Category II program testing an engineering change proposal to the M1135 Stryker NBCRV, a system currently in operations and sustainment. DOT&E originally put NBCRV on oversight in September 2018. In February 2023, DOT&E continued oversight of the NBCRV SSU for the engineering change proposal.

In September 2023, the Army completed testing in accordance with the DOT&E-approved TEMP for CS 2.1, to include an operational demonstration in September 2023. The program also conducted a Soldier Touchpoint in September 2024. Live fire testing was completed in October 2024.

In FY25, the Army decided that no new investment will go into the Stryker platform after FY26; however, the SSU will still be pursued. The Army has not yet determined which platform the SSU will be on. However, the program will continue testing sensors as a platform-agnostic suite until a platform is chosen. The program is currently reevaluating which sensors will be a part of the SSU for CS 2.2 and what testing will be needed. In July 2025, DOT&E removed the NBCRV SSU program from oversight because the Army is no longer investing in the Stryker platform.

Precision Strike Missile (PrSM)

In December 2024, the Army completed a limited user test (LUT) of the Precision Strike Missile (PrSM) Increment 1 (Inc 1) as a risk reduction for the IOT&E and to support a Milestone C (MS C) decision in July 2025. From November 2024 through April 2025, the Army executed the final eight production qualification test (PQT) events. In July 2025, DOT&E published a classified PrSM Inc 1 operational assessment (OA) report, covering findings from the LUT and PQT events. In May 2025, the Army conducted an adversarial assessment (AA) prior to IOT&E. From May through September 2025, the Army completed the IOT&E to support a full-rate production (FRP) decision scheduled for 2QFY26. DOT&E will publish a classified IOT&E report in early 2QFY26 to inform the FRP decision.

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 a wide variety of precisely and imprecisely located targets.

PROGRAM

The PrSM Inc 1 is an Acquisition Category IB Major Defense Acquisition Program. The Army plans to field four increments of the PrSM, with PrSM Inc 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. The Army expects to field an initial operational capability by 2QFY26 and a full operational capability by 2QFY27.

In June 2021, DOT&E approved the MS B TEMP, which supported the MS B decision in September 2021. The MS C decision occurred in July 2025. In August 2025, DOT&E approved the MS C TEMP. DOT&E's MS C TEMP approval had the following caveat: The Army should resource additional missiles to increase the confidence and likelihood that the number of missiles tested will be adequate to allow for DOT&E to conduct an integrated operational effectiveness and suitability evaluation; inform the Army's tactics, techniques, and procedures; and inform multiyear procurement quantities.

» MAJOR CONTRACTOR

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

TEST ADEQUACY

In December 2024, the Army completed a LUT, in accordance with a DOT&E-approved operational test plan, as a risk reduction for the IOT&E and to support the MS C decision in July 2025. Between February and April 2025, the Army executed the final eight PQT shots. Cumulatively, the LUT, PQT shots, and a cooperative vulnerability and penetration assessment conducted in September 2024 were adequate to assess the PrSM's progress towards operational effectiveness (including lethality), suitability, and cyber survivability. DOT&E published a classified PrSM Inc 1 OA report in July 2025 with those findings.

In May 2025, the Army conducted an AA prior to IOT&E, in accordance with a DOT&E-approved cyber test plan. From May through September 2025, the Army executed IOT&E, in accordance with a DOT&E-approved operational test plan, to inform the FRP decision scheduled for 2QFY26.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

DOT&E's assessment on the PrSM's progress toward operational effectiveness (including lethality), suitability, and cyber survivability is classified. Details can be found in the July 2025 OA report.

DOT&E will evaluate the operational effectiveness, lethality, suitability, and cyber survivability of PrSM following the completion of IOT&E in September 2025. DOT&E will publish a classified IOT&E report in 2QFY26.

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, as recommended in the FY24 Annual Report.
2. Provide additional resourcing to ensure reliability testing is completed with statistical confidence.

Sentinel A4 Radar

In FY25, the Army divided the AN/MPQ-64A4 Sentinel (Sentinel A4) radar program's IOT&E into two phases. The Army Test and Evaluation Command (ATEC) conducted IOT&E Phase 1 from February through April 2025. IOT&E Phase 2 is scheduled for 2QFY26, during the Integrated Fires Test Campaign 2026 (IFTC 26). DOT&E has concerns about the adequacy of IOT&E Phase 2 since it will not test some of Sentinel A4's critical capabilities, nor will it be integrated with the concurrent IOT&E of the key launcher it is intended to support. Following the completion of IOT&E, DOT&E will provide an assessment of the Sentinel A4's operational effectiveness, suitability, and survivability in a classified report to inform the full-rate production (FRP) decision.

SYSTEM DESCRIPTION

The Sentinel A4 radar is a three-dimensional X-band active electronically scanned array radar developed to replace the legacy Sentinel A3 and improve short- and medium-range air defense capabilities. It is designed to detect, classify, and track multiple aerial threats, including rockets, artillery, mortars, cruise missiles, unmanned aircraft systems, and fixed- and rotary-wing aircraft. The radar is mounted on a modified M1095 Medium Tactical Vehicle trailer, towed by an M1083 Family of Medium Tactical Vehicles A2 (FMTV A2) cargo truck carrying the generator and communications equipment. The system is operated by a two-person crew.

MISSION

Army Air Defense Artillery units plan to employ the Sentinel A4 radar to provide 360-degree hemispherical surveillance and fire-control-quality tracking for short- and medium-range air defense engagements. The radar is designed to integrate into either the Forward Area Air Defense Command and Control network or the Army Integrated Air and Missile Defense (AIAMD) architecture via the Integrated Battle Command System, providing target track data to air and missile defense interceptors. The Sentinel A4 radar is intended to support both fixed-site defense missions and maneuvering forces. The Army also intends to use the Sentinel A4 radar in the Defense of Guam architecture.

PROGRAM

The Sentinel A4 radar is an Army Acquisition Category II program within the major capability acquisition pathway. As the radar is a critical component of the Army air defense mission, DOT&E placed the program under operational test oversight in February 2023, and the Milestone Decision Authority, Program Executive Office Missiles and Space, approved Milestone C in July 2023. In March 2024, DOT&E approved the program's TEMP, which planned a single-event IOT&E to support a September 2025 FRP decision.

In FY25, the Army split the Sentinel A4 IOT&E into two phases and moved the Sentinel A4 FRP date from September 2025 to 4QFY26. In March 2025, DOT&E informed the Army that due to the lack of funding and production-representative assets, the IOT&E Phase 1 test plan that ATEC submitted to DOT&E for approval was not adequate to evaluate Sentinel A4's operational effectiveness, suitability, and survivability. DOT&E subsequently acknowledged a test plan change request in May 2025 that indicated the Army's intention to conduct cybersecurity and electronic warfare testing in the second phase of IOT&E.

The Army plans for IOT&E Phase 2 to occur in 2QFY26 during IFTC 26 as a standalone event instead of integrated with the IOT&E of its primary engagement system – the Indirect Fire Protection Capability Inc 2 (IFPC Inc 2) launcher – which is planned to begin six weeks later at the same location during IFTC 26. While the Army acknowledges that these systems were intended to undergo IOT&E concurrently in support of testing for the Defense of Guam, it stated that combining the IOT&Es, as originally planned, does not support the Sentinel A4 4QFY26 FRP decision date.

Due to the lack of sufficient low-rate initial production (LRIP) radars and production-representative FMTV trucks to support IOT&E Phase 2, the Army plans to use one LRIP radar and production-representative FMTV A2 truck and two pre-LRIP prototype radars, both connected to FMTV A1P2 trucks instead of FMTV A2 trucks. The Army has not yet submitted to DOT&E an updated TEMP reflecting the revised two-phased test strategy, the associated resources, and planned FOT&E. To ensure adequate testing, it is important that the revised plan include testing of critical capabilities the radar was intended to provide and include the cybersecurity and electronic warfare testing the Army committed to executing in IOT&E Phase 2. There is a risk that if the sole LRIP radar becomes unavailable during IOT&E Phase 2, the Army will be unable to collect data from any production-representative test assets for that phase of IOT&E. Despite the presence of a Sentinel A3 radar at the IFTC 26 test site, the Army has elected not to do a direct comparison between A3 and A4 to ensure no capability decrement.

» MAJOR CONTRACTOR

- Lockheed Martin Corporation – Syracuse, New York

TEST ADEQUACY

ATEC conducted IOT&E Phase 1 at White Sands Missile Range, New Mexico, from February through April 2025. DOT&E and the Army observed that the test did not include production-representative Sentinel A4 radar assets, operationally realistic network configurations, or the appropriate engagement systems intended to receive and use the radar's outputs to initiate an engagement. DOT&E is now coordinating with the Army to assess whether the testing planned in the second phase of IOT&E will be adequate to evaluate the system's operational effectiveness, suitability, and survivability.

The Army had planned for the Sentinel A4 radar to participate in IFTC 26 operational test events that integrated with AIAMD architecture and other air and missile defense sensors and shooters. Instead, these systems will be tested separately to accommodate the Sentinel A4 FRP date of 4QFY26. These events, whether standalone or integrated, 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 radar 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's operational effectiveness, suitability, and survivability following the completion of IOT&E.

RECOMMENDATIONS

The Army should:

1. Consider moving the Sentinel A4 FRP decision date one quarter to the right, from 4QFY26 to 1QFY27, to allow for an integrated IFTC 26 IOT&E that includes both the Sentinel A4 sensor and the IFPC Inc 2 launcher, as the Army originally intended.
2. Execute IOT&E Phase 2 in accordance with the DOT&E-acknowledged operational test plan change request, addressing all capability areas not tested in Phase 1 and including production-representative radars.
3. Develop M&S tools, along with a verification, validation, and accreditation strategy, to support future Sentinel A4 radar operational testing, as recommended in the FY24 Annual Report.
4. In accordance with DoD Instruction 5000.98, update the Sentinel A4 TEMP for its 4QFY26 FRP decision to reflect testing the program will be unable to complete prior to FRP and how those testing gaps will be addressed post-FRP.

Soldier Protection System (SPS)

The Army continues to field the Second Generation Modular Scalable Vest (MSV Gen II), Third Generation Vital Torso Protection (VTP Gen III) hard armor plates, and Next Generation Integrated Head Protection System (NG IHPS). The Army is pursuing to acquire a new VTP lightweight design for some Class I threats which complement existing VTP designs for Classes II and III. In FY25, the Army completed First Article Testing (FAT) for the lightweight design from two vendors.

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 at a reduced weight. The SPS is a modular system and provides 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.

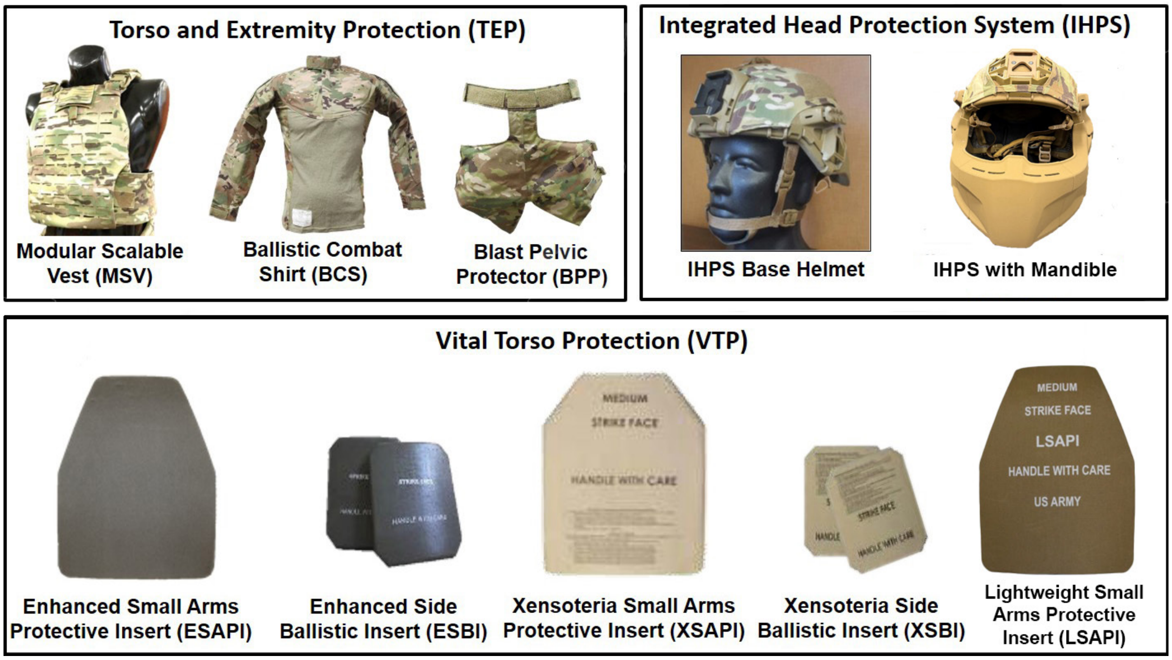
MISSION

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 subsystems are all Acquisition Category III programs. The three major subsystems are 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 is undergoing follow-on engineering change proposal efforts:

- MSV Gen II is replacing the Improved Outer Tactical Vest Gen III, the most widely proliferated



vest in the Army. The MSV Gen II provides handgun and fragmentation protection.

- The Army is transitioning to standalone plate technology eliminating the need for additional soft armor under the plate to meet minimum threshold performance requirements. The classes of plates with the program's respective plate types are as follows:
  - Class I (general purpose threats) - Lightweight Small Arms Protective Insert (LSAPI).
  - Class II (armor piercing threats) - Enhanced Small Arms Protective Insert (ESAPI) and Enhanced Side Ballistic Insert (ESBI).
  - Class III (advanced armor piercing) - Xenosteria Small Arms Protective Insert (XSAPI) and Xenosteria Side Ballistic Insert (XSBI).
- NG IHPS has replaced IHPS.

The Army started early fielding of MSV Gen II and VTP Gen III ESAPI/ESBI plates in 4QFY21 and plans to field through 4QFY28. The Army plans to field LSAPI Gen I plates through FY29. The target acquisition quantity is 190,618 ESAPI/ESBI sets of plates and 196,821 LSAPI sets of plates. The Army is still determining XSAPI Gen IV quantities. The Army started fielding of the IHPS Gen II in February 2024 to the 82nd Airborne Division. The Army is expected to reach LSAPI initial operational capability in 1QFY27.

» 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, LSAPI)
- Integris Composites – Hebron, Ohio (ESAPI, XSBI)
- Hardwire, LLC – Pocomoke City, Maryland (LSAPI)

NG IHPS Vendors:

- Avon Protection – Salem, New Hampshire
- Gentex Corporation – Carbondale, Pennsylvania
- Leading Technology Composites, Inc. – Wichita, Kansas

TEST ADEQUACY

The Army conducts multiple FATs and Lot Acceptance Tests (LATs) every year to qualify new vendors and designs. In FY25, the Army completed FAT for two vendors that produced LSAPI designs. The designs that passed FAT will proceed to LAT in 1QFY26. The Army completed all test series at Aberdeen Test Center, Maryland, in accordance with DOT&E-approved test plans. DOT&E observed some of the FAT.

In July 2025, DOT&E published the Hard Body Armor Test Protocol for FAT and LAT, an update to the 2010 protocols, to incorporate T&E best practices and provide a standardized methodology that can be used for testing across all Services. Representatives from the Army, Marine Corps, Navy, U.S. Special Operations Command, and Defense Logistics Agency participated in the development and review of the protocol. This protocol applies to future hard body armor contracts across the DoW; it is not intended to be applied against already qualified designs, already accepted lots, or to LATs for lots produced from designs not qualified using this protocol for FAT. Given the updated protocol and LATs being conducted at a government facility, DOT&E will no longer be reporting LAT results in the annual report.

The Army completed an expanded developmental test series for VTP Gen III ESAPI against fragment simulating projectiles for one ESAPI vendor in 1QFY25; the test series was previously conducted on the other ESAPI vendor in 1QFY24.

The Army plans to conduct full-up system-level (FUSL) testing in FY26 in accordance with a DOT&E-approved test plan to assess potential injuries to soldiers from threats that penetrate the NG IHPS, and to compare the results with the legacy IHPS protection.

After completion of the NG IHPS FUSL testing, DOT&E plans to publish a classified survivability report on the VTP Gen III and NG IHPS in 3QFY26.

The Army is currently drafting a T&E Strategy update that will include the scope and timeline for additional testing, beyond FAT, for the LSAPI plates and future VTP Gen IV plates.

Current test methods for personal protective equipment 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. In response to a recommendation from the FY22 – 24 Annual Reports, the Army is working to develop and accredit the Hybrid Foam Mannequin or other surrogate methods to address this limitation by 4QFY27.

The Army started the NG IHPS FAT for a new vendor, Leading Technology Composites, Inc., in September 2025, in accordance with the DOT&E-approved test plan.

PERFORMANCE

» SURVIVABILITY

Two LSAPI designs were submitted and tested in FY25 and met the ballistic FAT requirements. Additional testing is required to assess the performance of the LSAPI plates against additional operationally realistic threats and conditions.

Additional testing is required to assess the degree of potential injuries to warfighters from penetrating threats to the NG IHPS. FUSL testing is planned for FY26.

RECOMMENDATIONS

The Army should:

1. Submit a T&E Strategy update to DOT&E for approval, outlining the scope and timeline for testing of the LSAPI and future VTP Gen IV designs.
2. Update the SPS security classification guide to include new generation equipment.
3. Continue to develop methodologies and collect necessary data to improve modeling and simulation capabilities, allowing assessments of potential warfighter injuries for a range of conditions not tested.

Stryker Family of Vehicles (FoV)

In FY25, the Army conducted no operational testing on any variant in the Stryker Family of Vehicles (FoV). DOT&E removed the program from oversight in July 2025 because program development has stabilized, and there are no significant upgrade activities planned to the Stryker FoV fielded to Stryker brigade combat teams (SBCTs).

SYSTEM DESCRIPTION

The Stryker FoV is comprised of multiple variants of the eight-wheeled Stryker vehicle. The variants are equipped with unique mission-essential equipment to enable the accomplishment of a wide-range of tasks in support of unit-level mission command operations, employment of organic mortar fires, medical evacuation, transport of troops, and reconnaissance, engineering, and anti-tank missions.

MISSION

SBCTs employ the Stryker FoV to conduct offensive and defensive missions in support of multi-domain operations. The Stryker was designed and optimized primarily for employment in small-scale contingency operations in asymmetric, noncontiguous environments, confronting low-end and mid-range threats that may employ both conventional and asymmetric capabilities. Recent lethality upgrades, such as the CROWS-J and Double-V Hull A1 30mm, provided increased firepower to the SBCT to allow the formation to engage with near-peer mechanized infantry forces without augmentation.

PROGRAM OVERSIGHT HISTORY

The Army initiated the Interim Armored Vehicle program (later renamed Stryker) in 2000 to provide combatant commanders with a force more strategically deployable than armor forces, and with greater tactical mobility than light infantry forces. DOT&E approved the initial Stryker TEMP in November 2000 and an updated TEMP in May 2003. The Army began full-up system-level testing of production-representative configurations in July 2002, and completed IOT&E at Fort Knox, Kentucky, in 2003. In February 2004, DOT&E published a classified combined OT&E and LFT&E report on the Stryker FoV to inform the Army's original full-rate production decision.

In the two decades that followed, the Army conducted numerous engineering change proposal (ECP) modifications to the Stryker FoV to improve survivability, lethality, mobility, and situational awareness, while continuously integrating new mission essential packages on multiple variants. DOT&E was involved in the planning of LFT&E and FOT&E of major ECP efforts and published numerous classified and unclassified test reports assessing the operational effectiveness, suitability, and survivability of Stryker variants. Because program development has stabilized and there are no significant upgrades activities planned to the Stryker FoV fielded to SBCTs, DOT&E removed the Stryker FoV from oversight in July 2025.

Synthetic Training Environment Live Training Systems (STE-LTS)

Synthetic Training Environment – Live Training Systems Increment 1 (STE-LTS Inc.1) is a Middle Tier of Acquisition (MTA) program on the rapid prototyping (RP) pathway. The STE-LTS Program Office is developing the training devices, weapon engagement simulation, and instrumentation used to conduct live (force-on-force) collective training from the squad level to the brigade level. In July 2025, DOT&E determined that the program no longer requires oversight and removed STE-LTS from the oversight list.

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 antiaircraft 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 OVERSIGHT HISTORY

STE-LTS is an MTA RP program comprised of three planned increments of training capability development that will transition to the MTA rapid fielding or the major capability acquisition pathway for product maturation, production, and fielding. DOT&E placed the STE-LTS program on oversight in February 2023. In August 2024, DOT&E published a STE-LTS Inc. 1 Operational Demonstration report. In July 2025, DOT&E determined that the program no longer requires oversight and removed STE-LTS from the oversight list.

Terrestrial Layer System Brigade Combat Team (TLS BCT)

In July 2025, DOT&E removed the Terrestrial Layer System Brigade Combat Team (TLS BCT) programs from oversight. The TLS BCT Middle Tier of Acquisition (MTA) rapid prototyping (RP) program was removed because the Army cancelled the program. The TLS BCT Manpack (TLS BCT MP) MTA rapid fielding (RF) program was removed from oversight because the program had stabilized and no longer required oversight.

SYSTEM DESCRIPTION

The Army envisioned the TLS BCT as the next generation tactical system, delivering an integrated suite of signals intelligence (SIGINT), electronic warfare (EW), and cyberspace operations capabilities (future objective requirement) to enable multi-domain operations within the SIGINT Collection and EW Team. The Army had planned to deploy TLS BCT variants to Stryker BCT (SBCT), armored BCT (ABCT), and infantry BCT (IBCT) units.

TLS BCT was intended to modernize 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 would 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 had intended 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 was intended to be a man-packable configuration, and was transitioned to a separate MTA program known as TLS BCT MP. Each variant was 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 was intended to provide 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 was intended to operate on-the-move, at-the-halt, or dismounted, and near the forward lines of operating troops.

PROGRAM OVERSIGHT HISTORY

TLS BCT entered the MTA RP pathway in May 2020. DOT&E placed TLS BCT on oversight in January 2022. The Army conducted an operational demonstration (Ops Demo) for TLS SBCT in September 2023 to inform an MTA RF transition decision. The Ops Demo was adequate to identify operational issues related to combining SIGINT and EW capabilities onto one platform. Based on the results, the Army decided to separate TLS SBCT into two distinct variants: SIGINT and EW.

In March 2025, the Army determined that current requirements demonstrated during the MTA RP phase did not meet the Army's mission needs and halted further prototyping efforts for the SBCTs and ABCTs, pending revised requirements. The Army terminated the TLS BCT MTA RP program in July 2025. Based on the termination, DOT&E removed the TLS BCT MTA RP program from oversight later that month.

TLS BCT MP entered the MTA RP pathway as a TLS BCT variant in May 2020. The Army conducted an Ops Demo for TLS BCT MP in November 2023, to inform an MTA RF transition decision. The Ops Demo was adequate to support the program transition to an MTA RF pathway and the Army's decision to field an early capability to select IBCT units. In July 2025, DOT&E determined that the program had stabilized and removed TLS BCT MP from oversight.

This page intentionally left blank.

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 FY25, the Navy successfully completed one of three Advanced Anti-Radiation Guided Missile – Extended Range (AARGM-ER) integrated test (IT) weapon employment events from an F/A-18F. Subsequent weapon test events planned for FY25 have been delayed until problems identified in testing are addressed. AARGM-ER IT weapon employment events are scheduled to resume in 1QFY26. The Navy does not expect formal IOT&E events to begin until after AARGM-ER initial operational capability (IOC), which is now planned for 1QFY27.

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 weapons bay carriage, and a new rocket motor that provides increased range against surface-to-air threats. The F/A-18E/F and EA-18G are threshold 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 platforms.

MISSION

Commanders will use aircraft equipped with AARGM-ER to suppress or destroy enemy air defenses. AARGM-ER will detect, track, and suppress or destroy RF-enabled, surface-to-air missile systems that employ shutdown tactics, a common technique of modern systems, which the multi-mode seeker of AARGM-ER is intended to counter.

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 first low-rate initial production (LRIP) 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. Due to problems identified during qualification and weapon employment testing, the Navy is now planning for AARGM-ER IOC in 1QFY27, which is prior to the expected start of formal IOT&E events. DOT&E previously expected IOC to occur in 4QFY25, as stated in the FY24 Annual Report.

The AARGM-ER full-rate production (FRP) decision is planned for 1QFY30. Due to delays in development and to the incremental hardware and software changes in LRIP lots, the integrated and operational test strategy has changed significantly since the AARGM-ER Milestone C TEMP was approved. The TEMP's flight test strategy has not been updated to ensure that IOT&E is resourced to adequately evaluate both the intended AARGM-ER FRP configuration, and the planned incremental hardware and software changes between LRIP lots leading to the FRP configuration.

» MAJOR CONTRACTOR

- Northrop Grumman Corporation – Northridge, California

TEST ADEQUACY

In FY25, the program attempted three IT weapon employment tests using F/A-18F aircraft against a threat-representative integrated air defense land target at the China Lake Range in California. Testing was accomplished in accordance with the DOT&E-approved IT plan and observed by DOT&E. AARGM-ER successfully completed one of the three weapon events but exhibited performance discrepancies during the other two, to include one event during which range safety terminated the weapon after release. No further weapons employment testing was accomplished in FY25 pending implementation of updates required to address the problems that were identified.

Prior to restart of IT weapon employment testing, the program would benefit from an overall increase in the number of captive-carry events to better characterize performance and support problem identification and correction prior to a restart of weapon employment events.

The Navy has made limited progress collecting and analyzing data to support modeling and simulation (M&S) verification and validation (V&V). This lack of progress has been compounded by issues identified during testing that have resulted in test events that yield limited or no data, and by the subsequent software, changes required to address issues.

As discussed in the FY24 Annual Report, 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, adequate range capability and availability continues to be a challenge for the program, necessitating adjustments to the test plan and contributing to further schedule delays. Three of the four IT weapon employment tests attempted thus far demonstrated progress in this regard, as cooperation between the Air Force's Nevada Test and Training Range, the Navy's China Lake Range, and the FAA enabling employment of AARGM-ER shots from one range to a complex target set in the other, at near threshold employment range of the missile.

The program did not conduct cyber survivability test events in FY25. Since multiple software changes have been implemented since the April 2024 cooperative vulnerability and penetration assessment (CVPA), DOT&E may require additional CVPA testing before the adversarial assessment.

The program completed five arena tests of the newly designed AARGM-ER warhead between December 2021 and September 2023 and provided data to DOT&E 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. Once flight testing resumes, DOT&E will analyze the potential impacts from the lethality test data to evaluate more M&S scenarios, and suggest fuzing and weaponeering updates, as required.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

The current data 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 AARGM-ER TEMP flight test strategy and submit it for DOT&E's approval prior to the start of dedicated operational testing.
2. Update the IOT&E test plan with DOT&E recommendations and submit it for DOT&E's approval prior to the start of dedicated operational testing, as recommended in the FY24 Annual Report.
3. 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 a demonstration of missile guidance and warhead lethality, in an operationally realistic environment during IOT&E, as recommended in the FY23 and FY24 Annual Reports.
4. Increase the completeness and adequacy of data for M&S V&V with an overall increase in the number of captive-carry events, to better identify discrepancies before IOC, as recommended in the FY23 and FY24 Annual Reports.
5. Incorporate the EA-18G threshold platform into IOT&E weapon employment events.

Aegis Modernization Program

In FY25, the Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted an FOT&E of Aegis Advanced Capability Build (ACB) 16 on USS *Chosin* (CG 65), a *Ticonderoga*-class guided missile cruiser. In March 2025, DOT&E published a classified early fielding report (EFR) for the ACB 16, Baseline 9.2.3 Capability Package (CP) 22-1 variant of the Aegis Weapon System (AWS). 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 plans to submit a TEMP update to DOT&E for approval in FY26 as well as an updated test plan for the ACB 16, Baseline 9.2.4 CP 24 and Baseline 9.3 variants. The Navy expects to complete the FOT&E of ACB 16 variants in FY27, after which DOT&E will publish a classified FOT&E report.

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, which 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) the Phalanx Close-In Weapon System; (4) a 5-inch diameter multipurpose gun system; (5) the Vertical Launch System that can launch Tomahawk missiles, Standard Missiles (SM-2, SM-3, and SM-6), 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); (8) Cooperative Engagement Capability (CEC); and (9) the AN/SQQ-89A(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 CG 47 *Ticonderoga*-class guided missile cruisers and DDG 51 *Arleigh Burke*-class guided missile destroyers.

MISSION

The Joint Force Commander/Strike Group Commander employs CG 47-class and DDG 51-class 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 or other 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 now plans six 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), Baseline 9.2.4 (referred to as CP 24), and the new Baseline 9.3. 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 operational 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 Navy is working on an update to the TEMP and a new test plan for ACB 16 (Baseline 9 series, CP 24 and Baseline 9.3) and expects to submit both for DOT&E approval in FY26.

The newest Aegis variant, ACB 20 Baseline 10, has an updated system design architecture from the Baseline 9 series and is required for ships with a AN/SPY-6 variant radar, to include DDG 51-class Flight III destroyers with the AN/SPY-6(V)1 and FFG 62 *Constellation*-class guided missile frigates with AN/SPY-6(V)3. DOT&E approved a TEMP for the combined test programs of DDG 51 Flight III, AN/SPY-6(V)1, and Aegis ACB 20 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 testing of Baseline 10.0 in FY24 and expects to complete in FY28. The Navy expects to deliver both the IOT&E test plan and cyber survivability test plan to DOT&E for approval in FY26; both test plans will cover DDG 51 Flight III, AN/SPY-6(V)1, and Aegis ACB 20 Baseline 10.0.

In FY26, the Navy expects to deliver to DOT&E for approval an updated FFG 62 *Constellation*-class guided missile frigate TEMP that supports OT&E of Baseline 10. In addition, the Navy is developing a TEMP update to support the test program of Baseline 10 for DDG 51-class Flight IIA destroyers with AN/SPY-6(V)4.

» MAJOR CONTRACTORS

- Lockheed Martin Rotary and Mission Systems – Bethesda, Maryland
- Raytheon, a subsidiary of RTX – Arlington, Virginia

TEST ADEQUACY

In March 2025, DOT&E published a classified EFR for the ACB 16, Baseline 9.2.3 CP 22-1 variant. The EFR provided an initial assessment of operational effectiveness and suitability. DOT&E will assess cyber survivability on Aegis ACB 16, for CP 22-1 variant in FY26.

Also in March 2025, OPTEVFOR conducted an FOT&E of the ACB 16, Baseline 9.2.1 on the USS *Chosin* (CG 65), a *Ticonderoga*-class guided missile cruiser. Testing was conducted in accordance with a DOT&E-approved test plan and observed by DOT&E. Operational tracking exercises, conducted by USS *Chosin* including tracking exercises with USS *Mustin* (DDG 89) operating in a CEC network, revealed performance issues of both Aegis and CEC. The test period was reduced due to hull, mechanical, and electrical problems aboard the ship.

DOT&E approved the cyber survivability test plan for ACB 16, Baseline 9.2.3 CP 22-1 variant on USS *Frank E. Petersen Jr.* (DDG 121) in February 2025, and an updated version of it in September 2025. The Navy intends to complete cyber survivability testing of ACB 16, CP 22-1 in FY26, and complete operational testing of ACB 16, Baseline 9.2 series in FY26, with additional testing of AEGIS Baseline 9.3 in FY26 and beyond. The Navy expects to deliver an updated TEMP and a new test plan for ACB 16 CP 24 (Baseline 9.2.4) and Baseline 9.3 for DOT&E approval in FY26.

In FY25, the Navy continued to develop a Combat System Test Bed (CSTB) modeling and simulation suite to support the test strategy for Baseline 10.0. The Navy plans to deliver 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 OA of Baseline 10.0 in FY28.

PERFORMANCE

» EFFECTIVENESS

DOT&E's assessment of the operational effectiveness of Aegis ACB 16, Baseline 9.2.3 CP 22-1 is classified and can be found in DOT&E's March 2025 EFR.

Insufficient data are available to determine the operational effectiveness of Aegis ACB 16, Baseline 9 series variants. DOT&E will publish a classified FOT&E report upon completion of operational testing that the Navy expects to occur in FY27.

Insufficient data are available to determine operational effectiveness of Baseline 10.0. DOT&E will publish a classified OT&E report after completion of the operational testing that the Navy expects to occur in FY28.

» SUITABILITY

Aegis ACB 16 CP 22-1 is not currently operationally suitable due to low reliability and availability concerns. Details can be found in DOT&E's March 2025 EFR.

Insufficient data are available to determine operational suitability of Aegis ACB 16, Baseline 9 series variants. 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 FOT&E report upon completion of operational testing that the Navy expects to occur in FY27.

Insufficient data are available to determine Baseline 10.0 operational suitability. DOT&E will publish a classified OT&E report after completion of the operational testing that the Navy expects to occur in FY28.

» SURVIVABILITY

Insufficient data are available to assess the cyber survivability of Aegis ACB 16, Baseline 9 series variants. DOT&E will publish a classified cyber survivability OT&E report upon completion of the ACB 16, CP 22-1 cyber survivability test that the Navy has scheduled in FY26.

Insufficient data are available to assess cyber survivability of Baseline 10.0. DOT&E will publish a classified OT&E report after the completion of the operational testing that the Navy expects to occur in FY28.

RECOMMENDATIONS

As recommended in the FY24 Annual Report, 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 an OA of Baseline 10.0 and subsequent upgrades to AWS.
3. Schedule and conduct remaining test requirements for the Aegis ACB 16 test program, Baseline 9 series in FY26 and FY27.
4. Provide to DOT&E for approval in FY26, a TEMP update and test plan for Aegis ACB 16 Baseline 9 series for CP 24 (Baseline 9.2.4) and Baseline 9.3.
5. Develop and provide to DOT&E for approval in FY26, a TEMP update for Baseline 10 to support DDG 51-class Flight IIA destroyers with AN/SPY-6(V)4.

AIM-9X Block II Sidewinder

In February 2025, DOT&E approved the AIM-9X Block II TEMP Revision B and test plan detailing FOT&E of Operational Flight Software (OFS) 9.501. The test plan is adequate to evaluate operational effectiveness and suitability. The inadequacy over the number of live fire missile tests noted in the previous annual report was adjudicated with the Services in FY25.

In May 2025, DOT&E reviewed and provided input to the AIM-9X Block II TEMP Revision C, which details FOT&E for OFS 10.402 and OFS 10.5. DOT&E inputs were incorporated into the TEMP. DOT&E also reviewed and provided input to the OFS 10.402 test plan which have also been incorporated. DOT&E assessed the test plan adequate to evaluate operational effectiveness and suitability. In July 2025, DOT&E removed AIM-9X Block II from oversight because program development had stabilized and there are no significant upgrade activities scheduled at this time.

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 and aerial targets. 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, EA-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 9.501 is a software update of the currently fielded OFS 9.411. This update is intended to incrementally improve missile performance and provide new capabilities related to alternate target sets. OFS 10.402 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 9.501 with the new hardware. Previously, the program had planned to replace the current sapphire missile seeker dome with a new material during OFS 10.5 testing. Due to issues with the coating material for the new seeker dome at high-rate production quantities, this material change has been deferred to System Improvement Program IV (SIP-IV) missile hardware and future software (OFS 11.X) updates.

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. DOT&E placed the AIM-9X Sidewinder program on oversight in 2005 for operational and live fire testing. 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 (OPTEVFOR) is the lead Operational Test Agency (OTA) for OFS 9.501, 10.402, and 10.5 FOT&E efforts, and the Air Force Operational Test and Evaluation Center (AFOTEC) is the supporting OTA.

In February 2025, DOT&E approved the AIM-9X Block II TEMP Revision B and FOT&E test plan for OFS 9.501. The test strategy and resources provided in these documents are adequate to evaluate operational effectiveness and suitability for OFS 9.501.

In May 2025, DOT&E reviewed and provided inputs to the AIM-9X Block II TEMP Revision C for OFS 10.402 and OFS 10.5. In addition, the OTAs approved the OFS 10.402 test plan in June 2025, which DOT&E reviewed but did not sign, due to removal of the program from oversight in July 2025. DOT&E removed AIM-9X from oversight because program development had stabilized and there are no significant upgrade activities scheduled at this time.

The program has begun early development efforts for the AIM-9X Block II SIP-IV. This next iteration of the Block II Sidewinder program will address technology obsolescence via replacement of the seeker sensor from an analog to a digital focal plane array (DFPA), sensor refresh to accommodate the DFPA, electronics unit re-architecture to optimize recent processor upgrade, and a new cyro-engine. This hardware upgrade includes missile OFS update (OFS 11.X), which will take advantage of the DFPA sensor refresh and recent processor update to increase missile performance and add additional target sets.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX – Tucson, Arizona

TEST ADEQUACY

OPTEVFOR and AFOTEC began operational and live fire testing of the AIM-9X Block II missile with OFS 9.501 following the October 2024 Operational Test Readiness Review, in accordance with the DOT&E-approved OFS 9.501 test plan. DOT&E observed the testing. The Services are analyzing the data and expect to release their final OFS 9.501 FOT&E report in 2QFY26.

Operational and live fire testing of the AIM-9X Block II missile with OFS 10.402 started following OTA approval of the OFS 10.402 FOT&E test plan. To date, one live missile firing and four captive carry performance flights have been completed. OFS 10.402 FOT&E analysis is ongoing with anticipated completion in 2QFY26. Operational and live fire testing of the AIM-9X Block II missile with OFS 10.5 is expected to begin 4QFY26. Operational and live fire testing of the AIM-9X Block II missile with SIP-IV missile hardware upgrades and OFS 11.X is expected to begin 2QFY29.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

OPTEVFOR and AFOTEC are currently conducting data analysis of AIM-9X Block II OFS 9.501.

» LETHALITY AND SURVIVABILITY

The Navy has implemented one recommendation from DOT&E's July 2024 classified AIM-9X Block II OFS 9.411 Lethality and Cyber Survivability Annex, to improve lethality. The Navy is currently addressing the four recommendations from the classified annex to improve cyber survivability in the SIP-IV program.

RECOMMENDATION

The Services, in partnership with the OUSW(R&E)/Test Resource Management Center, should:

1. Fund, develop, and produce modern aerial targets, such as fifth generation fighter aircraft, large bomber and mobility aircraft, helicopters, and others, to ensure adequate testing against representative threat air vehicles. 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 level, as recommended in the FY24 Annual Report.

CH-53K® King Stallion®

In FY25, the CH-53K program conducted multiple integrated testing (IT) events to assess aircraft survivability systems, in accordance with the DOT&E-approved TEMP and test plans. The CH-53K Operational Testing (OT)-D2 phase is scheduled for 1QFY26. DOT&E will publish an FOT&E report, with findings from IT and OT, following OT-D2 completion in 3QFY26. In January 2025, the Navy completed the DoD Inspector General-directed analysis of the requirements to conduct LFT&E Phase II and determined that continuing Phase II LFT&E is not required.

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 external payload 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 (LAIRCM) system with advanced threat warning sensors, radar warning receiver, and countermeasure dispensing system. The LAIRCM is designed as a self-defense measure against infrared guided missile threats.

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.

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 April 2022, in accordance with a DOT&E-approved test plan. DOT&E published a combined IOT&E and LFT&E report in December 2022, to inform the full-rate production decision, which the Navy approved later that month.

In May 2024, DOT&E approved a tailored update to CH-53K TEMP Revision C to support execution of IT and the OT-D2 events to determine operational effectiveness, suitability, and cyber survivability of the CH-53K configured with Data Transfer Unit and Defensive Electronic Countermeasures System Replacement and Digital Interoperability Medium communications systems. The FOT&E phase, OT-D2, is scheduled to begin in 1QFY26 to complete the outstanding requirements from TEMP Revision C. Assessment of test data from IT, cyber vulnerability and penetration assessments, and OT-D2 will inform the CH-53K fleet prior to the first Marine Expeditionary Unit deployment, projected in 4QFY26.

U.S. Marines prepare to externally load an M777 Howitzer to a CH-53K King Stallion while conducting helicopter support team operations during a Weapons and Tactics Instructor course in Yuma, Arizona, October 2024

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. In September 2023, the DoD Office of Inspector General opened an audit into the Phase II effort and released a report with its CH-53K findings in November 2024. The report required the Navy to conduct a business case analysis on the impact of conducting the LFT&E Phase II test. The Navy completed its analysis in January 2025 and determined the testing already conducted during LFT&E Phase I was sufficient for initial fielding, and further testing is not required.

» MAJOR CONTRACTOR

- Sikorsky Aircraft Corporation, a subsidiary of Lockheed Martin Corporation – Stratford, Connecticut

TEST ADEQUACY

In April and May 2025, the CH-53K program conducted IT of the aircraft survivability equipment suite and LAIRCM integration, in accordance with DOT&E-approved operational test plans. DOT&E observed the testing. The OT-D2, previously planned for 4QFY25, is now scheduled to begin in 1QFY26, due to delays in test article aircraft modifications. DOT&E will assess the adequacy of the FOT&E following completion of the OT-D2.

A CH-53K King Stallion helicopter transports an M777 towed 155 mm howitzer during Exercise Northern Strike 2024 at Camp Grayling, Michigan, August 2024

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Data analyses for the FOT&E events completed thus far are ongoing and the final event, OT-D2, is scheduled to begin in 1QFY26 and conclude in 3QFY26, precluding an assessment of operational effectiveness, survivability, and suitability. DOT&E will publish the assessments in a classified FOT&E report, expected in 4QFY26.

RECOMMENDATIONS

The Navy should:

1. Continue to address cyber recommendations, as discussed in the FY24 Annual Report.
2. Continue coordination among the CH-53K Program Office, the Aircraft Survivability Equipment Program Office, and the intelligence community to remain current on the emerging threat environment, and inform DOT&E if additional survivability testing is required as new threats emerge.
3. Develop and route for DOT&E approval a TEMP Revision D for any additional testing requirements identified or emerging from the FY26 OT-D2.

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

The Navy has completed all planned testing in accordance with the March 2020 DOT&E-approved CMV-22B TEMP and Alternative LFT&E Plan. DOT&E has no changes to its assessment in the FY24 Annual Report or the classified July 2024 combined FOT&E and LFT&E report. The Navy is continuing to address recommendations from the report and plans for the CMV-22B program to reach full operational capability in FY26. DOT&E will retain the V-22 program, which includes the CMV-22B variant, on oversight in anticipation of projected aircraft subsystem modifications to the fuel cell, communications equipment, and gear boxes.

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 radio for over-the-horizon communications, and lighting to assist with cargo loading in the cabin and cargo areas.

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 CMV-22B program has completed all OT&E and LFT&E requirements, culminating with DOT&E's classified combined FOT&E and LFT&E report published in July 2024. The Navy declared initial operational capability in FY22 and plans to declare full operational capability in FY26. DOT&E will continue to monitor the program on oversight for operational and live fire testing and report on projected future aircraft modifications.

» MAJOR CONTRACTOR

- Bell-Boeing Joint Project Office – Amarillo, Texas

TEST ADEQUACY

DOT&E did not assess test adequacy in FY25 due to the Navy completing all TEMP-required testing during its second FOT&E in FY24.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E has no changes to its assessment in the FY24 Annual Report or classified July 2024 combined FOT&E and LFT&E report. The Navy conducted no additional testing or reporting in FY25. DOT&E will continue to monitor the program as projected modifications are made to the fuel cell, communications equipment, and gear boxes.

RECOMMENDATIONS

The Navy should:

1. Continue to implement the recommendations in the classified July 2024 combined FOT&E and LFT&E report.
2. Continue coordination for projected aircraft subsystem modifications and subsequent testing, to maintain readiness.

A CMV-22B Osprey refuels on the flight deck of USS George Washington *(CVN 73) while underway in the Pacific Ocean, September 2024*

Columbia-Class Submarine

In FY25, the Navy began conducting an operational assessment (OA) of the *Columbia*-class design with completion scheduled for 3QFY26. The *Columbia*-class submarine program also began system-level cybersecurity evaluations of the communications, combat control, and command and control systems; completion is scheduled for 1QFY27. DOT&E will report on the operational effectiveness and suitability upon completion of IOT&E, which the Navy expects in FY29.

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 by foregoing the *Ohio*-class mid-life refueling requirement, 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 is an Acquisition Category ID Major Defense Acquisition Program. USS *District of Columbia* (SSBN 826), the first ship of the class, is scheduled to be delivered in FY28 and to conduct its first Strategic Patrol in FY30. The Navy will procure a minimum of 12 *Columbia*-class submarines to support USSTRATCOM requirements.

DOT&E approved an update to the *Columbia*-class TEMP and LFT&E Management Plan in June 2023. In January 2025, DOT&E approved the Navy's latest test plan for an OA of the *Columbia*-class design. The Navy expects to complete this in-progress assessment in 3QFY26, to identify risks prior to commencing IOT&E. Although IOT&E is currently expected to begin in FY29, the Navy has initiated a review of its *Columbia*-class construction, test, and certification schedule to identify opportunities to mitigate an anticipated 12- to 18-month delivery delay of SSBN 826. This delivery delay may impact IOT&E, as the Navy evaluates options to mitigate schedule delays through adjustments to the post-delivery timeline in effort to maintain the USS *District of Columbia*'s first patrol date in FY30.

» MAJOR CONTRACTORS

- General Dynamics Electric Boat (GDEB) – Groton, Connecticut
- Newport News Shipbuilding, a division of HII – Newport News, Virginia

TEST ADEQUACY

In January 2025, the Navy commenced an OA of the *Columbia*-class submarine to identify risks that could affect operational effectiveness and suitability testing during IOT&E. The ongoing OA includes modeling and simulation of strategic patrols, shore-based system-level testing, and reviews of training and maintenance facilities. In 1QFY26, DOT&E expects to approve a change to the operational test plan canceling one shore-based event due to asset unavailability. The Navy plans to complete the OA in 3QFY26.

The Navy's joint *Columbia*- and *Virginia*-class Cyber Security T&E Strategy combines the efforts of both classes' cyber testing under a single test plan, due to the multitude of shared systems between the two submarine classes. Class-unique systems are tested as required to address differences. In April 2025, the Navy began a cooperative vulnerability and penetration assessment and a cooperative vulnerability identification of several systems comprised of the command, control, communications, computers, and intelligence network; exterior communications systems; the Submarine Warfare Federated Tactical System; and hull, mechanical, and electrical systems aboard a *Virginia*-class submarine. Schedule and system availability limited the first round of testing, but evaluators completed initial assessments of the BYG-1 combat control system and the Consolidated Afloat Networks and Enterprise Services. The Navy is scheduling follow-on testing to complete test objectives.

In FY25, the *Columbia*-class program office continued LFT&E survivability testing under DOT&E oversight to determine equipment failure thresholds and personnel injury model techniques for incorporation into the analysis of simulated threat weapon attacks. Once completed, the survivability assessment of the submarine, using validated modeling and simulation, will enable assessment of the class's vulnerability to threat weapons. The *Columbia*-class Total Ship Survivability Trial is scheduled for FY29, and Survivability Assessment Report (SAR) II will be provided to DOT&E in FY26, with SAR III expected in FY29.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Insufficient data are available at this time to determine the operational effectiveness, suitability, and survivability of the *Columbia*-class. DOT&E will internally assess the current platform design and its systems after completion of the OA, scheduled for 3QFY26. DOT&E will report on the operational effectiveness and suitability upon completion of IOT&E, which the Navy expects to occur in FY29, and on survivability upon completion of Total Ship Survivability Trial and SAR III, which the Navy expects to provide in FY29.

RECOMMENDATION

The Navy should:

1. Ensure testing adequacy of IOT&E is not compromised based on schedule pressures by continuing to work with the Operational Test and Evaluation Force and DOT&E to prioritize opportunities to collect operational-test-quality data prior to IOT&E.

Conventional Prompt Strike (CPS)

In December 2024, the Navy and Army completed the first end-to-end flight test of the prototype Conventional Prompt Strike (CPS) All-Up-Round (AUR) launched from an Army battery. In April 2025, the Navy conducted a flight test of the prototype CPS AUR launched from an operationally relevant Navy launcher. This flight test serves as the operational demonstration (Ops Demo) required to close out the Middle Tier of Acquisition (MTA) rapid prototyping phase of the overall CPS acquisition strategy. In August 2025, the Navy conducted a warhead arena test; results from this test remain under analysis.

SYSTEM DESCRIPTION

CPS is a conventional, boost-glide intermediate range 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 Long Range Hypersonic Weapon (LRHW) system, which is being reported on in a separate article, will fire a common AUR from their Transporter Erector Launcher (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 CPS program is a partnered effort between the Navy and the Army to design and deliver a common AUR. The Navy is employing a three-phase acquisition strategy to deliver CPS:

- Phase 1 is an MTA rapid prototyping effort to develop and demonstrate a prototype hypersonic missile system capability through a four-flight test campaign. The Navy will complete Phase 1 in 1QFY26, following final evaluation and reporting of the April 2025 Ops Demo.
- Phase 2, which commenced in August 2024, 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 planned as a Major Defense Acquisition Program through which the Navy intends to field CPS on the remaining two *Zumwalt*-class destroyers and aboard *Virginia*-class submarines.

The CPS Program Office plans to conduct Phases 2 and 3 under a single TEMP which will include the LFT&E Strategy, expected to be provided to DOT&E for approval in early FY26. The Navy plans to submit test plans to DOT&E for approval in FY26 to conduct additional integrated testing of the CPS AUR from the operationally relevant Navy launcher. In FY27, the CPS Program Office intends to conduct an Ops Demo to assess fielding readiness, by installing, integrating, certifying, and testing the AUR on the first *Zumwalt*-class destroyer.

» MAJOR CONTRACTORS

- Lockheed Martin Space – Littleton, Colorado
- Dynetics, a subsidiary of Leidos – Huntsville, Alabama (Common Hypersonic Glide Body)

TEST ADEQUACY

In December 2024, the Navy and Army completed the first successful end-to-end flight test of a prototype CPS AUR launched from an Army LRHW Battery Operations Center and TEL. As it was not an operational test, it did not require a DOT&E-approved test plan, but the flight test data will help inform future operational test plans.

In April 2025, the Navy completed a flight test of the CPS missile system, in accordance with a DOT&E-approved Ops Demo test plan, in an operationally relevant environment, demonstrating the CPS missile system's readiness to exit Phase 1 of the acquisition strategy. DOT&E observed the test. The Ops Demo was adequate to inform preliminary assessments of the development, capabilities, limitations, and risks of the CPS weapon system. Data collected from the April flight test supported the decision to proceed to MTA rapid fielding; it was not intended to support a full evaluation of CPS for operational effectiveness, suitability, and survivability.

In FY25, DOT&E observed multiple Navy surrogate and component tests to support LFT&E. The Navy conducted sub-scale warhead testing in January 2025 at Aberdeen Proving Ground, Maryland, to characterize the effect of drag on the warhead fragments. In June 2025 the Navy assessed the feasibility of firing the CPS warhead out of a large caliber gun at Yuma Proving Ground, Arizona. This novel test method would reduce the cost of conducting dynamic lethality testing against representative targets compared to sled and flight tests. Pending the analysis of the results, the Navy will use this method to conduct lethality tests against a field of targets in FY26. Work is ongoing to identify target assets for use in this testing. In August 2025, DOT&E witnessed the fourth warhead arena test of the CPS warhead at Naval Surface Warfare Center Dahlgren Division, conducted in accordance with a DOT&E-approved test plan. In FY26 and FY27, two additional arena tests are scheduled to characterize a different variant of the warhead.

The CPS program continued work on the verification and validation of their lethality modeling and simulation (M&S) tools throughout FY25. The Navy expects to provide an LFT&E Strategy, as part of the TEMP, for DOT&E approval in FY26.

The Navy has only evaluated the effect of a contested environment on CPS AUR missile performance to a limited extent. The Navy plans to use a combination of M&S, component testing, hardware-in-the-loop, and evaluations of flight testing to assess CPS performance in the contested environment but has not detailed this in the test strategy.

There was no cyber survivability testing conducted in FY25. Cyber testing originally planned for FY25 was rescheduled to FY26 due equipment availability. Between FY23 and FY24, the Navy completed 10 cyber survivability events to identify the attack surface and potential vulnerabilities of the CPS AUR missile and its supporting combat system. These events will support cyber survivability operational testing in Phases 2 and 3.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Insufficient data are available at this time to fully determine the operational effectiveness, suitability, and survivability of CPS in an operationally relevant environment. DOT&E intends to use the Navy's classified Phase I Ops Demo report, issued in September 2025, to support a risk assessment with feedback to the program office. DOT&E will further assess CPS for operational effectiveness, suitability, and survivability at the completion of Phase 2 and within a classified IOT&E report upon completion of Phase 3 testing, planned after FY30.

» LETHALITY

Insufficient data are available at this time to provide a preliminary assessment of CPS lethality. As noted in the FY22 – 24 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. Additionally, DOT&E has not yet received the test data from the August 2025 arena test.

RECOMMENDATIONS

The Navy should:

1. Submit to DOT&E for approval the updated CPS TEMP that fully captures the test strategy for Phases 2 and 3 of CPS development and delivery and that will sufficiently determine CPS AUR missile operational effectiveness, suitability, and survivability in a full-spectrum contested environment.
2. Submit to DOT&E for approval the LFT&E Strategy to evaluate the lethality and survivability of the CPS AUR in an operationally representative environment 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.
3. Submit to DOT&E for review a Cyber T&E Strategy that supports operational testing of cyber survivability of CPS on a *Zumwalt*-class destroyer in Phase 2 and a *Virginia*-class submarine in Phases 2 and 3.

Cooperative Engagement Capability (CEC)

In March 2025, the Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted FOT&E of the Cooperative Engagement Capability (CEC) on USS *Chosin* (CG 65), a *Ticonderoga*-class guided missile cruiser. OPTEVFOR plans to capture operational data from USS *Zumwalt* (DDG 1000), a *Zumwalt*-class destroyer in FY27.

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 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 (CTN) units

AN/USG-2B is integrated with three different Navy surface combat systems: Aegis Advanced Capability Build (ACB) 16-equipped *Ticonderoga*-class cruisers and *Arleigh Burke*-class destroyers, Total Ship Computing Environment equipped *Zumwalt*-class destroyers, and Ship Self-Defense System (SSDS)-equipped *Gerald R. Ford*-class aircraft carriers. Each of these three combat systems utilize CEC with different combinations of ship sensors.

CEC Increment I is considered legacy CEC on the *Ticonderoga*-class cruisers, *Arleigh Burke*-class destroyers, *Zumwalt*-class destroyers, and *Gerald R. Ford*-class aircraft carriers.

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. CEC Block II will be integrated with the different Navy surface combat systems on the cruisers (CG), destroyers (DDG), amphibious and frigate ships (LPD/LHD/LHA and FFG), and aircraft carriers (CVN), as well as with Marine Corps CTN units (USMC CTN).

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 SSDS 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 Increment I 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 the 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 combined Aegis ACB 16 and CEC FOT&E test plan in July 2023 supported operational test of the AN/USG-2B *Ticonderoga*-class variant in FY25. 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. DOT&E approved the combined CVN 78, SSDS, and CEC OT&E Plan in February 2025 to support operational effectiveness and suitability testing of the AN/USG-2B *Gerald R. Ford*-class variant.

CEC Increment II is a separate Acquisition Category II program. In February 2024, OPTEVFOR approved the Integrated Evaluation Framework for the operational test design of CEC Block II. In May 2024, DOT&E delivered a non-endorsement memo to OPTEVFOR to address concerns with operational effectiveness and cyber survivability testing. In August 2025, OPTEVFOR approved a revision to the Integrated Evaluation Framework to address DOT&E's test strategy and cyber concerns for CEC Block II. The Navy continues to develop the TEMP for CEC Block II. The Navy expects to deliver the TEMP to DOT&E for approval in FY26 to support OT&E of CEC Block II currently planned for FY27.

In addition, in October 2025, DOT&E approved the TEMP to support OT&E of CEC Block II for *Gerald R. Ford*-class and *Nimitz*-class aircraft carriers and *San Antonio*-class and *America*-class amphibious ships planned for FY28. The Navy expects to deliver the TEMP to DOT&E for approval in FY26 to support OT&E of CEC Block II for the FFG 62 *Constellation*-class guided-missile frigate ships planned for FY29.

» MAJOR CONTRACTORS

- Collins Aerospace, a subsidiary of RTX – St. Petersburg, Florida
- L3Harris Technologies, Inc. – Camden, New Jersey

TEST ADEQUACY

OPTEVFOR conducted FOT&E of the AN/USG-2B *Ticonderoga*-class variant from USS *Chosin* (CG 65), when it was underway in FY25. Testing was conducted in accordance with a DOT&E-approved test plan and observed by DOT&E. Operational tracking exercises conducted by USS *Chosin* included tracking exercises with USS *Mustin* (DDG 89) operating in a CEC network. The test period was reduced due to hull, mechanical, and electrical problems aboard the USS *Chosin*.

OPTEVFOR intends to collect CEC data aboard USS *Zumwalt* (DDG 1000) in FY27, as a result of the previous test event conducted of the AN/USG-2B *Zumwalt*-class variant discussed in the FY23 and FY24 Annual Reports. The Navy expects to deliver a data collection plan to DOT&E to support this test in FY26. The Navy intends to conclude evaluation of the *Arleigh Burke*-class and *Zumwalt*-class CEC Increment I in FY28.

OPTEVFOR had intended to complete operational effectiveness and suitability including cyber survivability testing of the AN/USG-2B *Gerald R. Ford*-class variant aboard USS *Gerald R. Ford* (CVN 78) in FY25. However, unplanned maintenance requirements prevented execution of this test.

OPTEVFOR also intended to conduct testing of operational scenarios for CEC employment of the AN/USG-2B *Gerald R. Ford*-class variant aboard USS *Gerald R. Ford* (CVN 78) in FY25, in conjunction with the platform's remaining IOT&E. CVN 78 was unable to support this testing due to competing fleet priorities. The Navy is currently examining options to conduct the remaining testing required to conclude FOT&E for the legacy CEC program variant.

In February 2025, DOT&E approved OPTEVFOR's cyber survivability test plan for Aegis ACB 16 Baseline 9.C2.3, which included cyber survivability boundary scans of AN/USG-2/2B. Subsequently, in August 2025, OPTEVFOR delivered an update to their cyber survivability test plan to clarify data collection of AN/USG-2/2B. DOT&E approved the updated cyber survivability test plan in September 2025. The Navy intends to complete cyber survivability testing of AN/USG-2/2B in FY26.

The Navy intends to conduct a data assessment in FY26 to determine the remaining test requirements to complete FOT&E for the legacy CEC program variants, which is currently expected to occur in FY28. DOT&E will collaborate with the Navy on the remaining FOT&E events for the legacy CEC program variants and provide applicable test and data collection plans, as required.

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 ACB 16 variants. DOT&E will publish FOT&E reports, or a combined report, for these variants after completion of their respective FOT&Es, which the Navy now expects to occur in FY28.

» SURVIVABILITY

The cyber survivability assessment of the AN/USG-2B *Zumwalt*-class variant is classified. Insufficient data are available to determine the cyber survivability of the AN/USG-2B *Gerald R. Ford*-class and Aegis ACB 16 variants. DOT&E will publish FOT&E reports, or a combined report, for these variants after completion of their respective FOT&Es, which the Navy now expects to occur in FY28.

RECOMMENDATIONS

The Navy should:

1. Conduct, in collaboration with DOT&E, the data assessment and determine the remaining test requirements to complete FOT&E in FY26 for legacy CEC program variants.
2. Provide the remaining applicable test and data collection plans for the remaining FOT&E events of the legacy CEC program variants.
3. Complete the remaining planned FOT&E events for the

legacy CEC program variants in FY26, FY27, and FY28 as recommended in FY23 and FY24 Annual Report.

4. Provide a CEC Increment II Block II TEMP for DOT&E's approval in FY26, as recommended in the FY23 and FY24 Annual Reports.
5. Ensure that cyber survivability evaluations on Aegis ACB 16 platforms comprehensively assess CEC, as recommended in the FY24 Annual Report.

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

In FY25, USS *Gerald R. Ford* (CVN 78) completed a pre-deployment workup cycle, the Total Ship Survivability Trial (TSST), and data collection in support of sortie generation rate (SGR) modeling and simulation (M&S). The January 2025 TSST demonstrated recoverability and damage control features of the *Ford*-class against simulated weapon damage and yielded numerous recommendations that would improve the survivability of the class. However, major IOT&E events remain, including the SGR live demonstration, M&S to assess the *Ford*-class SGR key performance parameter (KPP), Ship Self-Defense System (SSDS) testing, and underway cyber survivability testing. These events will be critical to evaluating the class's operational effectiveness, suitability, and survivability.

SYSTEM DESCRIPTION

The *Ford*-class is a 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, but it is scheduled to be replaced with the SPY-6(V)3 Enterprise Air Surveillance Radar (EASR) fixed variant, the SPQ-9B horizon search radar, and the Mk 9 Tracker Illuminator System. These new capabilities are installed on PCU *John F. Kennedy* (CVN 79) and will be installed on follow-on *Ford*-class ships.
- 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 on CVN 79 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 follow-on *Ford*-class ships 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 and track radar, which operates in stand-alone mode on CVN 78, but will be integrated with AN/USG-2B CEC and SSDS on CVN 79 and 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.
- 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.
  - 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, and in July 2024 the Navy delivered to DOT&E a revised test plan, labeled IOT&E Test Plan Update 1, which replaced the IOT&E's original two-phase structure with a more incremental approach. DOT&E initially withheld full test plan approval due to an insufficiently articulated reliability, maintainability, logistics supportability, and availability (RMLA) data collection strategy, but in February 2025, the Navy submitted to DOT&E an updated test plan revision that contained an improved RMLA data collection strategy. DOT&E then approved the revised IOT&E test plan. In May 2025, DOT&E approved an IOT&E test card detailing the process by which the Navy would execute the sustained SGR live demonstration, which was scheduled for June 2025.

CVN 79 delivery is now scheduled for FY27, two years later than reported in the FY24 Annual Report. A combination of supply chain impediments, difficulties with AAG installation and certification, and Advanced Weapons Elevator (AWE) installation progressing slower than forecasted all contributed to this delay. *Enterprise* (CVN 80) construction began in August 2017 and is now expected for delivery to the Navy in FY30, one year later than reported in the FY24 Annual Report. *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 Platform TEMP 1610 to include operational testing of the *Ford*-class's capability to support F-35 and CMV-22. Enterprise TEMP 1910 will document operational testing of the self-defense capabilities of CVN 79 and follow-on *Ford*-class carriers. The Navy now expects to submit the updated TEMP 1610 for DOT&E approval in FY26.

» 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 IOT&E Test Plan Update 1.

In March 2024, the Navy conducted *Ford*-class pierside shipboard cyber survivability tests, which included some testing of the ship's industrial control systems. The Navy conducted cyber survivability testing of the SSDS integrated combat systems at a land-based test site which was not accredited for the specific use of cyber survivability testing. The Navy conducted the test in accordance with a DOT&E-approved test plan and with observation by DOT&E. However, the Navy and DOT&E do not concur on the path forward for *Ford*-class underway cyber testing. The Navy believes they have collected sufficient data to evaluate cyber survivability for the class, but DOT&E assesses that the Navy has insufficient data to support their current cyber survivability assessment.

The Navy conducted the TSST aboard USS *Gerald R. Ford* in January 2025. This test was conducted in accordance with the DOT&E-approved test plan and was observed by DOT&E personnel. TSST simulated four weapon damage events against the ship and was adequate to evaluate many recoverability features and damage control systems. However, concerns of possible damage to vital equipment limited the ability to simulate power interruption and restoration to mission systems and the associated recovery timeline of these systems. Similarly, a previously undiscovered interdependency between auxiliary systems identified during pre-trial system checks limited the ability to simulate damage and recovery of selected distributed systems.

Evaluation of the *Ford*-class's anti-air warfare capability was coordinated between the CVN 78 TEMP Revision E and the Capstone Enterprise Air Warfare Ship Self-Defense (AW SSD) TEMP 1714 of March 2008. In 2QFY25, unplanned maintenance requirements prevented the execution of a series of live missile fire events aboard CVN 78 against a variety of anti-ship cruise missile (ASCM) threat surrogates, which were designed to demonstrate the ship self-defense capability of CVN 78's current combat system configuration (SSDS Baseline 10 and DBR) and are required to validate M&S used to predict CVN 78 performance across the spectrum of threat ASCMs. The Navy has not yet rescheduled these tests.

The *Ford*-class SGR evaluation comprises M&S (for both *Ford*- and *Nimitz*-class), a four-day live demonstration that includes flight operations executed at sustained SGRs, a one-day live demonstration of flight operations executed at the surge SGR, 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 still ongoing. Due to the complexity of SSAM, the Navy coordinated the use of high-power computing (HPC) facilities to expedite the model's validation and verification (V&V). However, difficulties porting SSAM to the HPC network, the nature of data processing within the model, and the need to collect data during the sustained SGR live demonstration persist, contributing to delays with SSAM V&V as well as assessing the SGR KPP. The Navy has not determined when SSAM V&V will be complete. Once finished with SSAM V&V, the Navy estimates that completing SGR runs for the record may take between 6 – 12 months. This timeline depends on the variance of the model and the Navy's ability to overcome challenges such as running the model in the HPC environment, extracting and converting outputs to a database format, and generating reports.

The Navy had planned to execute the sustained SGR live demonstration in 3QFY25, but unplanned aviation launch and recovery equipment maintenance coupled with a constrained operational schedule prevented the execution of the event. The Navy intends to execute the SGR live demonstration in FY26, and this event remains critical for SSAM V&V and evaluating the class's SGR KPP. Additionally, the Navy plans to apply lessons from the sustained SGR live demonstration to the surge SGR test, which is also currently unscheduled.

The Navy can mitigate the risk to SSAM V&V and evaluating the SGR KPP by scheduling and 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 yet-to-be-approved CVN 78 TEMP Revision F and the SSDS Enterprise TEMP. CVN 79 includes an updated combat system, SSDS Baseline 12, and the new SPY-6(V)3 radar system. 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*, now expected in FY29. 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*, as soon as possible.

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 continues to develop fixes to combat system deficiencies identified in DOT&E's classified interim assessment report dated April 2022, but as discussed in the FY24 Annual Report, the fixes still remain largely unfunded.

SGR

During the FY25 operational deployment, USS *Gerald R. Ford*'s crew reported that the ship and its embarked air wing maintained an SGR sufficient to meet combatant commander operational taskings. Although the SGRs sustained during 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 some operational limitations and restrictions are expected to persist. 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, have shown low or unproven reliability, or are highlighted as the most significant challenges to flight operations.

AAG

The Navy has not scored any AAG RMLA data for operational test since the beginning of IOT&E in 2022; therefore DOT&E has not received sufficient data to update the reliability metrics reported in the FY23 Annual Report with operational test data. Naval Air Systems Command (NAVAIR) continues to work on short- and long-term improvements to address AAG reliability degraders. However, difficulties such as obtaining replacement parts and the reliance on off-ship technical support remain a challenge. The Navy has allocated FY26 funding to support a fourth engine alternative, with installation of the new system targeted for FY29. The fourth engine alternative 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

Data collected during CVN 78's FY25 pre-deployment workup cycle indicate that EMALS reliability remains consistent with developmental and operational test data collected in FY23 and FY24. Engineering upgrades to hardware and software have produced gradual improvements in cumulative reliability and availability. Reliance on off-ship technical support remains a challenge. NAVAIR is continuing development on improvements.

AWEs

The *Ford*-class has yet to build and transfer ordnance to the flight deck at rates reflective of the Design Reference Mission. DOT&E expects the sustained SGR live demonstration to be the first operationally representative demonstration of high ordnance throughput. Of note, the crew is still reliant on off-ship technical support for correction of AWE hardware and software failures.

DBR

Details on DBR suitability can be found in DOT&E's classified EFR from April 2023. Due to the one-of-a-kind nature of the DBR, its availability will depend on the Navy's access to replacement parts and embarked contract maintenance support 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 the Final Survivability Assessment Report (FSAR). 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.

Through the TSST, the Navy was able to evaluate how well the ship's systems supported the crew in detecting, responding to, containing, and restoring operations after combat damage. The trial showed that the ship's design supports a robust damage control capability that is somewhat hindered by shortcomings in supporting systems. The TSST also highlighted previously undetected interdependencies in vital distributed systems that impacted the ship's mission capability. Additional details regarding the performance of CVN 78 during TSST will be included in a classified DOT&E report in FY26. The CVN 78 LFT&E program is nearing completion and now expects to issue a FSAR for the class in early FY26. The FSAR is a summation report that will include findings for the class gathered from all previous LFT&E activities, including recent findings from the TSST and updates to vulnerability M&S. The program office is in the process of updating the vulnerability M&S, as recommended in the FY24 Annual Report, and expects to provide updated results for the predicted vulnerability of the class to threat weapons in the FSAR package.

The survivability 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 cyber survivability assessment will be published following the underway test. The survivability of the *Ford*-class in contested and congested electromagnetic spectrum environments has not been evaluated. Discussions on how to evaluate CVN 78 survivability in these environments are ongoing with the Navy.

RECOMMENDATIONS

The following recommendations remain as stated in the FY23 and FY24 Annual Reports. 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. 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 P_{RA} modeling.
3. 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.
4. Prioritize and correct deficiencies identified in DOT&E's classified FSST report of December 2022.
5. 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.
6. 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.
7. Continue to fully fund the scheduled replacement of DBR on CVN 78 with the EASR configuration.
8. 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.
9. Identify, fund, and deliver a replacement capability for the Navy's self-defense test ship, ex-USS *Paul F. Foster*, to support planned testing of CVN 79 capability.
10. Characterize and validate performance of the SSAM model for SGR.

The following recommendation from the FY24 Annual Report has been updated. The Navy should:

1. Submit an update of the *Ford*-class TEMP for DOT&E approval in FY26 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.

The Navy should address the following recommendations, which are new:

1. Review findings from the CVN 78 TSST and implement recommendations as soon as possible to improve the recoverability and damage control capabilities of the class.
2. Complete evaluation of system interdependencies identified during TSST and identify potential design improvements.

DDG 1000 *Zumwalt*-Class Destroyer

In FY25, the Navy's Operational Test and Evaluation Force (OPTEVFOR) continued operational testing of the DDG 1000 *Zumwalt*-class destroyer with a surface strike missile exercise and concluded the modeling and simulation (M&S) testbed runs to evaluate the anti-air warfare capability against threat anti-ship cruise missiles (ASCMs) and aircraft. The *Zumwalt*-class Program Office has not funded or scheduled Full Ship Shock Trials (FSST) and does not plan to update ship survivability M&S to reflect the as-built configuration or the installation of Conventional Prompt Strike (CPS). *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 destroyers' 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 has begun the installation of CPS modules on USS *Zumwalt* (DDG 1000) and anticipates the completion of CPS module installation for the remainder of the *Zumwalt*-class in 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.

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. Due to the Navy's decision to operationally employ USS *Zumwalt* prior to completion of IOT&E, DOT&E published a classified early fielding report in October 2022.

DOT&E previously reported in the FY24 Annual Report that expected completion of IOT&E was to occur in FY25, following the completion of testing of the *Zumwalt*-class primary mission of open-ocean surface strike. In 2QFY25, the program completed a Tomahawk live fire shot; however, there were other operational test events which were not completed prior to the deployment of USS *Michael Monsoor* in March 2025, which delayed the completion of IOT&E. DOT&E now expects IOT&E to continue into FY27 onboard USS *Zumwalt*, following completion of a Build Yard Modernization Period (BYMP). Due to the Navy's decision to operationally deploy USS *Michael Monsoor* prior to completion of IOT&E, DOT&E will publish a classified interim operational testing assessment in FY26.

Evaluation of SM-6 integration of *Zumwalt*-class is planned for FOT&E. DOT&E also recommends an FSST after completion of the Navy's shock qualification program, which will conclude following installation of CPS.

Testing of the *Zumwalt*-class with CPS will be conducted by Strategic System Programs. See the Annual Report entry on CPS for further details.

» 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 2QFY25, the Navy conducted testing to evaluate the *Zumwalt*-class's primary mission of offensive surface strike with a Tomahawk missile launch, including shipborne strike planning events. The Navy conducted this testing in accordance with the DOT&E-approved test plan, and it was observed by DOT&E. USS *Michael Monsoor* was able to successfully launch a Tomahawk missile but was not able to complete secondary test objectives due to communication issues. The Navy continues to analyze data to determine the *Zumwalt*-class's offensive surface strike capability.

In May 2025, OPTEVFOR completed Probability of Raid Annihilation M&S testbed runs. 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 program office completed a review of the M&S testbed federation in December 2024 and recommended accreditation to OPTEVFOR. DOT&E continues to work with OPTEVFOR to ensure the appropriate use of the M&S testbed.

Evaluation of *Zumwalt*-class employment of CPS will occur as described in the CPS Annual Report entry, following completion of BYMP.

The Navy has yet to fund or schedule an FSST for the *Zumwalt*-class. As previously identified in the FY22 – 24 Annual

Reports, this test is required to adequately assess ship survivability against underwater threat weapons and determine residual mission capability following such an occurrence.

In FY25, the Navy completed the final vulnerability assessment report, which included survivability findings gathered from the program's LFT&E activities to date. However, the Navy did not update the survivability M&S supporting this report to reflect the class as-built and did not conduct verification, validation, and accreditation of the M&S. Without these updates and M&S accreditation, the survivability findings included in the report cannot be validated as accurate.

The Navy reports that current budget and schedule shortfalls preclude updates to vulnerability and recoverability M&S to reflect the as-built *Zumwalt*-class and inclusion of CPS when installed.

» EFFECTIVENESS AND SUITABILITY

Insufficient data are available to determine *Zumwalt*-class operational effectiveness and suitability or change the preliminary assessments provided in DOT&E's classified early fielding report from October 2022. In FY26, DOT&E will publish a classified interim operational testing assessment, updating the assessments of *Zumwalt*-class operational effectiveness and suitability for those areas where additional test data is available.

» SURVIVABILITY

Assessment of *Zumwalt*-class cyber survivability is classified. Failure and recoverability mode testing aboard USS *Michael Monsoor*, 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.

Data remain insufficient to determine *Zumwalt*-class survivability against threat weapons because the Navy did not update the outdated survivability M&S to credibly represent the ships as-built. DOT&E cannot evaluate shock survivability of the class without conducting a shock trial or alternate shock assessment. DOT&E will recommend that the survivability M&S be updated and validated as part of the upcoming TEMP revision and will hold open the requirement to conduct a shock trial unless an adequate alternate approach to shock survivability assessment is planned and funded.

In FY26, DOT&E will publish a classified interim operational testing assessment that includes an assessment of the *Zumwalt*-class cyber survivability as well as LFT&E survivability for those areas where data is available, including findings from testing aboard the ship in 2022.

RECOMMENDATIONS

The Navy should:

1. Complete remaining IOT&E events, as recommended in the FY23 and FY24 Annual Reports.
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, as recommended in the FY24 Annual Report.
3. Submit for DOT&E approval an update to the LFT&E Strategy that includes evaluation of the as-built *Zumwalt*-class following the installation of CPS, as recommended in the FY24 Annual Report.
4. Fund and schedule an FSST of a *Zumwalt*-class ship with CPS installed, as recommended in the FY23 and FY24 Annual Reports, or engage with DOT&E to determine an alternate method of assessing the risk of shock events to the class.
5. Document the risk to the warfighter associated with incomplete component shock qualification and lack of an FSST, as recommended in the FY22 – 24 Annual Reports.
6. Sufficiently fund modernization and sustainment of the *Zumwalt*-class to include improvements determined from failure and recoverability mode testing documented in the Navy's report on the event, as recommended in the FY22 – 24 Annual Reports.

E-2D Advanced Hawkeye

In FY25, the Navy began operational testing (OT) on the E-2D Delta System Software Configuration Build 5.1 (DSSC-5.1). DSSC-5.1 improves the Advanced Hawkeye's command and control capability and is the fifth in a series of biennial hardware and software upgrades to the E-2D.

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, 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 FY25, DOT&E approved the DSSC-5.1 FOT&E test plan and the E-2D Advanced Hawkeye TEMP Revision G, covering DSSC-5.1 and Global Lightning, a beyond-line-of-sight communications upgrade. During the OT period, OT-D5.1 began in June 2025 and is expected to conclude in 1QFY26. As part of DSSC-5.1 OT, the Navy conducted DSSC-4 Hawkeye Integrated Training System (HITS) OT, a holdover test event from the DSSC-4 TEMP, which was unable to be completed in FY24 due to HITS immaturity.

As reported in the FY24 Annual Report, the Navy presented a modeling and simulation framework for developing DSSC capabilities using the E-2D Systems Test and Evaluation Laboratory (ESTEL) in the DSSC-4 TEMP. 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

DSSC-5.1 evaluation 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-D5.1, and DOT&E awaits the conclusion of DSSC-5.1 OT to determine whether sufficient data exist to evaluate DSSC-5.1's operational effectiveness, suitability, and cyber survivability.

In 4QFY25, the Navy conducted DSSC-5.1 operational effectiveness and suitability test period OT-D5.1 in accordance with the DOT&E-approved test plan. Testing occurred on the Atlantic Test Ranges and incorporated the Aegis land-based test site at Wallops Island, Virginia. DOT&E observed a portion of these events. In September 2025, the Navy conducted DSSC-5.1 operational effectiveness and suitability testing during the GRAY FLAG 2025 large force test event at Naval Base Ventura County, California. DOT&E observed these test events.

The Navy intends to execute DSSC-5.1 cyber survivability testing in 1QFY26, in accordance with the DOT&E-approved test plan. This test will include a cooperative vulnerability and penetration assessment and an adversarial assessment.

PERFORMANCE

» 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 early fielding report. In 1QFY26, after the conclusion of HITS testing data analysis, DOT&E will publish a classified, final DSSC-4 FOT&E end-of-test report.

During the FY25 OT-D5.1 test period, DOT&E observed that E-2D operational test aircraft suffered shortfalls in overall availability, reliability, and logistic supportability. These shortfalls remain consistent with previous E-2D operational test periods, and DOT&E's DSSC-3 FOT&E report and DSSC-4 early fielding report had similar assessments on the suitability of the E-2D. Following the conclusion of the OT-D5.1 test period, DOT&E will publish a classified DSSC-5.1 FOT&E report, assessing operational effectiveness, suitability, and survivability.

RECOMMENDATIONS

As recommended in the FY23 and FY24 Annual Reports, 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. Accredit the ESTEL for use during OT of future DSSC builds.

F/A-18 Infrared Search and Track (IRST) Block II

The Navy completed F/A-18E/F Infrared Search and Track (IRST) Block II IOT&E in November 2024. IRST demonstrated the ability to detect operationally relevant targets at tactically relevant ranges, but it was not operationally suitable due to poor reliability. DOT&E's classified IOT&E report, published in February 2025, provided details on IRST operational effectiveness, suitability, and cyber survivability and informed the Navy's full-rate production decision in June 2025. DOT&E removed the IRST Block II program from oversight in July 2025, as program development has stabilized, and no significant upgrades are planned.

SYSTEM DESCRIPTION

The ASG-34A(V)1 F/A-18E/F IRST Block II 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 operates autonomously, or in combination with other sensors, to support the guidance of beyond-visual-range air-to-air missiles, particularly in a heavy electronic attack or radar-denied environment.

MISSION

The F/A-18E/F Super Hornet aircrew 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-18E/F IRST Block II is an Acquisition Category IC program. DOT&E placed IRST on oversight in September 2011. DOT&E approved the Milestone C TEMP in May 2021, and the IOT&E test plan in March 2024. The Navy began developmental testing on Block II pods in 2023 and completed IOT&E in November 2024. IRST entered full-rate production in June 2025, and the Navy is fielding IRST to carrier-based F/A-18E/F Super Hornet squadrons. DOT&E removed the IRST program from oversight in July 2025, as program development has stabilized, and no significant upgrades are planned.

» MAJOR CONTRACTORS

- Lockheed Martin Corporation – Orlando, Florida
- Boeing Defense, Space & Security – St. Louis, Missouri

TEST ADEQUACY

The Navy executed IOT&E flight testing between April and September 2024 and a ground cyber survivability test in November 2024. The Navy conducted testing in accordance with DOT&E-approved test plans, and DOT&E observed the events. DOT&E published a classified IOT&E report in February 2025. 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, reliability, and cyber survivability of the IRST Block II pod. However, resource and production constraints forced the developmental test and operational test squadrons to share the available IRST Block II pods, which contractor personnel maintained. This deviation from the planned use of dedicated pods with Navy maintainers prevented DOT&E from assessing IRST Block II maintainability.

PERFORMANCE

» EFFECTIVENESS

IRST Block II demonstrated the ability to detect operationally representative targets at tactically relevant ranges. However, IOT&E revealed some problems that limit the effectiveness of IRST Block II for air-to-air combat. Additional details are provided in the February 2025 classified IOT&E report.

» SUITABILITY

IRST Block II demonstrated significant reliability problems during IOT&E. Throughout the test period, IRST Block II experienced hardware and software deficiencies, which required the aircrew to restart the pod multiple times. Many of these problems were discovered during integrated and operational testing, after the Navy had completed a minimal developmental test program with the representative hardware.

Reliability improved during IOT&E with the release of two software updates. After the updates, the mean time between failures improved from 4 hours to 12 hours but still did not meet the required 40 hours. Additional details are provided in the February 2025 classified IOT&E report.

» SURVIVABILITY

Installing IRST Block II does not introduce additional cyber risk to the F/A-18. Additional details are provided in the February 2025 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 FY24 Annual Report.
2. Implement the recommendations provided in DOT&E’s February 2025 classified IRST Block II IOT&E report.

F/A-18E/F Super Hornet and EA-18G Growler

Left: F/A-18E Super Hornet | Right: EA-18G Growler

In FY25, the F/A-18E/F Super Hornet and EA-18G Growler programs tested two different system configuration set (SCS) builds. SCS H18 Release 3 FOT&E began in FY24 and extended into FY25, with events added to address problems discovered during operational test (OT). In March 2025, DOT&E published an early fielding report on F/A-18E/F and EA-18G SCS H18 Release 3 (versions 23.2.1 – 23.2.3). The Navy also began FOT&E of the FY25 Continuous Integration, Delivery, and Deployment (CID&D25) SCS build. CID&D25 testing is ongoing. DOT&E will publish a classified FOT&E report following the completion of the CID&D25 testing. DOT&E is awaiting final test data from the H18 Release 3 and the CID&D25 OT events, which is needed to evaluate operational effectiveness, suitability, and survivability.

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 and is also available as a Block II aircraft retrofit. The F/A-18E/F Block III Super Hornet, includes upgraded hardware, advanced cockpit displays, and improved networking capability.

The EA-18G Growler is a two-seat, electronic attack variant of the F/A-18F Super Hornet that can provide standoff, escort, and self-protection jamming using both noise and deception techniques against land- or surface-based and airborne radar systems. The EA-18G Growler carries up to five AN/ALQ-99 tactical jamming 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 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 for SCS updates. Urgent fleet capability needs are driving the Navy's acquisition strategy for tactical aircraft SCS releases.

In 2023, DOT&E approved the F/A-18E/F and EA-18G SCS H18 TEMP, and in 2024 DOT&E approved the H18 Release 3 FOT&E plan. The F/A-18 Super Hornet and EA-18G Growler SCS programs have completed H18 FOT&E, officially ending the H-series development strategy. In March 2025, DOT&E published an early fielding report on SCS H18 Release 3 (versions 23.2.1 – 23.2.3).

In FY25, the F/A-18E/F and EA-18G Program Office (PMA-265) completed the transition from the H-series development strategy to the more agile CID&D strategy for the F/A-18E/F and EA-18G platforms. The Navy's CID&D strategy prioritizes capabilities for annual releases and enables early releases to address urgent fleet needs. Each year the Navy will conduct developmental testing, integrated testing, and OT, leading to a fleet release. The Navy will also conduct a maintenance update period and, if needed, release an additional build after the fleet release to correct any severe problems discovered.

The Navy is currently conducting FOT&E of the CID&D25 build, which is focused on correcting existing issues. In September 2025, DOT&E approved the CID&D25 FOT&E plan and FY25 – 27 CID&D TEMP. DOT&E will report on the CID&D25 SCS performance once all FOT&E data are received and analyzed.

The Navy is developing the CID&D26 build, which will introduce new capabilities, some of which were originally planned for CID&D25. Open-Air Battle Shaping test instrumentation, which is essential for adequate mission-level evaluations, is built into SCS CID&D25 and expected to expand with CID&D26.

» MAJOR CONTRACTORS

- Boeing Defense, Space & Security – St. Louis, Missouri
- Raytheon, a subsidiary of RTX – Arlington, Virginia
- 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

In April 2024, the Navy began conducting FOT&E events (e.g., RIM OF THE PACIFIC and GRAY FLAG 2024), in accordance with the DOT&E-approved test plan for H18 Release 3 into FY25. During OT, the Navy identified several problems that required further software development, and released SCS versions 23.2.4, 23.2.5, and 23.2.6 to address them. The Navy planned to use BLACK FLAG 2025 and several standalone events to assess version 23.2.6. VX-9 – the operational test squadron for both platforms – attended BLACK FLAG 2025 with the F/A-18E/F and EA-18G platforms. VX-9 completed all the standalone events for the F/A-18E/F, but due to funding constraints, could not conduct the final standalone events for the EA-18G platform. Consequently, the Navy will not execute all testing planned for the EA-18G. DOT&E is still waiting to receive the version 23.2.6 test data and is unable to assess the build's performance or determine the effect of the missed events on EA-18G OT adequacy.

The Navy delivered the CID&D25 FOT&E plan to DOT&E in June 2025 and began CID&D25 FOT&E events in July 2025. DOT&E issued a memorandum approving data collection for several CID&D25 test events in July 2025 due to not receiving the FY25 – 27 CID&D TEMP prior to the beginning of OT. Because testing is ongoing, DOT&E is unable to assess test adequacy. The draft FY25 – 27 CID&D TEMP was sent out to all stakeholders in July 2025, and the final version was delivered to and approved by DOT&E in September 2025.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

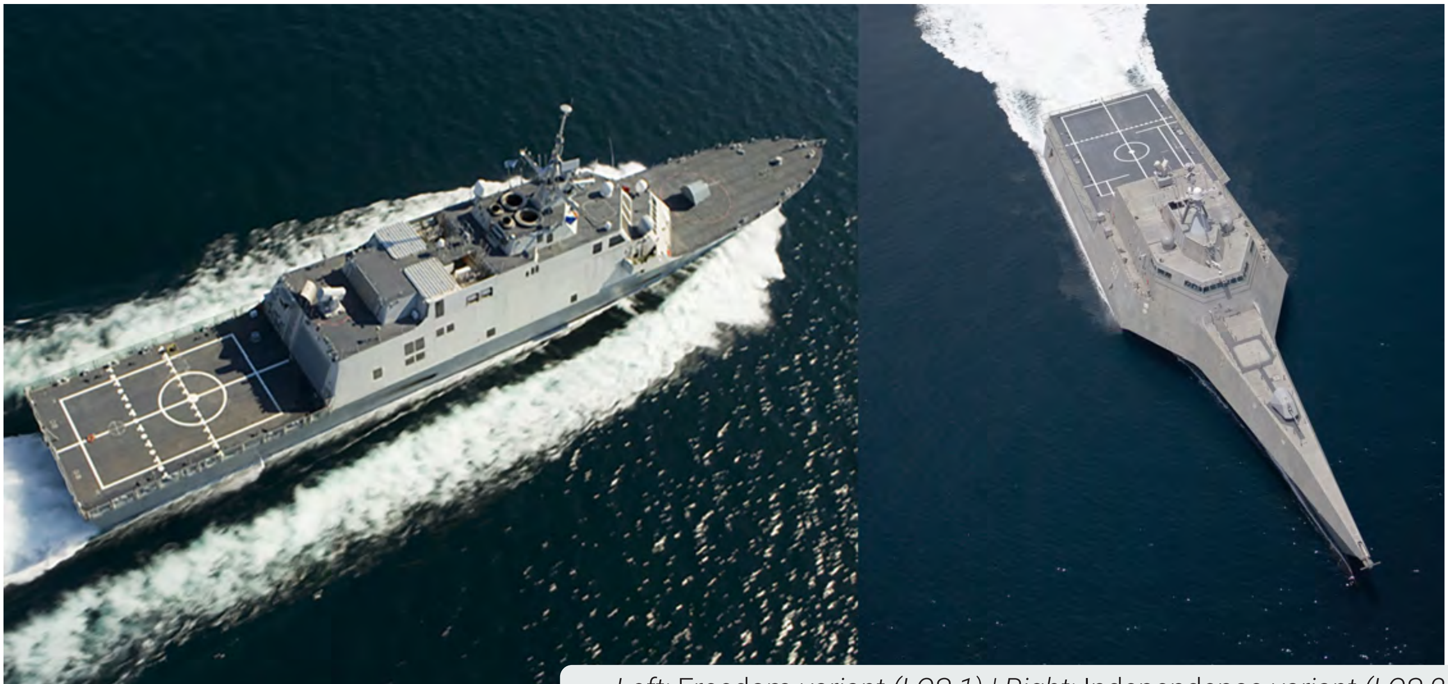
As testing is ongoing, insufficient data are available to assess the operational effectiveness, suitability, and survivability of F/A-18E/F and EA-18G with the CID&D25 SCS build. DOT&E will provide an assessment of the CID&D25 SCS build at the conclusion of FOT&E.

RECOMMENDATIONS

The Navy should:

1. Complete dedicated OT of CID&D25 to assess operational effectiveness, suitability, and survivability prior to fielding subsequent versions.
2. Continue to incorporate Open-Air Battle Shaping, high-fidelity active electronically scanned array threat radar emulators, and other new test assets (as they become available) into SCS FOT&E to improve data collection, integrity, and thoroughness, as recommended in the FY24 Annual Report.
3. Continue refining the CID&D strategy so that its implementation will ensure the Navy can deliver new capabilities to the F/A-18E/F and EA-18G platforms after adequate OT and efficiently addressing deficiencies.

Littoral Combat Ship (LCS)



Left: Freedom *variant (LCS 1) | Right:* Independence *variant (LCS 2)*

In FY25, the Navy conducted no operational tests of the Littoral Combat Ship (LCS) with the Mine Countermeasures (MCM) Mission Package (MP). In June 2025, the Secretary of the Navy certified the replacement of the *Avenger*-class MCM ships and the MH-53E Sea Dragon helicopters in the U.S. Central Command (USCENTCOM) area of responsibility with the *Independence* variant of the LCS with MCM MP complemented by existing Expeditionary MCM capabilities.

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
- An 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 system, pending continued system development:

- Barracuda Mine Neutralization System employed from MCM USV

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 FY22, the Navy divested the Anti-Submarine Warfare MP. In FY25, the final *Independence* variant ship and the second-to-last *Freedom* variant ship were delivered. The final *Freedom* variant ship will deliver in 1QFY26.

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. An additional payload – the Barracuda Mine Neutralization System – is in development for future integration into MCM USV. The Navy is also implementing a variety of enhancements to improve communications range, system endurance, system employment depth, and post-mission analysis.

In June 2025, the Secretary of the Navy certified that 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. The Navy is in the process of planning a separate certification for the U.S. Indo-Pacific Command area of responsibility.

» 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 FY25, the Navy introduced no modifications to the *Freedom* variant that would change SUW MP performance and conducted no operational testing.

In FY25, the Navy conducted no operational testing on the *Independence* variant with the MCM MP. 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 field in FY16 without conducting IOT&E. The Navy has provided relevant fleet data from current employments of AMNS and ALMDS, but the data are insufficient to make a determination.

As discussed in DOT&E's FY24 Annual Report, the Navy deferred 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 the test asset. DOT&E accepted data from Naval Sea System Command (NAVSEA) Red Team cyber security testing conducted onboard USS *Canberra* (LCS 30) with MCM MP embarked, but scope of test was insufficient to determine cyber survivability.

The Navy program office has communicated that it does not intend to conduct a cyber survivability evaluation and an operational performance evaluation of AMNS and ALMDS, which are needed 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.

The Navy has not provided sufficient data from operational employment of AMNS and ALMDS to determine operational effectiveness of the *Independence* variant with MCM MP.

» 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.

The Navy has not provided sufficient data from operational employment of AMNS and ALMDS to determine operational suitability of the *Independence* variant with MCM MP. 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.

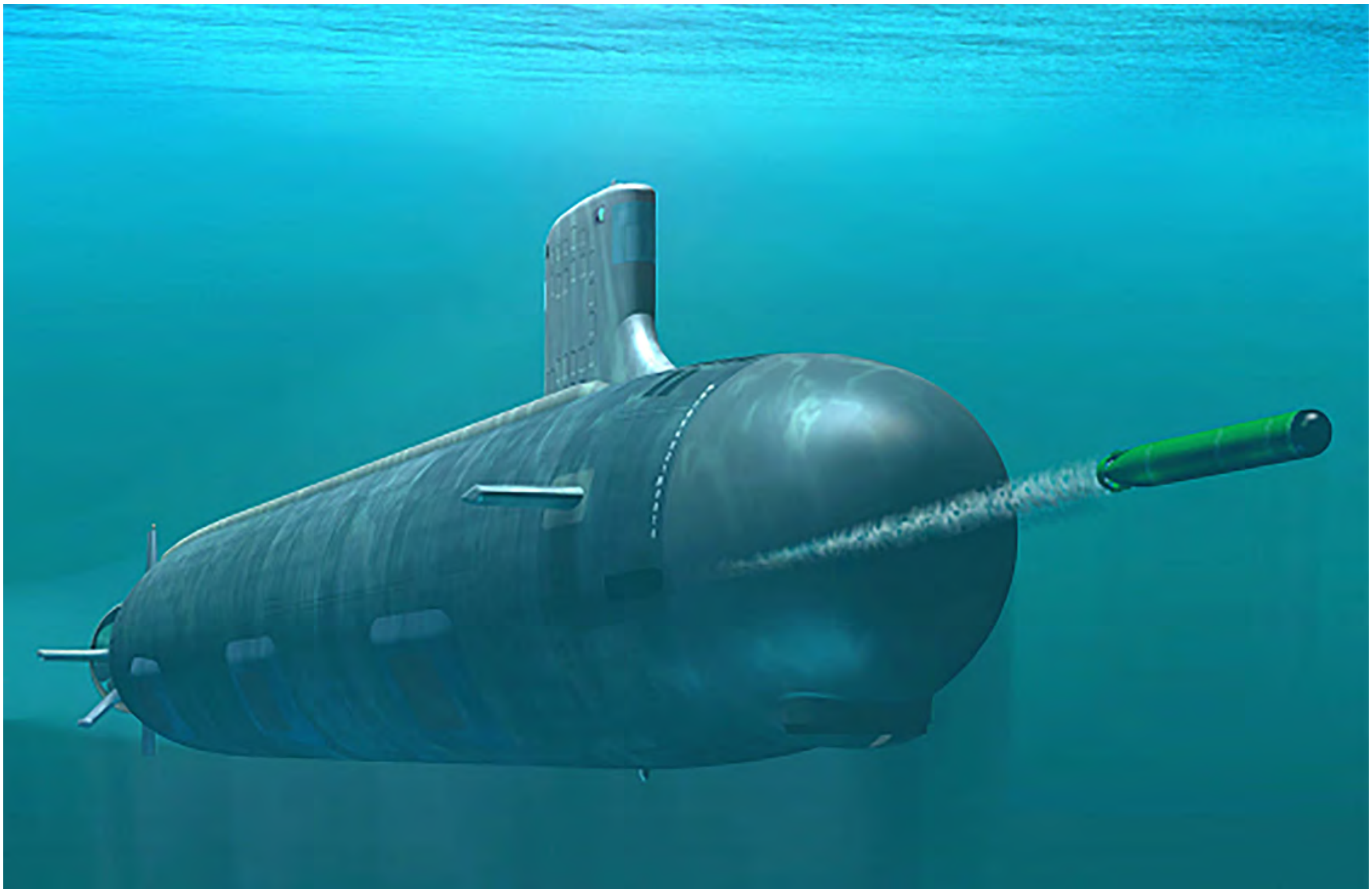
Insufficient data are available to determine cyber survivability of the *Independence* variant with MCM MP.

RECOMMENDATIONS

The Navy should:

1. Submit for DOT&E approval an update to the LCS TEMP that addresses changes in the test program, or issue an official memorandum detailing plans and intentions to discontinue testing, in lieu of a TEMP update.
2. Continue to engage with OPTEVFOR and DOT&E to scope future testing requirements as capability changes occur for either of the LCS seaframes, the SUW MP, and the MCM MP.

Mk 48 Torpedo Modifications



In May 2025, the Navy conducted 30 torpedo firing test events, during two separate fleet exercises, to evaluate Mk 48 Mod 7 Advanced Processor Build (APB) 6 and collect additional data on the Shallow Water Urgent Build (SWUB). In July 2025, DOT&E removed the Mk 48 program from oversight for operational testing; however, the program remains on oversight for LFT&E lethality assessment.

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 (in development) implements 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, including 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 6 and 7 torpedoes) – Modifications focused on detection and discrimination of target submarines and 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 developed in FY23 and fielded in FY24 to address a classified urgent fleet need. The capability is an add-on to APB 5 and will be included in future baselines.
- 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.

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 Mod 7 Heavyweight Torpedo with SWUB Software. The Navy fielded the Mk 48 with SWUB the following month. In July 2025, DOT&E removed the Mk 48 program from oversight for operational testing, but will keep it on oversight for an LFT&E lethality assessment.

The Navy is completing integrated testing of the Mk 48 Mod 7 APB 6 and expects to complete FOT&E in FY27.

The Navy is developing Mod 8 APB 6 and intends to reach a Milestone C decision in FY27 and complete FOT&E in FY29. The Navy initiated Mod 9 development in December 2023 as an MTA rapid prototyping effort with operational demonstration planned within five years.

» MAJOR CONTRACTORS

- Lockheed Martin Sippican, Inc. – Marion, Massachusetts
- Lockheed Martin Corporation – Syracuse, New York
- Science Applications International Corporation, Inc. – Reston, Virginia

TEST ADEQUACY

In May 2025, the Navy fired 30 torpedoes during two separate fleet exercises, to gather additional data on SWUB capability. Twelve of the 30 torpedoes employed APB 6 software to support operational testing of the Mod 7 APB 6 variant. Previous SWUB test events suffered from limited operational realism, preventing DOT&E from making an end-to-end performance assessment.

Due to removal of the Mk 48 program from oversight in July 2025 for operational testing, the two May 2025 test events were not evaluated by DOT&E.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

In July 2025, DOT&E determined the Mk 48 program no longer requires DOT&E oversight as it is not a Major Defense Acquisition Program under the current acquisition strategy. As a major munitions program, the program remains on oversight for LFT&E lethality assessment.

» LETHALITY

DOT&E did not evaluate lethality in FY25. The Mk 48 program remains on DOT&E oversight for lethality and will be evaluated as changes to the weapons system are made that affect lethality.

RECOMMENDATION

The Navy should:

1. Address the outstanding recommendations, as provided in the FY24 Annual Report.

MQ-25® Stingray Carrier Based Unmanned Aerial System (CBUAS)

In May 2025, the Navy received its first MQ-25 air test vehicle. The Navy is planning to transition the program to Milestone C (MS C) in FY26, and to submit a MS C TEMP to DOT&E for approval in 1QFY26.

MQ-25® is a registered trademark of the Department of the Navy.

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-25A 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-25A 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. MQ-25A will be the first operational, carrier-based, fixed-wing, and catapult-launched UAS.

In the DOT&E-approved MQ-25 MS B TEMP, published in 2020, the Navy scheduled the MS C decision for FY23, and an operational assessment (OA) based on testing up to and including initial sea trials to inform their decision. However, in December 2022, based on production delays and sub-vendor quality control issues, 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. DOT&E assessed this EOA as inadequate for a MS C decision for multiple reasons. First, there are significant differences between the prototype and the MQ-25A Engineering Development Model (EDM) design. These differences include, but are not limited to, internal structures, fuel system design, communications, and network architecture. 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.

Due to an extension of the engineering and manufacturing development phase, as well as delays with production of test air vehicles, MS C did not occur in FY23. The Navy received the first MQ-25 EDM air test vehicle in May 2025 and expects to conduct the first flight test event in 1QFY26. Because production delays rendered the 2020 MS B TEMP's ground and flight test schedule obsolete, DOT&E recommended that the Navy produce an updated MS B TEMP to accurately scope and resource MQ-25 integrated test events, including outlining an adequate OA that would inform a MS C decision. In FY25, the MQ-25 Program Office developed a MS B TEMP update and submitted it to the Navy for approval, but the Navy rejected this update and directed the creation of a MS C TEMP to support a MS C decision that was then planned for 4QFY25. DOT&E assessed that insufficient data existed to inform a MS C decision because the Navy has not completed an adequate EOA or OA with production-representative air vehicles or a production-representative ground station. In 1QFY26, the Navy submitted an adequate MS C TEMP to DOT&E for approval, and DOT&E approved the MS C TEMP in November 2025. The Navy plans to transition the program to MS C in FY26.

» MAJOR CONTRACTORS

- Boeing Defense, Space & Security – St. Louis, Missouri (MQ-25A Stingray)
- Lockheed Martin Corporation – Marietta, Georgia (MDCX)

TEST ADEQUACY

DOT&E has not approved any operational test plans for MQ-25. The Navy should submit to DOT&E for approval a test plan that 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. Therefore, the OA should use non-prototype air vehicles and incorporate all ground and flight test events up to and including the first CVN flight test period. An OA traditionally informs a MS C decision, and the Navy should use the data from this OA to inform the joint force regarding MQ-25 capabilities and limitations prior to initial operational capability (IOC).

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. Conduct an adequate OA prior to MQ-25 IOC.

MQ-4C Triton

The MQ-4C Triton program has not entered IOT&E. Immature systems that prevented IOT&E in FY23 persist in precluding operationally representative testing for the primary missions. The Navy has continued to field new MQ-4C configurations in FY25 without operational testing. In May 2025, DOT&E published a classified early fielding report (EFR) for MQ-4C Triton Integrated Functional Capability (IFC) 4.2.1. Integrated testing indicates that signals intelligence (SIGINT) deficiencies continue to challenge the execution of operationally realistic testing.

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 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 NDAA prohibits the Navy from retiring or preparing to retire the EP-3E until it fields one or more platforms that, in the aggregate, provide an equivalent or superior capability.

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. As previously reported, DOT&E published a classified EFR regarding that configuration in August 2023. Since then, the Navy has not started IOT&E, but has fielded the IFC 4.1.2.4, IFC 4.1.2.6, IFC 4.2, IFC 4.2.1, and Flight Release (FR) 5.0 configurations. DOT&E published an unclassified early fielding report regarding IFC 4.1.2.6 in January 2024, addressing only test adequacy, and another, classified EFR in May 2025 regarding IFC 4.1.2.6 through 4.2.1. DOT&E deferred publishing the latter EFR from December 2024, as reported in the FY24 Annual Report, to incorporate observations from additional testing.

» MAJOR CONTRACTOR

- Northrop Grumman Corporation Aeronautics Sector – Rancho Bernardo, California

TEST ADEQUACY

The Navy has not started IOT&E. As stated in previous annual reports, 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. DOT&E subsequently approved conduct of the electronic intelligence and communications intelligence portions of the IOT&E plan for integrated testing in December 2024.

The MQ-4C integrated test team conducted three dedicated SIGINT flights in December 2024 at the Atlantic Test Range, with a system in the IFC 4.2.1 configuration, to assess the performance of the SIGINT systems. These flights were conducted in accordance with a DOT&E-approved test plan, and DOT&E observed these events. The test team also conducted integrated testing with systems in Test Release 5.0 configurations as part of large force exercises in April and August 2025.

The Navy has not conducted any operational testing of the effectiveness or suitability of the fielded IFC 4.1.2.4, 4.1.2.6, 4.2, 4.2.1, or FR 5.0 configurations.

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 previous annual reports, 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. Any effects of the changes in IFC 4.1.2.4, IFC 4.1.2.6, IFC 4.2, IFC 4.2.1, and FR 5.0 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 Joint Signal Processor (JSP) capability and an update on SIGINT systems are provided in the May 2025 classified EFR. Integrated testing in FY25 indicates that SIGINT deficiencies continue to challenge the execution of operationally realistic testing.

» SUITABILITY

As stated in previous Annual Reports, 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 a suitability assessment occurred during JSP testing. An update of the operational suitability of the MQ-4C in the IFC 4.2 configuration is provided in the May 2025 classified EFR.

» SURVIVABILITY

An initial assessment of the survivability of the MQ-4C in contested cyberspace is provided in the May 2025 classified EFR.

RECOMMENDATIONS

As recommended in EFRs 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.

Next Generation Jammer Mid-Band (NGJ-MB)

The Navy completed Next Generation Jammer Mid-Band (NGJ-MB) IOT&E in December 2024. In July 2025, DOT&E published a classified IOT&E report to inform a full-rate production decision review, which occurred in September 2025. Although challenges still exist, the NGJ-MB performed as well as, and in some cases better than, the legacy AN/ALQ-99 against the threats tested on the open-air test ranges. The NGJ-MB is currently not suitable for supporting operational missions, primarily due to lingering reliability concerns, but is continuing to develop into its potential.

SYSTEM DESCRIPTION

The NGJ-MB is an airborne electromagnetic attack system that consists of two pods, mounted under the EA-18G wings, containing active electronically scanned arrays that transmit over a range of frequencies. The NGJ-MB is the first of three proposed programs for the overall NGJ upgrade that is intended to augment and eventually replace the legacy AN/ALQ-99 Tactical Jamming System on the EA-18G. The NGJ-MB will add increased jamming capability at higher effective power and longer ranges than the AN/ALQ-99 Tactical Jamming System, and the ability to rapidly update hardware and software to counter rapidly evolving threat characteristics.

MISSION

Combatant commanders will employ EA-18G Growlers equipped with the NGJ-MB to deny, degrade, or disrupt the adversary's use of the electromagnetic spectrum, while enabling and protecting friendly forces. The NGJ-MB is typically employed as a capability of a carrier air wing embarked on an aircraft carrier in support of operations in a carrier strike group or deployed from a forward location in support of operational forces overseas.

PROGRAM

The NGJ-MB is an Acquisition Category IC program. In June 2021, the Secretary of the Navy approved the NGJ-MB program to move past Milestone C, thereby authorizing procurement of low-rate initial production pods. The Navy certified the NGJ-MB for IOT&E in April 2023, and DOT&E approved the IOT&E test plan in July 2024. The Navy completed IOT&E in December 2024, with a full-rate production decision expected in September 2025. The Navy has deployed the NGJ-MB to five different Electronic Attack Squadrons.

Currently, the program is updating the TEMP to include the NGJ-MB Extended (NGJ-MBX) engineering change proposal, which will extend the frequency range of the NGJ-MB to counter a broader class of threats.

» MAJOR CONTRACTORS

- Raytheon, a subsidiary of RTX – El Segundo, California
- The Boeing Company – St. Louis, Missouri
- Northrop Grumman Mission Systems – Linthicum, Maryland

TEST ADEQUACY

The Navy completed IOT&E in December 2024, with all operational testing performed in accordance with the DOT&E-approved TEMP and test plans, and observed by DOT&E. The IOT&E was adequate to assess NGJ-MB operational effectiveness against the threats used in the test, given the available range resources, as well as operational suitability and cyber survivability.

Due to the range infrastructure limitations, which limited the ability of open-air ranges to support an adequate complex electromagnetic environment and testing against cutting-edge adversary systems, DOT&E used the program's modeling and simulation data to supplement the operational effectiveness assessment.

DOT&E assessed cyber survivability using an analysis of supply chain security as well as the results from developmental cyber testing, in accordance with the DOT&E-approved IOT&E test plan.

PERFORMANCE

» EFFECTIVENESS

The NGJ-MB is assessed to be at least as operationally effective as the legacy AN/ALQ-99 system, against the threats tested on the open-air test ranges during IOT&E. DOT&E's full assessment of operational effectiveness is provided in the classified IOT&E report published in July 2025.

» SUITABLITY

The NGJ-MB with the OFP 5.3 software series is not currently suitable for supporting operational missions, due to additional progress required to improve reliability and availability. The NGJ-MB system met its maintainability requirements, and aircrew and maintainers found training to be adequate. Insufficient data are currently available to draw any significant conclusions on pilot and maintainer workload and usability, given the sample size of the data. Additional details on suitability are provided in the classified IOT&E report published in July 2025.

» SURVIVABILITY

DOT&E's assessment of NGJ-MB cyber survivability is provided in the classified IOT&E report published in July 2025.

RECOMMENDATIONS

The Navy should:

1. Continue to explore options for testing NGJ-MB against the most challenging threat systems and scenarios available.
2. Address the recommendations within the July 2025 classified IOT&E report.
3. Support investments to improve the modeling and simulation, hardware-in-the-loop, anechoic chambers, and open-air flight test ranges required to test this system and others, such as the EA-37B, operating in a modern, complex electromagnetic environment representative of combat against a peer adversary.

Offensive Anti-Surface Warfare (OASuW) Increment 1

In FY25, the Offensive Anti-Surface Warfare (OASuW) Increment 1 program conducted an AGM-158C-1 Long Range Anti-Ship Missile (LRASM 1.1) operational test (OT) event, employing a salvo of seven missiles against a moving maritime target, and conducted a cyber survivability cooperative vulnerability and penetration assessment (CVPA). The OT event provided new data that will be detailed in the classified IOT&E report expected in FY26. The Navy continues its development on the next missile upgrade, LRASM C-3, which brings a 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 a U.S. Pacific Fleet urgent 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.

Two variants of LRASM comprise the OASuW Increment 1 program: the AGM-158C and the AGM-158C-3. The AGM-158C was delivered in two increments – LRASM 1.0 and LRASM 1.1 – and all AGM-158C have been upgraded to the LRASM 1.1 configuration.

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 Defense Advanced Research Projects Agency (DARPA)'s LRASM initiative as the weapon system for OASuW Increment 1. DOT&E approved the LRASM 1.1 Master Test Strategy (MTS) in January 2020, in lieu of a TEMP. In 2QFY23, the Navy announced the intention to field LRASM 1.1, following FY22 integrated test 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 upon completion of IOT&E flights, modeling and simulation (M&S), and cyber survivability testing in FY26 to inform continued fielding.

In FY22, the Navy began development of LRASM C-3 to bridge the capability gap against predicted threats until an OASuW Increment 2 program of record is established. 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. In FY25, the Navy continued drafting the LRASM C-3 TEMP and continues to work through the details required to plan and execute test events to meet the LRASM C-3 early operational capability in 4QFY26.

» MAJOR CONTRACTOR

- Lockheed Martin Missiles and Fire Control – Orlando, Florida

TEST ADEQUACY

With DOT&E approval, the Navy began LRASM 1.1 IOT&E data collection in July 2024, as the complete IOT&E test plan was not ready. In March 2025, DOT&E approved the LRASM 1.1 IOT&E test 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 will include increased threat realism to the extent practicable to provide better validation data for the M&S tools.

In March 2025, the Navy completed one LRASM 1.1 OT flight event and engaged a moving maritime target with a salvo of seven free-flight evaluation missiles employed from F/A-18E/F aircraft. This test event included kill chain participants, employment conditions, and a test scenario that were more operationally representative, and more stressing, than was used for prior integrated test events. This OT flight event resulted in new data that will be detailed in the classified combined IOT&E and LFT&E report that DOT&E will publish after operational flight, cyber survivability, and M&S tests are complete in FY26.

In May 2025, the Navy performed a LRASM 1.1 CVPA cyber survivability test event. This will be followed by an adversarial assessment, which is the final cyber survivability test event for LRASM 1.1 and expected in 1QFY26. In FY25, the Navy continued development of the M&S environment and continued work to support M&S validation, verification, and accreditation, in preparation for the start of the OT M&S runs for record in 1QFY26.

The Navy continued preparations to conduct an OT event with an LRASM 1.1 All-Up-Round (AUR) employed from an F/A-18E/F aircraft against a maritime target in FY26. The Navy should develop, and submit to DOT&E for approval, an LFT&E test plan to ensure that this event will provide the data required to evaluate the lethality of LRASM 1.1. The Navy previously attempted to conduct this event in July 2024; however, the required data were not collected. Without the data from an AUR test event to augment this limited dataset, the Navy will have difficulty validating previously run or future lethality M&S.

The Navy continued to develop the LRASM C-3 TEMP and OT plan in FY25.The Navy should continue to work with DOT&E to develop, resource, and execute an adequate OT&E and LFT&E plan for LRASM C-3.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

OT is ongoing and limited data are available for an assessment of the operational effectiveness, lethality, suitability, and survivability of LRASM 1.1. DOT&E will provide an assessment in the classified combined IOT&E and LFT&E report, once testing and analysis are complete in FY26.

RECOMMENDATIONS

The Navy should:

1. Complete development, verification, validation, and accreditation of the M&S environment to facilitate the evaluation of LRASM 1.1, as recommended in the FY24 Annual Report.
2. Submit for DOT&E approval an LRASM 1.1 LFT&E test plan.
3. Complete LRASM 1.1 IOT&E, including the LRASM 1.1 lethality test event, to support continued fielding.
4. Complete development of the LRASM C-3 TEMP and OT plan and submit both for DOT&E approval.

Over-The-Horizon Weapon System (OTH-WS)

In FY25, in partnership with the Air Force's Joint Strike Missile program, the Navy executed four warhead arena tests of the Over-The-Horizon Weapon System (OTH-WS) in accordance with the DOT&E-approved LFT&E Strategy. A total of three more arena tests remain in the series. In July 2025, DOT&E removed the OTH-WS program from oversight for operational testing (OT); however, the program remains on DOT&E oversight for live fire (LF), which will culminate with a lethality assessment.

SYSTEM DESCRIPTION

The OTH-WS is a standalone system providing surface-to-surface missile capability that the Navy intends to use to defeat maritime targets inside and beyond the firing unit's radar horizon. The Navy employs the OTH-WS on *Independence*-class littoral combat ships, with plans to employ it from *Arleigh Burke*-class guided missile destroyers and *Constellation*-class guided missile frigates. 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). The Air Force's Joint Strike Missile utilizes same warhead and the NSM.

PROGRAM

OTH-WS is an Acquisition Category II, non-developmental item program. The U.S. Navy and Kongsberg Defence and Aerospace (KDA) are responsible for integrating the OTH-WS onto Navy platforms. 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, OT and LFT&E events (including arena/sled tests and M&S) continued to be delayed due to funding shortfalls and test asset reallocation to support the Marine Corps NMESIS project.

In March 2017, DOT&E placed OTH-WS on OT and LF oversight, as a high-interest item filling a critical warfighting gap. In July 2025, DOT&E removed OTH-WS from OT oversight. OTH-WS remains on oversight for LF to complete a lethality assessment.

» MAJOR CONTRACTORS

- Raytheon, a subsidiary of RTX – Tucson, Arizona
- Kongsberg Defence and Aerospace – Kongsberg, Norway

TEST ADEQUACY

In FY25, the Navy partnered with the Air Force's Joint Strike Missile Program to conduct four arena tests of the OTH-WS warhead at Eglin Air Force Base, Florida, in accordance with the DOT&E-approved test plan. DOT&E observed the first of these tests in February 2025. The fourth and final test in FY25 was not completed due to a yet undetermined test issue. Two more arena tests remain in the series. These tests are defined within the OTH-WS TEMP and provide warhead blast and fragmentation data to support the lethality evaluation of the system against its target set.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E removed OTH-WS from OT oversight and will not be assessing the operational effectiveness, suitability, and cyber survivability of the OTH-WS. The Navy intends to complete OT in FY27 after completion of the modeling and simulation (M&S) OT runs for the record.

» LETHALITY

Insufficient data are available to assess the lethality of the OTH-WS. The three live flight tests in FY21 demonstrated that the OTH-WS has potential to provide the Navy with an over-the-horizon capability to engage surface ships. However, the Navy has not fully characterized this capability.

The Navy completed verification and validation of their lethality M&S in FY25 but has yet to accredit it. After the remaining warhead arena tests are completed, the Navy will use the data to improve the representation of the warhead's blast and fragmentation characteristics in the lethality M&S and use the updated M&S to predict lethality against representative maritime targets.

The Navy procured sleds to support tests in FY25 and currently plans to conduct one test in FY26. The Navy continues to request resources to complete the remaining five sled tests. These tests are required to verify the warhead will survive impact against maritime targets and fuze successfully inside the target.

RECOMMENDATION

As recommended in the DOT&E FY24 Annual Report, the Navy should:

1. Fund and schedule the arena tests, sled tests, and M&S runs for adequate evaluation of OTH-WS.

Surface Electronic Warfare Improvement Program (SEWIP)

Top Left: SEWIP Block 2 on an Arleigh Burke*-class destroyer*
Bottom Left: SEWIP Block 3 on an Arleigh Burke*-class destroyer*
Right: USS Mason *(DDG 87), where SEWIP Block 2 FOT&E events were to occur in FY25*

In FY25, the Navy's Operational Test and Evaluation Force (OPTEVFOR) intended to conduct operational testing of the AN/SLQ-32(V)6 variant of SEWIP Block 2 on USS *Mason* (DDG 87). However, unfavorable weather conditions and platform issues related to the system under test prevented execution of the test.

In September 2025, DOT&E approved OPTEVFOR's cyber survivability test plan for Aegis Combat System, Advanced Capability Build (ACB) 16 Baseline 9.C2.3, which included AN/SLQ-32(V)6 boundary scans. Later that month, OPTEVFOR conducted the cyber test on USS *Frank E. Petersen Jr.* (DDG 121), including data collection from AN/SLQ-32(V)6.

SYSTEM DESCRIPTION

SEWIP is a series of planned evolutionary upgrades to the surface Navy electronic warfare (EW) capability, AN/SLQ-32, which detects, identifies, and tracks threat anti-ship missiles and targeting radars. Block 2 is the second in the series of upgrades with the introduction of the AN/SLQ-32(V)6 EW system, providing improved electronic surveillance. SEWIP Block 2 incorporates a new antenna system, enhanced processing capabilities, and associated hardware to improve battlefield situational awareness. Some AN/SLQ-32 variants include SEWIP Block 2 with additional software, known as the Soft Kill Coordination Subsystem (SKCS), to improve use of EW countermeasures, such as decoys, by utilizing combat system information to counter threats.

SEWIP Block 3 provides an advanced electronic attack (EA) capability, integrated with AN/SLQ-32(V)6 system and incorporates the Block 2 electronic surveillance receivers, which together make AN/SLQ-32(V)7. SEWIP Block 3 provides the following additional functions:

- Transmission of advanced EA waveforms to engage anti-ship missiles as well as land-based, shipboard, and airborne targeting platforms.
- Provide an onboard EA capability with increased frequency coverage and power relative to previous AN/SLQ-32(V)3.

MISSION

Navy commanders use AN/SLQ-32(V)6 to perform anti-ship missile defense (ASMD), counter-targeting, and counter-surveillance, similar to earlier variants of the AN/SLQ-32. SEWIP Block 2 upgrades the electromagnetic support capabilities and integrates more closely with the combat system to improve ASMD against emerging threats.

Navy commanders will use AN/SLQ-32(V)7 EA capability to engage anti-ship missiles and targeting radars, improving ship survivability.

PROGRAM

SEWIP is the U.S. Navy initiative to upgrade the AN/SLQ-32 EW system on surface ships.

SEWIP Block 2 is an Acquisition Category II program that achieved Milestone C in January 2013. The program 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 with the Total Ship Computing Environment (TSCE) combat system.
- AN/SLQ-32B(V)6 on *Gerald R. Ford*-class aircraft carriers with the Ship Self-Defense System (SSDS) combat system.

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 TSCE combat system on the *Zumwalt*-class, and the SSDS combat system on the *Gerald R. Ford*-class.
- Combat system integration and decoy integration capabilities of the SKCS for the variant fielded on *Arleigh Burke*-class destroyers with the Aegis Combat System.

DOT&E has approved the following test plans relevant to SEWIP Block 2:

- AN/SLQ-32(V)6 operational test plan in October 2024.
- AN/SLQ-32A(V)6 operational test plan in July 2023.
- AN/SLQ-32B(V)6 operational test plan in April 2021.
- DDG 1000 cyber survivability test plan, which included testing of AN/SLQ-32A(V)6, in November 2022.
- CVN 78 cyber survivability test plan, which included testing of AN/SLQ-32B(V)6, in February 2024.
- Aegis Combat System ACB 16 cyber survivability test plan, which included boundary scans of AN/SLQ-32(V)6, in February 2025, and an update for data collection of AN/SLQ-32(V)6 in September 2025.

SEWIP Block 3 is a separate Acquisition Category II program. SEWIP Block 3 currently has one variant, which has distinct hardware and software suites:

- AN/SLQ-32(V)7 on *Arleigh Burke*-class (Flight IIA) destroyers.

The Navy expects to deliver a SEWIP Block 3 TEMP to DOT&E for approval in FY26 to support IOT&E of AN/SLQ-32(V)7. In January 2025, DOT&E approved the AN/SLQ-32(V)7 IOT&E test plan. The Navy expects to deliver the SEWIP Block 3 cyber survivability test plan in FY26.

» MAJOR CONTRACTORS

- Lockheed Martin Corporation – Syracuse, New York
- Northrop Grumman Corporation – Baltimore, Maryland

TEST ADEQUACY

OPTEVFOR intended to complete operational effectiveness and suitability testing of the

AN/SLQ-32(V)6 variant of SEWIP Block 2 on USS *Mason* (DDG 87) in FY25. However, unfavorable weather conditions and platform issues related to the system under test prevented execution of the test. The Navy is currently examining options to conduct the remaining testing required to conclude FOT&E of the AN/SLQ-32(V)6 variant of SEWIP Block 2.

In September 2025, OPTEVFOR began cyber survivability testing of Aegis Combat System ACB 16 Baseline 9.C2.3 on USS *Frank E. Petersen Jr.* (DDG 121), in accordance with the DOT&E-approved Aegis Combat System ACB 16 cyber survivability test plan. The event included cyber survivability boundary scans of AN/SLQ-32(V)6. OPTEVFOR will use the results from the DDG 121 boundary scans, along with the AN/SLQ-32A(V)6 cyber survivability testing detailed in the FY23 Annual Report and the AN/SLQ-32B(V)6 cyber survivability testing detailed in the FY24 Annual Report, to complete cyber survivability evaluation of SEWIP Block 2.

The Navy plans to complete the remaining operational effectiveness, suitability, and cyber survivability testing for FOT&E of AN/SLQ-32(V)6 in FY26; however, the Navy has not scheduled the remaining operational effectiveness and suitability testing for FOT&E of AN/SLQ-32A(V)6 (*Zumwalt*-class destroyers) due to ship availability. OPTEVFOR completed operational effectiveness and suitability testing of AN/SLQ-32B(V)6 in FY21.

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 is currently working to fund improvements to existing threat emulators for test, in accordance with recommendations DOT&E has included in the annual report since FY21. These assets are needed for both SEWIP Block 2 FOT&E and SEWIP 3 IOT&E to adequately evaluate operational effectiveness and suitability. Additionally, all SEWIP variants require testing in comprehensive and complex electromagnetic spectrum environments to fully evaluate their effectiveness in a realistic combat environment.

OPTEVFOR had planned to commence SEWIP Block 3 IOT&E with testing of AN/SLQ-32(V)7 aboard USS *Pinckney* (DDG 91) in September 2025, in accordance with the DOT&E-approved AN/SLQ-32(V)7 IOT&E test plan; however, the testing was delayed due to ship availability. The Navy is evaluating the *Arleigh Burke*-class destroyer ships' availabilities to schedule and conduct IOT&E.

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 publish a classified FOT&E report on SEWIP Block 2, with operational effectiveness and suitability assessments, when the Navy completes SEWIP Block 2 FOT&E, currently expected in FY26.

SEWIP Block 3 has not yet started IOT&E.

» SURVIVABILITY

Insufficient data are available to determine cyber survivability of SEWIP Block 2 due to ongoing testing on AN/SLQ-32(V)6. DOT&E will deliver a classified FOT&E report for SEWIP Block 2, with a cyber survivability assessment, when the Navy completes SEWIP Block 2 FOT&E, currently expected in FY26.

SEWIP Block 3 has not yet started IOT&E.

RECOMMENDATIONS

The Navy should:

1. Fund the resources for more stressing threats within threat stimulators and incorporate them into remaining SEWIP test events as they become available, as recommended since the FY21 Annual Report.
2. Schedule and complete remaining tests for operational effectiveness, suitability, and cyber survivability of AN/SLQ-32A(V)6 and AN/SLQ-32(V)6 in FY26.
3. Deliver the SEWIP Block 3 IOT&E TEMP and cyber survivability test plan for AN/SLQ-32(V)7 in FY26.

T-AO 205 *John Lewis*-Class Fleet Replenishment Oiler

In February 2025, T-AO 205 *John Lewis*-class completed IOT&E, and in May 2025, DOT&E published a classified combined IOT&E and LFT&E report. The T-AO 205 class was determined to be operationally effective and suitable, demonstrating the ability to deliver fuel and cargo to combatant, amphibious, and logistics ships. DOT&E removed the T-AO 205 *John Lewis*-class program from oversight in July 2025, as IOT&E, LFT&E, and associated reporting were complete.

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.

T-AO 205 class ships have port and starboard refueling stations, an astern fuel delivery station, connected cargo transfer stations, and a vertical replenishment station from the flight deck.

Each T-AO 205 class ship has an advanced degaussing system, the Nixie torpedo countermeasure system, and mounts for security team machine guns. The ships have 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 with 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 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, T-AO 207 in May 2024, and T-AO 208 in December 2024. Five ships (T-AOs 209 – 213) are under construction.

DOT&E approved the TEMP Revision 1 in September 2021 and IOT&E test plan in October 2022.

DOT&E removed the T-AO 205 *John Lewis*-class from oversight in July 2025, as IOT&E and LFT&E are complete and the associated combined IOT&E and LFT&E report was released in May 2025 to inform the full-rate production decision planned for FY26.

» MAJOR CONTRACTOR

- General Dynamics NASSCO – San Diego, California

TEST ADEQUACY

The Navy evaluated cyber survivability of T-AO 205 class 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 October 2022 and July 2023, the Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted IOT&E onboard USNS *John Lewis* (T-AO 205), in accordance with the DOT&E-approved test plan and observed by DOT&E. Between April 2024 and December 2024, OPTEVFOR continued IOT&E aboard USNS *Oscar V. Peterson* (née *Harvey Milk*) (T-AO 206). The Navy declared IOT&E testing complete in February 2025. The T-AO 205 class demonstrated the ability to deliver fuel and cargo to combatant, amphibious, and logistic ships. Testing could not demonstrate transfer of fuel and cargo to all ship classes within the IOT&E test design due to customer ship unavailability during test execution, as well as limited T-AO 206 crew manning that could not support one test event; however, data collected were adequate to assess 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 class 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 provided a Total Ship Survivability Trial (TSST) Report in FY24. 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 2023. The findings can be found in DOT&E's classified combined IOT&E and LFT&E report published in May 2025.

The Navy issued the Final Survivability Assessment Report (FSAR) for T-AO 205 in December 2024. The FSAR is a compilation report that details the findings from all T-AO 205 LFT&E tests and analyses over the course of the program, including TSST and predictions from M&S. The details of the FSAR can be found in DOT&E's classified combined IOT&E and LFT&E report published in May 2025. As identified above, the M&S tool could not be fully accredited for its use in LFT&E analysis, but cumulatively the FSAR, TSST, and associated testing were adequate to assess survivability.

PERFORMANCE

» EFFECTIVENESS

The T-AO 205 *John Lewis*-class of fleet replenishment oilers is operationally effective for the logistics mission of conducting connected replenishment and vertical replenishment of all customer ships available during the testing. The class is also effective for supporting the mobility mission. However, ship manning at the time of the test was not sufficient to evaluate the most stressing operation of refueling at design capacity of the T-AO 205 class. Additionally, astern refueling was unable to be accomplished within the duration of the test due to unavailability of a receiving ship. Details can be found in DOT&E's classified combined IOT&E and LFT&E report published in May 2025.

» SUITABILITY

The T-AO 205 *John Lewis*-class of fleet replenishment oilers is operationally suitable for the logistics mission of conducting connected replenishment and vertical replenishment of all customer ships available during the testing. The class demonstrated sufficient reliability. Details can be found in DOT&E's classified combined IOT&E and LFT&E report published in May 2025.

» SURVIVABILITY

DOT&E's survivability assessment, including resolution of LFT&E critical issues for the T-AO 205 class and recommendations for potential design improvements for ship survivability against threat weapons, and cyber survivability findings can be found in DOT&E's classified combined IOT&E and LFT&E report published in May 2025.

RECOMMENDATIONS

The Navy and Military Sealift Command should:

1. Validate, when manning supports, the capability to demonstrate the most stressing operations of the T-AO 205 class.
2. Demonstrate astern refueling.
3. Address the recommendations in DOT&E's classified combined IOT&E and LFT&E report published in May 2025.

Tomahawk Weapon System (TWS)

In FY25, the Navy conducted operational testing of the Maritime Strike Tomahawk (MST) as part of a quick reaction assessment (QRA). In March 2025, DOT&E published a classified Tomahawk Weapon System (TWS) FOT&E report using FY24 data from operational testing of upgrades to the Theater Mission Planning Center (TMPC) and Tactical Tomahawk Weapon Control System (TTWCS). Due to hardware issues, the Navy did not conduct the anticipated LFT&E of the Joint Multi-Effects Warhead System (JMEWS) in FY25 but plans to resume testing in FY26.

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 Navy intends for the MST, currently in development, to integrate a maritime seeker into a Block V AUR, designated variant Va. The JMEWS integrates a new multistage, 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 against enemy ships.

PROGRAM

The TWS is an Acquisition Category (ACAT) IC program. The Block V AUR variant completed operational testing in 2021, and findings are detailed in DOT&E's October 2021 classified TWS FOT&E report. In May 2023, DOT&E approved Revision I of the TWS TEMP to evaluate hardware and software modifications to the TTWCS (TTWCS v5.6.1) and the TMPC (TMPC 6.0.2/7.0.X).

The Navy transitioned the MST from a rapid fielding 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 yet to develop program requirements for MST or provide to DOT&E for approval a TEMP update that includes an evaluation of MST.

The JMEWS, an ACAT III program, is scheduled for a Milestone C decision in 2QFY27. Operational testing of JMEWS employed from TTWCS 7.0 and TMPC 8.0 is planned for FY28. DOT&E approved the JMEWS LFT&E Strategy in January 2021 with testing planned through FY28.

» 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 March 2025, DOT&E released a classified TWS FOT&E report based on FY24 data from operational testing of upgrades to the TMPC and TTWCS. Test data are adequate for regression evaluation of the legacy system capabilities and cyber survivability.

In 4QFY25, the Navy conducted a QRA of MST. The Navy is finishing their report, and DOT&E will publish a report on the results of the test. The Navy 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 did not complete any of the LFT&E activity specified in the JMEWS and MST LFT&E Strategies during FY25. While the Navy successfully executed two sled tests with the JMEWS warhead in FY21 and FY24 and used arena test data and modeling and simulation assessments to evaluate lethality against JMEWS target sets, the multi-layer target sled test, scheduled to occur in FY25 to provide additional lethality data, was postponed due to hardware availability issues. The Navy intends to conduct the delayed target sled test in FY26 and is working with DOT&E to define the target configuration. Additionally, the Navy has not resourced LFT&E events to collect data for MST against representative maritime targets.

PERFORMANCE

» EFFECTIVENESS

The operational effectiveness assessment of the TTWCS and TMPC upgrades are included in the classified March 2025 TWS FOT&E report. Insufficient data are available to provide an operational effectiveness assessment of JMEWS or MST.

» LETHALITY

TTWCS and TMPC upgrades do not change AUR lethality.

Insufficient data are yet available to determine MST lethality. LFT&E data from surrogate tests against representative maritime panels suggest that MST will fuze as designed when employed against ship targets. Additional data from lethality modeling and simulation are required to determine MST lethality against threat-representative ships.

Insufficient data are yet available to determine JMEWS lethality. Additional data from the remaining sled test are required to fully characterize the warhead and support lethality assessment against representative targets.

» SUITABILITY

The suitability assessment of the TTWCS and TMPC upgrades are included in the classified March 2025 TWS FOT&E report. Insufficient data are available to provide a suitability assessment of JMEWS or MST.

» SURVIVABILITY

The cyber survivability assessment of the TTWCS and TMPC upgrades is included in the classified March 2025 TWS FOT&E report. No data are yet available to determine cyber survivability of JMEWS or MST.

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 against threat representative targets and improve weaponeering tools.

VH-92A® Patriot® Presidential Helicopter

The Navy continues to address recommendations from DOT&E's January 2023 FOT&E report and classified annex. DOT&E will retain the VH-92A program on oversight in anticipation of projected subsystem modifications to the rotors, engine, and the Mission Communications System (MCS).

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 Patriot 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 with a classified annex, based upon FOT&E completed in 4QFY22, that assessed operational effectiveness, suitability and cyber survivability, and verified the correction of deficiencies identified during IOT&E conducted in FY21.

The program's roadmap has funded MCS modernization planned through FY30. The Navy intends to conduct an additional FOT&E to assess these future MCS capability improvements, beginning in FY26. 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

Following DOT&E-observed developmental testing of MCS version 4.0 in October 2024 and January 2025, the program office identified an opportunity to accelerate towards a comprehensive upgrade. In February 2025, the Navy decided to consolidate the validated improvements from MCS 4.0 directly into the forthcoming MCS 5.0 release. DOT&E plans to observe a combined assessment in 4QFY26 of an integrated proliferated low earth orbit satellite communications system.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E has no changes to its assessment in the FY24 Annual Report. DOT&E will evaluate the operational effectiveness, suitability, and survivability of the next build – MCS 5.0 – during a future phase of FOT&E.

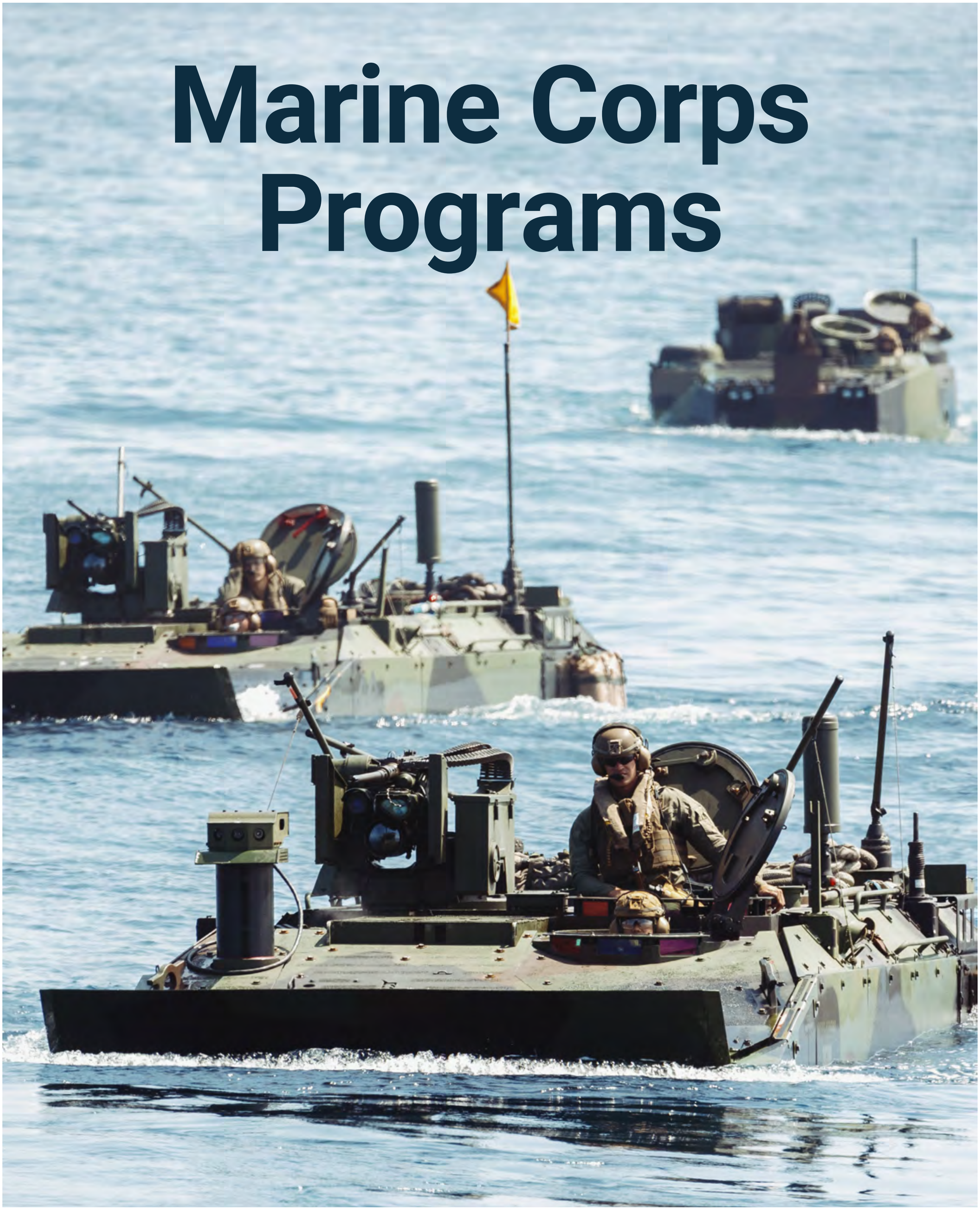
DOT&E will continue to monitor the program as projected modifications are made to the MCS, rotor system, and operations manuals.

RECOMMENDATIONS

As recommended in prior Annual Reports, the Navy should:

1. Continue to address the recommendations in the September 2021 IOT&E and January 2023 FOT&E reports and classified annexes.
2. Submit an updated TEMP for DOT&E approval to support future MCS capability upgrades.
3. Plan and conduct a comprehensive FOT&E to formally assess the operational effectiveness and suitability of all new capabilities in a representative environment.

Marine Corps Programs



This page intentionally left blank.

Amphibious Combat Vehicle (ACV) Family of Vehicles (FoV)

In May 2025, the Amphibious Combat Vehicle (ACV) Family of Vehicles (FoV) program completed all operational, live fire, and cyber testing for the ACV 30mm cannon (ACV-30) variant. DOT&E found testing to be adequate and will publish a classified FOT&E report in 1QFY26. The ACV – Maintenance and Recovery (ACV-R) variant will begin live fire testing in 1QFY26. The operational test for the ACV-R is currently scheduled in FY27.

SYSTEM DESCRIPTION

The ACV FoV program consists of four variants: Personnel (ACV-P), Command and Control (ACV-C), ACV-R, and ACV-30. This year's article focuses on ACV-30 and ACV-R.

The ACV-30 variant shares a common powertrain, drivetrain, water propulsion system, navigation and communication, and survivability features as the ACV-P. The ACV-30 upper hull is modified from the ACV-P to accommodate a remotely operated turret equipped with a stabilized, dual feed, medium caliber weapon system and coaxial medium machine gun. The ACV-30 carries two days of supply (food, water, and ammo), up to 300 rounds for the cannon, and a maximum of 800 rounds for the machine gun. The ACV-30 carries up to eight embarked marines in addition to the three-marine crew (driver, gunner, and vehicle commander). The vehicle is equipped with independent thermal and visible-light sighting systems for both the gunner and vehicle commander, in addition to the driver's enhanced vision system. The ACV-30 is present within ACV-equipped company formations in a density of six per company.

The ACV-R also shares a common powertrain, drivetrain, water propulsion system, navigation and communication, and survivability features as the ACV-P. The ACV-R payload features include an internal hydraulic winch for recovery and an external crane to assist with engine pack removal. The ACV-R has a crew of two (driver and vehicle commander) and carries two maintainers. A ring-mounted M240 Medium Machine Gun (MMG) is provided for self-defense.

MISSION

The overall ACV-equipped amphibious assault (AA) company will provide tactical lift for a reinforced Marine Corps infantry company, from amphibious ships to inland objectives. The ACV-30 carries a medium caliber weapon system capable of supporting dismounted maneuvers while still embarking marines. The ACV-30 is present within ACV-equipped company formations in a density of six per company. The ACV-30 medium caliber weapon system is optimized towards infantry support, with sufficient lethality to destroy adversary vehicles.

The ACV-R is an armored amphibious wheeled vehicle that provides field maintenance, recovery, and limited repair capabilities to the AA battalion. The ACV-R is designed to recover similar or smaller sized vehicles and also carries basic maintenance equipment to provide field support maintenance to vehicles in the field. The ACV-R is organic to the AA company and battalion. The maintenance platoon operates and maintains the battalion's ACV-Rs.

PROGRAM

The ACV FoV is an Acquisition Category IC program. DOT&E reported on the ACV-P in November 2020 and the ACV-C in June 2022. The Navy signed the full-rate production decision for the ACV-P in December 2020 and authorized all production for future variants after briefing the Assistant Secretary of the Navy for Research, Development, and Acquisition. The ACV-30 is an engineering change proposal for the ACV-P and completed live fire testing in December 2024 and operational testing in May 2025. The Marine Corps awarded production contracts for the ACV-30 base vehicle in March 2025 and for the turret in August 2025. Initial operational capability for the ACV-30 is planned for 2QFY26. The program has planned live fire and operational testing for the ACV-R in FY26 and FY27, to inform a full-rate production decision in 4QFY27.

» MAJOR CONTRACTORS

- Kongsberg Defense & Aerospace – Kongsberg, Norway
- BAE Systems, Inc. – Sterling Heights, Michigan

TEST ADEQUACY

ACV-30 testing was adequate to support the evaluation of operational effectiveness, suitability, and survivability. The Marine Corps Operational Test and Evaluation Activity (MCOTEA) conducted a cooperative cyber assessment in June 2024, and an FOT&E from February – April 2025 at Aberdeen Test Center, Maryland, and Camp Pendleton, California, and a cyber adversarial assessment in May 2025, at Camp Pendleton, California. MCOTEA conducted multiple ACV-30 live fire tests at the Aberdeen Test Center, Maryland, from March 2024 through December 2024. All testing was conducted in accordance with DOT&E-approved test plans, and DOT&E observed the tests.

ACV-R live fire and operational testing is currently scheduled to occur in FY26 and FY27, in accordance with DOT&E-approved test plans. DOT&E will assess that variant's operational effectiveness, suitability, and survivability following completion of the testing.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY, AND SURVIVABILITY

DOT&E will publish a classified combined FOT&E and LFT&E report in 1QFY26 to assess the operational effectiveness, suitability, and survivability of the ACV-30. The assessment will use ACV-30 test data from, operational, live fire, and cyber testing. Additionally, DOT&E will leverage some data from prior ACV-P testing.

RECOMMENDATION

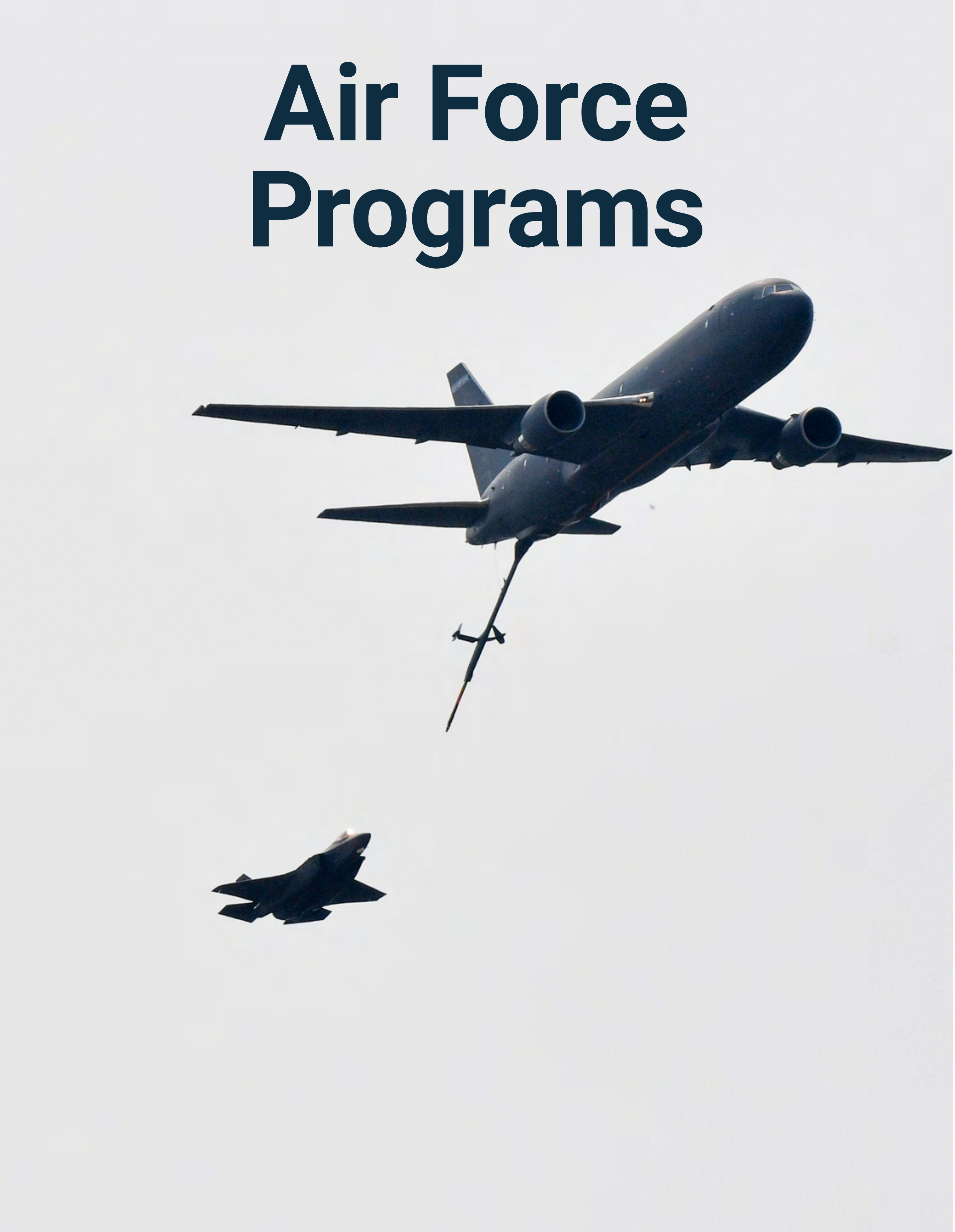
The Marine Corps should:

1. Submit a T&E Strategy update to DOT&E for approval, outlining the scope and timeline for testing of the ACV-R.

DEPARTMENT OF THE AIR FORCE PROGRAMS

This page intentionally left blank.

Air Force Programs



This page intentionally left blank.

Advanced Battle Management System (ABMS)

The Cloud-Based Command and Control (CBC2) is the only Advanced Battle Management System (ABMS) component to conduct operational testing (OT) in FY25. The Air Force has tested quarterly CBC2 minimum viable capability releases (MVCRs) since June 2023, and in September 2025, the Air Force completed the CBC2 Operational Assessment (OA), which had been delayed from 4QFY24 due to software immaturity, as stated in the FY24 Annual Report. DOT&E will publish an OA report in 2QFY26, once data analysis is complete.

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 and Space Force systems to share data that will enable faster C2 decision making. The portfolio is comprised of multiple programs and lines of effort including: CBC2, Digital Infrastructure (DI), Distributable Battle Management Node (DBMN), and Aerial Connectivity (AC), formerly referred to as Aerial Networking (AN).

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 four U.S. and one Canadian Air Defense Sectors with modern cloud-based applications to create a single fused C2 air picture and automated decision aids.

MISSION

DoW military commanders will use ABMS to get a real-time, complete picture of the battlespace so they can quickly make informed decisions, direct action, and monitor execution of operations. ABMS is the Department of the Air Force (DAF) contribution to Combined Joint All Domain Command and Control.

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 component of ABMS is a separate acquisition program. CBC2, a software acquisition pathway program, is the only component to conduct OT in FY25. The other ABMS component programs are Middle Tier of Acquisition rapid prototyping programs. DOT&E approved the CBC2 T&E Strategy in August 2024, the AC T&E Strategy in February 2025, and the DBMN Tactical Operations Center – Light (TOC-L) T&E Strategy in August 2025. The Air Force will conduct T&E of ABMS DI in conjunction with other ABMS systems and capabilities.

» MAJOR CONTRACTORS

- Science Applications International Corporation – Rosslyn, Virginia
- Booz Allen Hamilton – McLean, Virginia
- Leidos – Herndon, Virginia

TEST ADEQUACY

DOT&E approved the DBMN TOC-L T&E Strategy in August 2025 with two test caveats that require further cyber testing and software integration detail as part of the TOC-L OA test plan.

The Air Force has tested eight CBC2 MVCRs since June 2023. Even though the first eight MVCRs were developmental test and evaluation (DT&E) events, the Air Force made significant efforts to ensure early OT involvement in CBC2. The Air Force Operational Test and Evaluation Center (AFOTEC) Detachment 2 observed all MVCRs and was a key stakeholder in all CBC2 DT&E events and processes.

In September 2025, AFOTEC Detachment 2 performed an OA during the ninth MVCR, in accordance with the DOT&E-approved OA test plan. DOT&E also observed the OA. The objective of the OA was to inform the North American Aerospace Defense (NORAD) Command and U.S. Northern Command operations acceptance decision in 1QFY26, and to inform the Air Force on CBC2 progress towards readiness for IOT&E. Testing was adequate for those purposes. The Air Force had delayed the OA from 4QFY24, when it was originally scheduled, due to software immaturity, as stated in the FY24 Annual Report.

AFOTEC Detachment 2 also observed a developmental test of AC on a prototype palletized airborne edge node aboard a KC-46A tanker in the EMERALD FLAG 24-3 exercise and published an observation report.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E will provide an assessment of CBC2's operational effectiveness, suitability, and survivability in an CBC2 OA report in 2QFY26, once data analysis is complete.

RECOMMENDATIONS

The Air Force should:

1. Continue to develop T&E Strategies for all future ABMS components.
2. Submit as part of the DBMN TOC-L OA test plan a detailed list of cyber test limitations, mitigations, and testing resources.
3. Clarify which software versions TOC-L will integrate and test in Phase 2, and provide a description, test dates, and resources for the software integration and testing effort.

AGM-183A Air-Launched Rapid Response Weapon (ARRW)

In FY25, the Air Force's AGM-183A Air-Launched Rapid Response Weapon (ARRW) program conducted lethality data analyses from flight tests that were accomplished in FY24, which concluded the rapid prototyping Increment 1 program. The Air Force utilized the results of the ARRW Increment 1 program to inform decisions regarding potential procurement as well as potential further developmental areas to deliver improved warfighter capability. In July 2025, DOT&E removed ARRW from oversight, as the program has completed Increment 1 of rapid prototyping T&E.

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 OVERSIGHT HISTORY

ARRW used 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. DOT&E placed the ARRW program on oversight for operational and live fire testing in

July 2018. The program completed its Critical Design Review in February 2020. In FY21 – 22, the Air Force conducted a series of booster test flights, followed by a series of All Up Round (AUR) (including live warhead) test flights (ATFs) from FY22 – 24. In August 2023, DOT&E approved the ARRW Integrated Master Test Plan, and in February 2024, DOT&E approved the Ops Demo test plan. The Air Force used the ATF results to inform the way ahead for the technologies developed in the ARRW program. In July 2025, DOT&E removed ARRW from oversight, as the program has completed Increment 1 of rapid prototyping T&E.

AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM)

The Advanced Medium-Range Air-to-Air Missile (AMRAAM) AIM-120D0 System Improvement Program (SIP)-3 Tape 2 began FOT&E in September 2025, and testing is scheduled to complete in 2QFY26. The AIM-120D3 SIP-4 will execute FOT&E in FY26. DOT&E plans to publish a classified SIP-3 Tape 2 FOT&E report in 3QFY26 and a classified SIP-4 FOT&E report in 1QFY27, when data analyses are complete. The reports will inform fielding decisions of the SIP-3 Tape 2 and SIP-4 software upgrades.

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 for 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, starting with SIP-4, 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. SIP-3 Tape 2 is the first of these updates that 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 report in January 2024, and SIP-3F fielded in March 2024.

The Services are now testing the next set of updates for AIM-120D0 and AIM-120D3 to enhance missile performance and resolve deficiencies. DOT&E approved the operational test plan for SIP-3 Tape 2 in September 2025. DOT&E approved the SIP-4 TEMP in February 2025 and the SIP-4 FOT&E test plan in October 2025.

The 53rd Wing is the Operational Test Organization for SIP-3 Tape 2 OT&E, and the Air Force Operational Test and Evaluation Center is the Operational Test Agency for SIP-4 FOT&E.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX – Tucson, Arizona

TEST ADEQUACY

AIM-120D0 SIP-3 Tape 2 FOT&E began in September 2025 and is expected to be completed in 2QFY26, in accordance with the DOT&E-approved test plan. The AIM-120D3 SIP-4 FOT&E is expected to be completed in FY26. DOT&E will publish classified reports assessing test adequacy and missile performance after completing data analysis.

A cyber self-assessment on both SIP-3 Tape 2 and SIP-4 was completed in August 2025, with a cyber tabletop planned in 1QFY26. DOT&E will assess the cyber survivability of SIP-3 Tape 2 and SIP-4 using data from these events, which are informed by previous AIM-120D results and a review of current threats.

The availability of threat surrogates for testing remains a challenge when assessing missile effectiveness and lethality. Upcoming FOT&E testing may include limited full-scale targets due to test asset availability limitations. Additionally, surrogates for many other modern threats do not currently exist, nor are they programmed to deliver in the future. These test asset limitations put greater importance on modeling and simulation to adequately characterize the performance of the AIM-120D. However, verification, validation, and accreditation of modeling and simulation is problematic due to the lack of relevant data from flight testing against representative targets. The Services should fund, develop, and produce modern aerial targets, such as fourth- and fifth-generation fighter and large aircraft.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, AND SUITABILITY

There are insufficient data at this time to assess the operational effectiveness, lethality, and suitability of SIP-3 Tape 2, as FOT&E is ongoing. These assessments will be provided in the classified SIP-3 Tape 2 FOT&E report in 3QFY26.

There are insufficient data at this time to assess the operational effectiveness, lethality, and suitability of SIP-4, as the FOT&E is planned for FY26. These assessments will be provided in the classified SIP-4 FOT&E report in 1QFY27.

» SURVIVABILITY

Analysis of the cyber survivability data is ongoing. Assessment of SIP-3 Tape 2 and SIP-4 cyber survivability will be provided in classified DOT&E test reports for each program once data analysis is complete.

RECOMMENDATION

The Air Force and Navy should:

1. Fund, develop, and produce modern aerial targets, such as fourth- and fifth-generation fighter and large aircraft. 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 level.

Air Operations Center – Weapon System (AOC-WS)

In February 2025, the Air Force conducted a cooperative vulnerability and penetration assessment (CVPA) of the Air Operations Center – Weapon System (AOC-WS) Increment 10.1. DOT&E published a classified report on the cyber vulnerability findings in July 2025. The Air Force has not conducted 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. DOT&E published an early fielding report (EFR) on AOC-WS Block 20 in May 2025, documenting risk and testing concerns with associated recommendations.

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:

- AOC-WS Increment 10.1 (AN/USQ-163 Falconer) is the currently fielded baseline system for AOCs.
- 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 transition 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. Simultaneously, the program office is working to fully integrate C2Core Air, a vendor-provided suite of applications intended to perform many of the AOC core warfighting functions, into the AOC-WS Increment 10.1 baseline to support testing and enterprise-wide deployment in FY26 as an interim capability solution prior to full fielding and employment of AOC-WS Block 20. As the Air Force develops more AOC-WS 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 or completely replace AOC-WS Increment 10.1 capabilities with AOC-WS 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

In October 2021, the Assistant Secretary of the Air Force for Acquisition, Technology and Logistics designated both AOC-WS Increment 10.1 and AOC-WS Block 20 as software acquisition pathway programs, merged them, and authorized them to enter the execution phase of development. AOC-WS Increment 10.1 has a DOT&E-approved overarching test plan, and the Air Force submitted a T&E Strategy for the merged AOC-WS Increment 10.1 and AOC-WS Block 20 program, which DOT&E approved in September 2025.

The program office continues to deliver incremental capability updates and software revisions to AOC-WS Increment 10.1 via periodic Agile Release Events (AREs). The Air Force delivered and fielded AREs 24-09 and 25-05 in FY25 and intends to deliver ARE 25-10 in 2QFY26.

AOC-WS Block 20 capabilities are developed and fielded at numerous sites, following Agile software development and continuous integration and deployment principles.

» MAJOR CONTRACTORS

- RTX – Dulles, Virginia
- Science Applications International Corporation, Inc. – Reston, Virginia
- Parsons Corporation – Chantilly, Virginia

TEST ADEQUACY

The Air Force is conducting planned AOC-WS Increment 10.1 system upgrades via AREs and testing them in accordance with the DOT&E-approved overarching test plan. DOT&E monitors the releases, observes the testing, and reports on significant capability releases. In FY25, the Air Force conducted integrated tests on AREs 24-09 and 25-05 in accordance with DOT&E-approved test plans. The integrated test of ARE 24-09, which began in October 2024 and was completed in April 2025, required additional testing of both functionality and deployability at a geographic AOC because of the complexity of the software content and installation. ARE 25-05 testing occurred in May 2025, completing on schedule with no notable test execution issues. ARE 25-10 testing is scheduled to begin in 2QFY26 and will include testing for C2Core Air as a part of the AOC-WS Increment 10.1 baseline, as well as AppTX capabilities.

The Air Force conducted a CVPA at a geographic AOC in February 2025, in accordance with the DOT&E-approved test plan. The CVPA was adequate to identify cyber vulnerabilities of the AOC-WS Increment 10.1. Although AOC-WS Block 20 software and hardware were present at the CVPA site, and at the CVPA and adversarial assessment test site in FY24, operational constraints, system administration decisions, and inadequate program office support prevented the test team from being able to collect usable data needed to identify potential AOC-WS Block 20 vulnerabilities. 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. DOT&E published a classified report on the CVPA results in July 2025. The Air Force intends to conduct a CVPA and AA at another geographic AOC in FY26.

The Air Force did not conduct operational testing of AOC-WS

Block 20 or the AOC-WS Block 20 software supply chain in FY25. AOC-WS Block 20 capabilities continue to be deployed incrementally through an Agile release capabilities model. The Air Force delayed the start of the planned OT&E of AOC-WS Block 20 from late 1QFY26 to 2QFY26, due to system maturity. DOT&E published an EFR on AOC-WS Block 20 in May 2025, documenting risk and testing concerns with associated recommendations. In FY25, the Air Force conducted a mission-based cyber risk assessment as well as a test design and measures review event, to support eventual cyber OT&E of AOC-WS Block 20 and the hybrid weapon system.

PERFORMANCE

» EFFECTIVENESS

The Air Force found that AOC-WS Increment 10.1 ARE 24-09 was operationally effective with limitations and assessed ARE 25-05 as operationally effective. Since the Air Force has not conducted operational effectiveness testing of AOC-WS Block 20, there are insufficient data for DOT&E to comment on its effectiveness.

» SUITABILITY

The Air Force found that AOC-WS Increment 10.1 ARE 24-09 was not suitable and assessed ARE 25-05 as operationally suitable. Since the Air Force has not conducted operational suitability testing of AOC-WS Block 20, there are insufficient data for DOT&E to comment on its suitability.

» SURVIVABILITY

The most recent DOT&E 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. DOT&E documented additional cyber vulnerability findings in the July 2025 classified CVPA test report.

RECOMMENDATIONS

The Air Force should:

1. Continue to address all recommendations in DOT&E's September 2024, May 2025, and July 2025 reports.
2. Provide an updated AOC-WS Block 20 acquisition strategy with product roadmaps that identify when capabilities under development are expected to be sufficiently mature for operational testing, as recommended in the FY22 – 24 Annual Reports.
3. Conduct a cyber survivability assessment of the AOC-WS Block 20 software supply chain, to include the unclassified development environment and distribution environments, and to adequately inform subsequent OT&E, as recommended in the FY22 – 24 Annual Reports and in the May 2025 AOC-WS Block 20 EFR.
4. Complete an annual CVPA and an AA at a fielded AOC, which has both AOC-WS Increment 10.1 and AOC-WS Block 20 capabilities present, to characterize the cyber vulnerabilities of the hybrid weapon system, as recommended in the FY24 Annual Report and in the May 2025 AOC-WS Block 20 EFR.
5. Implement a solution to meet the long-standing requirement to collect and report stability, reliability, availability, and maintainability data for the AOC-WS, as recommended in the FY22 – 24 Annual Reports.

B-52 Radar Modernization Program (RMP)

In spring 2025, the Air Force notified Congress of a significant Nunn-McCurdy cost breach in the B-52 Radar Modernization Program (RMP), due to ongoing technical integration challenges. To address cost growth, the Air Force is restructuring the program around a minimum viable product (MVP) approach, which will deliver basic radar functionality first and defer other new capabilities to future upgrades. This restructuring will require updates to the program's T&E Strategy.

SYSTEM DESCRIPTION

The B-52 RMP will replace the legacy AN/APQ-166 radar with the AN/APQ-188 Bomber Modernized Radar System. 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.

Following its Critical Design Review in February 2022, the program has continued to face significant technical challenges including integrating the new radar onto the B-52 aircraft. These challenges led to cost growth that triggered a significant Nunn-McCurdy breach in spring 2025.

As a result, the Air Force is revising the acquisition strategy to focus on delivering an MVP to control costs. This MVP will include a subset of the capabilities originally documented in the MS B Capability Development Document, with other functionalities deferred to future increments, including the new wideband nose radome. Modification of test aircraft and development of initial flight software, which began in FY23, is ongoing. The MVP will utilize the legacy radome in place of developing a new radome. The Air force will need to characterize the capability of the new radar with the legacy radome. Developmental and integrated flight testing is scheduled to begin in FY26, with a MS C decision planned for 4QFY26. A full-rate production decision for the remaining aircraft will follow IOT&E in FY28.

DOT&E approved the B-52 Cybersecurity T&E Strategy in September 2023. This strategy defines a comprehensive, integrated cybersecurity test approach across all planned modernization programs, including the Commercial Engine Replacement Program, the RMP, multiple communication system upgrades, and system sustainment programs.

» MAJOR CONTRACTORS

- The Boeing Company – Oklahoma City, Oklahoma
- Raytheon, a subsidiary of RTX – El Segundo, California

TEST ADEQUACY

The DOT&E-approved April 2021 TEMP no longer aligns with the restructured program due to the Nunn-McCurdy breach and subsequent shift to an MVP strategy. An update to the TEMP is required, prior to the MS C decision in 4QFY26, for the reduced capability set to define the test scope for the MVP, establish new performance metrics, and realign the integrated test schedule. The B-52 Cybersecurity T&E Strategy defines an adequate cybersecurity test approach across all B-52 modernization programs, but it will require an RMP-specific update prior to the 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 assess the operational effectiveness, suitability, and survivability of the B-52 RMP following IOT&E in FY28.

RECOMMENDATIONS

The Air Force should:

1. Update the B-52 RMP TEMP prior to the MS C decision to align with the new MVP strategy, to include revised test objectives and success criteria for the reduced capability set.
2. Characterize radar performance with the legacy radome design to inform operational employment tactics, as recommended in the FY24 Annual Report.
3. Develop and submit for DOT&E approval an RMP-specific Cybersecurity T&E Strategy prior to the program's MS C decision, as recommended in the FY24 Annual Report.

B-52J Commercial Engine Replacement Program (CERP)

Following its transition from the Middle Tier of Acquisition rapid prototyping pathway to the major capability acquisition pathway in December 2023, the B-52J Commercial Engine Replacement Program (CERP) is now undergoing subsystem laboratory and platform integration testing. The program's Milestone B (MS B) TEMP, which will guide T&E through the current phase of development, is pending final approval.

SYSTEM DESCRIPTION

The B-52J CERP is the final phase of a multi-year, multi-program modernization effort that will produce the B-52J aircraft configuration. The 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-52J 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 Middle Tier of Acquisition rapid prototyping efforts with delivery of Virtual System Prototype digital models in FY23. The program is currently testing the different engine subsystems, which will inform the system's Critical Design Review (CDR) in FY26. This phase of testing will include various subsystem tests and creation of subsystem laboratories. Prior to the MS C decision point, the current phase of testing will end with the modification of two low-rate initial production (LRIP) aircraft for use in testing.

At the direction of the Air Force Acquisition Executive, the program transitioned to the major capability acquisition pathway in December 2023. The acquisition strategy extends system development until FY33. The program schedule includes a system-level CDR in FY26, followed by the modification of the two LRIP aircraft in FY27 for testing. Developmental and integrated flight testing is scheduled to begin in FY29, leading to IOT&E in FY32. The proposed production program would award LRIP contracts to procure engines and modify 51 of the 74 B-52 fleet aircraft (69 percent) prior to the planned completion of IOT&E in FY32. IOT&E will be conducted using the two fully modernized B-52J LRIP aircraft. Two full-rate production decisions, planned for FY33 and FY34, will address the remaining 23 aircraft.

Integration of new engines on a legacy aircraft is a major design change. B-52J commercial engine integration will require extensive flight testing 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 weapons.

The Air Force acquisition strategy implements a highly concurrent flight test and production program, awarding LRIP contracts for 69 percent of fleet aircraft prior to IOT&E. Contracts for the first two LRIP lots, totaling 17 aircraft, would be awarded prior to the start of the flight test program. Two additional LRIP contracts for 34 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. The Air Force's 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 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 approved the B-52 Cybersecurity T&E Strategy in September 2023. The strategy defines a comprehensive, integrated cybersecurity test approach across all planned modernization programs, including CERP, radar modernization, multiple communication system upgrades, and system sustainment programs. Prior to the MS C decision in FY29, DOT&E requires both an updated TEMP and a CERP-specific update to the B-52 Cybersecurity T&E Strategy.

» MAJOR CONTRACTORS

- The Boeing Company – Oklahoma City, Oklahoma
- Rolls-Royce North America – Indianapolis, Indiana

TEST ADEQUACY

DOT&E is awaiting the approved MS B TEMP, which should define an adequate operational test strategy for the modernized B-52J CERP aircraft configuration. The program will update the TEMP prior to MS C in FY29 to prepare for ground and flight testing starting at the end of FY29. The DOT&E-approved B-52 Cybersecurity T&E Strategy 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 the 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. Ensure that the subsystem component-level testing is complete prior to the CDR in FY26 and LRIP test aircraft modification in FY27.
2. Develop and submit for DOT&E approval a CERP-specific update to the Cybersecurity T&E Strategy prior to the program's MS C decision.
3. Continue to 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 and FY24 Annual Reports.

Defense Enterprise Accounting and Management System (DEAMS)

Since FY15, DOT&E has evaluated the evolving Defense Enterprise Accounting and Management System (DEAMS) program through multiple test events. DEAMS is a deployed system for which the program management office (PMO) continues to provide updates by implementing the Scaled Agile Framework (SAFe®) to develop and deliver software. In July 2025, DOT&E removed the DEAMS program from oversight because all testing and associated reporting to inform formal acquisition decisions is complete.

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 of financial system management: general ledger management, funds management, payment management, receivable management, cost management, and reporting.

Air Force financial managers and tenant organizations use DEAMS across the Air Force, the

Space Force, and their supported combatant and field commands to compile and share accurate, up-to-the-minute financial management data and information; and satisfy congressional and DoW requirements for auditing of funds, standardizing of financial ledgers, timely reporting, and reduction of costly rework.

PROGRAM OVERSIGHT HISTORY

DEAMS is a Business Acquisition Category I program of record that has been on DOT&E oversight for operational testing since 2004. In FY15, Air Force Operational Test and Evaluation Center (AFOTEC) conducted an IOT&E of DEAMS Increment 1. In August 2015, DOT&E published a DEAMS Increment 1 Release 3 (R3) IOT&E report with a classified annex. DOT&E determined from that testing that DEAMS Increment 1 was not operationally effective, suitable, or cyber survivable. The verification of fixes test conducted in FY16 demonstrated that DEAMS Increment 1 remained neither operationally effective nor suitable.

From the operational utility evaluation (OUE) AFOTEC conducted in FY17 – 18, DOT&E determined that DEAMS Increment 1 improvements had made it operationally effective and suitable, but it was still not cyber survivable. The OUE showed that DEAMS could support financial operations and meet all key performance parameters. Additionally, all accounts were correctly reconciled at the end of the accounting periods that DOT&E observed.

In FY20, the DEAMS PMO released an Oracle R12 software upgrade to users worldwide. Following deployment of the Oracle R12 software, operational users reported numerous major deficiencies that reduced the system's operational effectiveness and suitability. DOT&E issued an early fielding report in July 2020, recommending the Air Force delay the full deployment decision until these major deficiencies had been resolved.

The DEAMS PMO has since adopted the SAFe® to facilitate software development. DEAMS was designated an Agile Software Development Pilot Program in the FY19 NDAA. The PMO has developed an integrated test environment to support development and deployment cycles, though the Air Force should continue to work to verify, validate, and accredit this environment to better understand its realism.

In July 2025, DOT&E removed the DEAMS program from oversight because all testing and associated reporting to inform formal acquisition decisions is complete. DOT&E recommends that the Air Force continue conducting operationally realistic testing for DEAMS, including cyber survivability testing, to reduce risk when fielding upgraded capabilities.

Deliberate and Crisis Action Planning and Execution System (DCAPES) Increment 2B

The Air Force Operational Test and Evaluation Center (AFOTEC) conducted the Deliberate and Crisis Action Planning and Execution System (DCAPES) Increment 2B IOT&E from February to September 2024 but deviated from the DOT&E-approved IOT&E test plan by not collecting the needed data required to support DOT&E's evaluation of operational effectiveness, suitability, or cyber survivability.

Following the IOT&E, in December 2024, the Air Force approved the full deployment decision and DCAPE's subsequent transition to the software acquisition pathway (SWP). The DCAPES program management office (PMO) selected the Joint Interoperability Test Command (JITC) to replace AFOTEC as the DCAPES operational test organization (OTO) for the SWP execution phase.

In July 2025, DOT&E removed DCAPES from oversight. The program is releasing quarterly software improvements with stable development and no major planned upgrades.

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 predefined 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 OVERSIGHT HISTORY

DCAPES Increment 2B is an Acquisition Category IAC program that has been on DOT&E oversight since October 2015. The Air Force Service Acquisition Executive delegated the decision authority and source selection authority to Program Executive Officer for Business and Enterprise Systems in September 2023.

AFOTEC conducted the IOT&E of DCAPES Increment 2B from February to September 2024, to assess its operational effectiveness, suitability, and cyber survivability. AFOTEC deviated from the IOT&E test plan approved by DOT&E. Data collection was limited to surveys. AFOTEC did not administer the surveys to a representative sample of the operational users and mission owners. AFOTEC did not collect the data as described in the DOT&E test plan approval caveats. Therefore, the IOT&E test data were not adequate for DOT&E to provide an assessment of DCAPES' operational effectiveness, suitability, and cyber survivability.

In December 2024, the Air Force approved DCAPES's full deployment decision, and the program subsequently transitioned to the SWP, as planned, per the Air Force's October 2023 memorandum. The DCAPES PMO selected JITC to replace AFOTEC as the OTO for the execution phase of the SWP. JITC is the OTO for Joint Planning and Execution Services (JPES) system, DCAPES's most important interface.

In July 2025, DOT&E removed DCAPES from oversight after the program transitioned to the SWP execution phase. The program makes regular modifications through quarterly software releases following developmental testing. Software development remains stable with no significant planned upgrades.

DOT&E recommends that JITC continue to assess DCAPES releases and coordinate as needed with JPES testers to ensure that the systems interoperate to support their respective users' missions.

EA-37B Compass Call Rehost

In July 2025, the Air Force completed EA-37B Compass Call IOT&E, in accordance with DOT&E-approved test plans. The Air Combat Command EA-37B full-fielding authorization decision is scheduled for 1QFY26. DOT&E is awaiting final test data from IOT&E in order to publish a classified IOT&E report in FY26 to assess EA-37B operational effectiveness, suitability, and cyber survivability.

SYSTEM DESCRIPTION

The EA-37B is a wide-area airborne electromagnetic attack weapon system utilizing a Gulfstream G550 conformal airborne early warning (CAEW) aircraft, modified to host an updated EC-130H Compass Call mission system. The EC-130H Baseline 2 prime mission equipment (PME) was redesigned to fit into the G550 airframe. The EA-37B's new PME (Baseline 3) includes obsolescence and modernization updates to the hardware and software while reducing the size, weight, and power. Baseline 3 is a software-based open architecture design with software-defined radios, which converts the previous mission software from a proprietary operating system to a modern, open-source operating system.

MISSION

Combatant commanders will use the EA-37B to amplify joint force military advantage in the electromagnetic battlespace and build a more robust combat force by employing electromagnetic attack capabilities to deny peer competitors' tactical networks and information ecosystems. The system denies, degrades, and disrupts adversary communications, information processing, navigation, radar systems, and radio-controlled threats.

The Compass Call system will employ offensive counter-information and electromagnetic attack capabilities in support of U.S. and coalition tactical air, surface, and special operations forces.

PROGRAM

The EA-37B is an Acquisition Category II program established to rehost and integrate proven EC-130H Compass Call mission systems into a derivative of the G550-based CAEW aircraft modification developed for use by allied air forces. It was added to DOT&E oversight for operational and live fire testing in September 2022 already post-Milestone C. DOT&E approved he EA-37B Compass Call Integrated Test Plan in January 2025.

Ten EA-37B aircraft will replace the Air Force's current fleet of 14 EC-130Hs: five in the Baseline 3 configuration and five in a future Baseline 4 configuration. The 55th Electronic Combat Group will continue to employ EC-130Hs into FY26 as it ramps up EA-37B training, testing, and initial operations. Five EA-37B aircraft have been delivered, with the remaining five deliveries planned through 2028. The Air Force plans to make a full-fielding decision in 1QFY26.

» MAJOR CONTRACTORS

- L3Harris Technologies, Inc. – Waco, Texas (aircraft integration)
- BAE Systems – Nashua, New Hampshire (mission system)
- Gulfstream Aerospace Corp. – Savannah, Georgia (aircraft subcontractor to L3 Harris)

TEST ADEQUACY

EA-37B integrated testing began in August 2023, and dedicated IOT&E completed in July 2025. Integrated testing consisted of 10 phases, covering 25 weeks of ground and anechoic chamber testing, and 40 weeks of flight testing. The final three test phases were the operational test events. DOT&E approved the IOT&E test plan and observed some of this testing. These events evaluated the Compass Call mission systems in operationally relevant basic conditions, to include the altitudes, ranges, and geometries that reflect realistic combat-like conditions against available threat representations. Test personnel flying the mission were Air Force pilots, electromagnetic warfare officers, and mission crews with experience in the EC-130H Compass Call mission, with many having significant combat experience. The test aircraft were the first two production aircraft equipped with the production-representative PME and flight test instrumentation. End-to-end mission testing included anechoic chamber tests and open-air flight tests, using available test resources representing Compass Call targets. Most testing occurred against systems that are considered less advanced threats; however, this is a DoW-wide limitation with available modeling and simulation, hardware-in-the loop test facilities, and open-air flight test range limitations. Testing was adequate to assess operational effectiveness, suitability, and survivability at a baseline level.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E is working with the Air Force to obtain all of the integrated and operational test data. DOT&E will publish a classified IOT&E report in FY26 to assess EA-37B operational effectiveness, suitability, and cyber survivability following completion of data analysis.

RECOMMENDATION

The Air Force should:

1. Support investments to improve the modeling and simulation, hardware-in-the-loop, anechoic chambers, and open-air flight test ranges required to test systems such as the EA-37B operating in a modern, complex electromagnetic environment representative of combat against a peer adversary.

F-15EX Eagle II

In March 2025, DOT&E published a classified live fire annex update to the November 2023 combined F-15EX Eagle II IOT&E and LFT&E report. This live fire annex cleared the way for the program to begin FOT&E, which is now underway, in accordance with a DOT&E-approved TEMP. While initial FOT&E events have occurred, those events attempted during a large force exercise in FY25 were deemed not operationally representative, precluding the use of its data.

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 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.

MISSION

Although the aircraft is multi-role capable, the Air Force intends to use the F-15EX initially in an air superiority role. Units equipped with the F-15EX will provide offensive counter-air, 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 currently in FOT&E following the full-rate production decision in June 2024. The Air Force intends to procure 129 F-15EX aircraft, training systems, and support equipment over 8 procurement lots. The arrival of aircraft at the Portland Air National Guard Base, Oregon in June 2024, marked the first delivery of the F-15EX to an operational unit. In April 2025, DOT&E approved the FOT&E TEMP and the initial FOT&E test plan. A detailed F-15EX cyber test plan for an on-aircraft cooperative vulnerability and penetration assessment (CVPA) was subsequently approved in June 2025.

» MAJOR CONTRACTORS

- Boeing Defense, Space & Security – St. Louis, Missouri
- RTX, Agile Radar Solutions – El Segundo, California
- General Electric – Cincinnati, Ohio

TEST ADEQUACY

During FOT&E in FY25, DOT&E and the Air Force Operational Test and Evaluation Center observed a large force exercise. Both organizations determined the test was not operationally relevant, precluding the use of the data for operational assessment and highlighting the need for rigorous test discipline in future events. The Air Force is making progress toward improving the maintenance technical orders, which DOT&E found to be immature during IOT&E. Air Force testers are holding focus groups with operational maintainers to correct and revise the technical orders, which is a crucial step for assessing suitability during FOT&E.

LFT&E that occurred during IOT&E was adequate and conducted in accordance with the DOT&E-approved test plan. Air Force analysts used a set of operationally relevant threats and scenarios from the F-15EX's expected roles and missions to assess platform survivability. The Air Force applied engineering analysis, modeling and simulation, and utilized prior data to assess critical LFT&E issues for susceptibility and vulnerability. The Air Force used data from the joint live fire program, prior test data from earlier F-15 models, and other relevant tactical aircraft to inform susceptibility and vulnerability assessments.

PERFORMANCE

» EFFECTIVENESS

No FOT&E testing data are available to determine operational effectiveness. DOT&E will publish a classified FOT&E report once data is received and analysis is complete.

» SUITABILITY

DOT&E will publish a classified FOT&E report determining suitability once data is received and analysis is complete.

» SURVIVABILITY

In March 2025, DOT&E published a classified live fire annex update to the November 2023 combined F-15EX Eagle II IOT&E and LFT&E report. The analysis from this live fire annex found that the legacy data used to model F-15EX ballistic vulnerabilities were incomplete for certain munitions, resulting in uncertainties of vulnerability calculations. In the November 2023 report, DOT&E previously stated that cyber testing on a production-representative Lot 2 aircraft was required. The Air Force has since shifted plans to conduct this testing on Lot 3 aircraft. A CVPA was completed on a Lot 3 aircraft in FY25, and an adversarial assessment is planned for 1QFY26.

RECOMMENDATIONS

The Air Force should:

1. Ensure the F-15EX test fleet is production-representative by modifying test aircraft to include any configuration changes that occur in future production lots, as recommended in the FY22 – 24 Annual Reports.
2. Continue to incorporate advanced, high-fidelity threat systems during ongoing F-15EX FOT&E.
3. Collect additional data for select munitions so that F-15EX vulnerabilities can be calculated with higher confidence. Specific details on the data to collect are in the classified March 2025 live fire annex update.

F-22A – Raptor Advanced Tactical Fighter Aircraft

The Air Force is modernizing the F-22A with a series of capability releases delivered once every 12 – 18 months. In February 2025, DOT&E published a classified combined early fielding and LFT&E report on the F-22A Release 3 (R3) Operational Flight Program (OFP). The Air Force completed operational testing on the R4 OFP in FY25. DOT&E plans to publish a classified FOT&E report summarizing the results of R4 testing in the first half of FY26. The lack of instrumentation in the F-22A operational test aircraft to provide high-fidelity accurate mission-level results continues to restrict the Air Force's ability to accomplish adequate mission-level evaluations. A model of Sensor Enhancement (SeE) for the Joint Simulation Environment (JSE) will be important for adequate operational effectiveness testing, but development of the model is currently unfunded.

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 Air Force is modernizing the F-22 hardware and software via the F-22 Raptor Agile Capability Release program. Capability releases take place every 12 – 18 months and are focused on sensor upgrades, data link upgrades, and survivability enhancements.

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. To modernize the fleet, the Air Force initiated hardware and software modernization efforts under the Middle Tier of Acquisition rapid prototyping pathway, eventually transitioning most of those efforts to traditional Acquisition Category programs. The R4 OFP is the current focus of F-22A FOT&E, and R5 software is in development. The Air Force intends to deliver SeE, which should significantly upgrade the capability of the F-22A, with R6.

The Tactical Link 16 and Tactical Mandates TEMP, approved by DOT&E in 2018, supported testing through the R2 Force Development Evaluation (FDE). DOT&E published a classified R2 FOT&E report in March 2024. DOT&E approved the R3 test plan and a combined R3/R4 TEMP in 4QFY23. DOT&E published a classified combined early fielding and LFT&E report on F-22A Capability R3 OFP in February 2025. DOT&E approved the R4 test plan in January 2025 and observed the R4 test events in February 2025. DOT&E will publish a classified FOT&E report on R4 testing in FY26.

The F-22 Program Office is writing an F-22 Overarching TEMP that contains test planning details for future capability releases up to R10 in FY26. The program office will provide shorter, more detailed TEMP annexes that outline and resource testing for specific capability releases on an annual cadence. The Air Force Operational Test and Evaluation Center is writing an accreditation plan to use the JSE for SeE IOT&E testing.

» MAJOR CONTRACTOR

- Lockheed Martin Aeronautics Company – Fort Worth, Texas

TEST ADEQUACY

» OVERARCHING CHALLENGES

The lack of instrumentation, such as the Common Range Integrated Instrumentation System (CRIIS) and Open-Air Battle Shaping (OABS), in the F-22A operational test aircraft to provide high-fidelity accurate mission-level results continued to restrict the Air Force's ability to accomplish adequate mission-level evaluations in FY25. DOT&E required F-22A capability releases, starting with R1, to use high-fidelity, real-time kill removal instrumentation for accurate mission-level results during operational flight test events. This capability is also needed for the Air Force to use data collected during operational flight tests for verification, validation, and accreditation (VV&A) of the F-22A model in the JSE, which is required for SeE testing.

Technical challenges have prevented the Air Force from integrating a capability to provide high-fidelity, real-time kill removal for accurate mission-level results with the F-22A. Omissions in the F-22A OFP and delays integrating the requisite hardware to utilize OABS, the currently identified pathway for delivering the capability, have prevented the CRISS/OABS solution from functioning. No F-22A operational test events to date have used OABS or an equivalent capability, making effectiveness testing inadequate.

The Air Force needs to use the JSE to test capability upgrades that are part of the SeE program. The adequacy of future testing of the F-22A with the planned SeE capability is at risk, because delivery of the SeE model for the JSE is unfunded. Moreover, the required environment upgrades to the JSE baseline may not be delivered in time for the IOT&E of the F-22A model with SeE.

» R3 FOT&E

R3 FOT&E testing included FDE flight test events in FY24, suitability testing, a cyber vulnerability investigation (CVI) event, and a live fire evaluation of the low-drag fuel tanks, pylons, and sensor pod. FOT&E was adequate to determine operational suitability and survivability; however, FOT&E was not adequate to determine operational effectiveness, because the capability to provide high-fidelity, real-time kill removal for accurate mission-level results has not been integrated onto the aircraft. The Air Force also conducted R3 test events that included live employment of three AIM-120 Advanced Medium-Range Air-to Air Missiles (AMRAAM). This was the only portion of integrated testing that DOT&E observed.

» R4 FOT&E

R4 FOT&E testing in FY25 included an FDE flight test event, suitability testing, and a CVI event. DOT&E observed the FDE flight test event in February 2025. The aircraft used for the FDE were operationally representative, and all missions took place in accordance with the

DOT&E-approved test plan. DOT&E observed AIM-120 AMRAAM employment during Weapon System Evaluation Program integrated test events and the R4 CVI event in May 2025. The CVI took place at the Agile Integration Laboratory in St. Louis, Missouri. An on-aircraft cooperative vulnerability and penetration assessment planned for April 2025 was canceled because of scheduling conflicts.

PERFORMANCE

» EFFECTIVENESS

DOT&E did not assess R3 operational effectiveness because the capability to provide high-fidelity, real-time kill removal for accurate mission-level results has not been integrated onto the aircraft, resulting in testing being inadequate.

DOT&E will assess R4 operational effectiveness in a classified R4 FOT&E report in FY26.

» SUITABILITY

The R3 upgrade for the F-22A is not operationally suitable. While hardware reliability has improved relative to R2, the F-22A is still not maintainable without contractor support. Air Force maintainers rely on Lockheed Martin contractors to diagnose hardware failures. Additional details are discussed in the DOT&E classified R3 combined early fielding and LFT&E report published in February 2025.

DOT&E will assess R4 operational suitability in a classified R4 FOT&E report in FY26.

» SURVIVABILITY

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, are discussed in the DOT&E classified R3 combined early fielding and LFT&E report published in February 2025.

DOT&E will assess R4 cyber survivability in a classified R4 FOT&E report in FY26.

RECOMMENDATIONS

As recommended in the FY24 Annual Report, the Air Force should:

1. Conduct all future mission-level evaluations of the F-22A with the capability to provide high-fidelity, holistic mission evaluations of new capabilities in operationally representative environments. The data collected via such capabilities are critical for accomplishing the VV&A of the F-22A model in the JSE.
2. Fund and contract for the delivery of the SeE model in time to complete VV&A prior to its 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.

HH-60W Jolly Green II

In FY25, the Air Force decided not to pursue the addition of the GAU-18 weapon to the HH-60W, thus eliminating one of the three remaining objectives in the HH-60W FOT&E test plan. DOT&E approved the deviation from the test plan in July 2025. As no other FOT&E objectives were achieved in FY25, the Air Force has two remaining objectives – one concerning cueing symbology and one regarding the external gun mount – to evaluate deficiency corrections from the FY22 IOT&E. DOT&E intends to publish a classified FOT&E report when the remaining 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. The FOT&E is evaluating mission planning and defensive system updates (completed in FY24), upgraded hover symbology for reduced visibility approaches (RVAs), and a new external gun mount to correct deficiencies identified in IOT&E. In FY25, the Air Force elected not to pursue the addition of the GAU-18 weapon to the HH-60W, removing one of the five objectives. However, the updated GAU-21 weapon is still planned and will continue testing in accordance with the approved HH-60W test plan.

» MAJOR CONTRACTOR

- Sikorsky Aircraft Corporation, a subsidiary of Lockheed Martin Corporation – Stratford, Connecticut

TEST ADEQUACY

In October 2024, the Air Force completed developmental testing of the upgraded system software with hover symbology to support RVAs. An operational military flight release was released in 4QFY25, which will enable the Air Force Operational Test and Evaluation Center to accomplish FOT&E of the RVA objective in 1QFY26. Developmental testing of the modified external gun mount with the GAU-21 is expected to begin by 3QFY26, but FOT&E is on hold until the Air Force determines if the gun mount design is in a final production-representative configuration. DOT&E approved the deviation to remove one test objective from the FOT&E test plan and will publish a classified FOT&E report, assessing test adequacy and system performance, when the remaining FOT&E objectives are complete.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

The preliminary findings from completed FOT&E events are unchanged from the FY24 Annual Report. DOT&E will publish a detailed assessment of HH-60W operational effectiveness, suitability, and survivability in a classified report when the remaining FOT&E objectives are complete.

RECOMMENDATION

The Air Force should:

1. Complete FOT&E objectives regarding the upgraded hover symbology and the updated external gun mount, as recommended in the FY24 Annual Report.

KC-46A Pegasus

The Air Force continues to work with Boeing to make technical upgrades to the KC-46A's Remote Vision System (RVS) and the Boom Telescope Actuator Redesign (BTAR) in order to meet operational requirements. Upon completion of those upgrades, IOT&E will be resumed. In FY25, the Air Force Operational Test and Evaluation Center (AFOTEC) completed the cybersecurity portion of IOT&E.

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 Wing Aerial Refueling Pod 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 a 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 aerial refueling (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 November 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 continues to implement corrections to the RVS (version 2.0) and the BTAR. Upon completion of those efforts, IOT&E will be completed. In the interim, 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

AFOTEC has collected 85 percent of the planned IOT&E flight test data but cannot complete the remaining IOT&E events until the program office implements final RVS and BTAR upgrades. Operational testing of the upgrades will be as fully integrated with developmental flight testing as possible, and all remaining IOT&E test events will be completed in conjunction with developmental test objectives. DOT&E will complete its assessment and publish a report once IOT&E is complete.

KC-46A IOT&E has been ongoing since May 2019. In previous years, AFOTEC has collected 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.

AFOTEC completed two cybersecurity adversarial assessments in December 2024. Upon completion, the Air Force published a cybersecurity report, concluding all IOT&E cyber testing outlined in the DOT&E-approved test plan.

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 27th candidate receiver will resume testing after the BTAR upgrade is complete.

The program office continues efforts to remediate all previously reported Category 1 deficiencies, including improvements to the RVS and BTAR as well as improving other various airframe deficiencies discovered during previous portions of test.

» SUITABILITY

The KC-46A has not been able to meet several suitability metrics in past years, and this trend has continued through FY25. The operational availability and mission capable rates are still well below their threshold requirements. Fleet suitability metrics will be updated at the end of IOT&E and included in the subsequent report. DOT&E will publish a report to address suitability once IOT&E is complete.

» SURVIVABILITY

The Air Force conducted ground and flight developmental testing on RFSDS software version 6.0 in FY25 and is preparing a preliminary report. Additional RFSDS testing is scheduled for 1QFY26. DOT&E will consider the developmental test findings in its final IOT&E report.

RECOMMENDATIONS

The Air Force should:

1. Continue to pursue design changes necessary to close the remaining Category 1 deficiencies, as recommended

in the FY23 and FY24 Annual Reports.

2. Develop and implement a strategy to address high drivers of availability and mission capable rate shortfalls, as recommended in the FY24 Annual Report.

Massive Ordnance Penetrator (MOP) Modification

In June 2025, the GBU-57 Massive Ordnance Penetrator (MOP) was successfully employed in a real-world event, during the significant B-2 bomber strike. According to the Chairman of the Joint Chiefs of Staff (CJCS), all 14 weapons met release parameters, guided accurately to their aimpoints, and functioned as intended. In July 2025, DOT&E removed the MOP Modification program from oversight.

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 GBU-57 warhead is intended to be more lethal than its predecessors, the GBU-28 and GBU-37. The Large Penetrator Smart Fuze (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. The B-2 Spirit is the only aircraft capable of employing the MOP.

MISSION

Combatant commanders 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. DOT&E placed the original MOP program on oversight in 2011 and transferred oversight focus to the MOP Modification program in February 2021.

The Air Force established the LPSF Quick Reaction Capability program in August 2018 to respond to an urgent operational need, validated in July 2018, to integrate and qualify a smart fuze capability into the MOP 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, and target construction commenced in FY25.

In June 2025, the MOP was successfully employed in a real-world event. As briefed by the CJCS, all 14 weapons met release parameters, guided accurately to their aimpoints, and functioned as intended.

DOT&E removed the MOP Modification program from oversight in July 2025.

» 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.

In FY25, subscale phenomenology testing validated enhanced weaponeering capabilities.

PERFORMANCE

» LETHALITY, SUITABILITY, AND SURVIVABILITY

DOT&E provided a classified assessment of the Enhanced Threat Response weapon modifications in the November 2017 early fielding report of the currently fielded MOP configuration. DOT&E sent a classified memorandum to the Secretary of Defense in August 2024, providing an update on the MOP integration with the B-2.

RECOMMENDATIONS

The Air Force should:

1. Continue funding LPSF T&E activities outlined in the draft TEMP in order to successfully complete adequate testing and eventual fielding of the LPSF.

DTRA should:

1. Continue efforts to streamline their contracting and test plan review processes to minimize delays and cost growth for target construction and test execution, as recommended in the FY22 – 24 Annual Reports.

MH-139A Grey Wolf

In June 2025, the Air Force completed the MH-139A IOT&E in accordance with the DOT&E-approved test plan, and DOT&E observed the testing. DOT&E will publish a classified IOT&E report to inform a full-rate production decision in 2QFY26.

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

Air Force Global Strike Command (AFGSC) intends for the MH-139A to replace the UH-1N to provide rapid transport capability to support nuclear security missions by providing emergency security response and convoy escort at Minot Air Force Base (AFB), North Dakota; Malmstrom AFB, Montana; and Francis E. Warren AFB, Wyoming.

In addition, the Air Force Reserve Command will use the MH-139A to 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.

The Air Force began IOT&E in January 2025, following DOT&E's approval of the IOT&E test plan. In May 2025, DOT&E approved a test deviation request to suspend Air Force District of Washington (AFDW) mission testing. IOT&E concluded in June 2025, and the Air Force intends to make a full-rate production decision in 2QFY26. DOT&E will publish a classified IOT&E report in 2QFY26 to inform this decision.

» MAJOR CONTRACTOR

- Boeing Defense, Space & Security – Ridley Park, Pennsylvania

TEST ADEQUACY

In October 2024, the Air Force conducted developmental testing of MH-139A modifications and removed flight restrictions that had delayed aircrew training for IOT&E. The Air Force provided three operationally representative aircraft for IOT&E, each equipped with a trunked radio for AFGSC missions, an environmental control system, and an updated cabin configuration.

The Air Force Operational Test and Evaluation Center (AFOTEC) conducted IOT&E from January through June 2025, in accordance with the DOT&E-approved test plan and test deviation request. DOT&E observed the testing. Operational testing focused on the ability of the MH-139A to support the two core nuclear security missions at three main operating bases, in a variety of environmental and threat conditions in over 36 formation sorties. IOT&E aircrews also participated in the AFGSC Nuclear Convoy Course to collect data on higher complexity convoy escort scenarios. The IOT&E included two phases, each of cooperative and adversarial cyber survivability testing. The IOT&E was adequate to assess MH-139A operational effectiveness, suitability, and survivability in performing its AFGSC missions. In accordance with the approved test deviation, AFOTEC did not test AFDW mission scenarios within the National Capital Region; this change did not affect the adequacy of testing to evaluate the AFGSC missions.

In FY25, the Air Force completed all live fire testing and analyses in accordance with the DOT&E-approved Alternative LFT&E Strategy, with the exception of electromagnetic pulse (EMP) testing. The Air Force plans to conduct EMP testing in 2QFY26.

PERFORMANCE

» EFFECTIVENESS

Preliminary IOT&E data analyses show the MH-139A is faster, has longer endurance times, can support longer-range missions, and can carry more security force personnel than the legacy UH-1N. However, testing also identified performance concerns with the intercommunication system (ICS) and gun mount that require further testing for MH-139 meeting operational effectiveness. The program is developing upgrades to the ICS and gun weapon system. DOT&E will provide a full assessment of MH-139A operational effectiveness in a classified IOT&E report planned for 2QFY26.

» SUITABILITY

During IOT&E, the MH-139A demonstrated low availability and mission capable rates, due to long repair times caused by supply chain issues. IOT&E flights were constrained by engine restrictions against hovering or landing in dusty conditions. DOT&E will provide a full assessment of MH-139A operational suitability in a classified IOT&E report planned for 2QFY26.

» SURVIVABILITY

DOT&E will provide a full assessment of MH-139A survivability, including cyber survivability, based on data from the cooperative and adversarial cyber testing, in a classified IOT&E report planned for 2QFY26. However, insufficient data are available to evaluate the survivability of the MH-139A against EMP. DOT&E will publish a classified survivability annex to the IOT&E report, following completion of the EMP testing planned for 2QFY26.

RECOMMENDATIONS

The Air Force should:

1. Increase availability and mission capability by addressing supply chain issues that drive repair delays.
2. Conduct EMP testing as outlined in the DOT&E-approved Alternative LFT&E Strategy.

Small Diameter Bomb Increment II (SDB II)

In FY25, the Navy conducted the last two remaining operational test (OT) events for the quick reaction assessment (QRA) of SDB II as integrated on F/A-18E/F aircraft. The program office anticipates SDB II will achieve initial operational capability (IOC) for those aircraft in early FY26. There were no OT events with SDB II employed from F-35B or F-35C aircraft in FY25; the next OT events from F-35C aircraft are scheduled for 1QFY26. The program office anticipates IOC for SDB II on F-35B and F-35C in FY27.

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 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 cue 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 static targets at designated 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). MOT&E Phase I flight testing was completed in December 2019, and DOT&E published a classified MOT&E Phase I combined OT and live fire test report in July 2020. The Air Force authorized fielding of SDB II on the F-15E in FY20 and declared IOC for SDB II on F-15E in September 2022.

In FY20, the Navy initiated a QRA of SDB II as integrated onto the F/A-18E/F. DOT&E approved a six-test-event QRA test plan. The Navy conducted QRA testing between December 2020 and May 2025. The Navy declared early operational capability on SDB II on the F/A-18E/F in October 2023. DOT&E published the SDB II Integration on the F/A-18E/F early fielding report in February 2024. The program office anticipates SDB II IOC on the F/A-18E/F in early FY26.

OT of SDB II on the F-35B and F-35C remains delayed due to integration problems identified during testing with SDB II on aircraft. MOT&E Phase II originally was intended to focus on the SDB II's integration on the F-35B and F-35C, the complete characterization of SDB II's performance against small boats, and the evaluation of SDB II's carrier and shipboard operability. However, to support an SDB II full-rate production (FRP) decision in 3QFY26, the program office has requested to change the Navy's threshold platform from the F-35B and F-35C to the F/A-18E/F, deferring completion of OT of SDB II on the F-35B and F-35C until after FRP and delaying IOC for SDB on those aircraft until FY27. The program office continues to draft the SDB II FRP TEMP, which will reflect the changes to the threshold aircraft. The FRP decision is now planned for 3QFY26, a delay of a year from what was anticipated in the FY24 Annual Report.

The Navy's Operational Test and Evaluation Force continues working to complete the MOT&E Phase II test plan, based on the anticipated change in the Navy threshold platform. DOT&E is assessing the OT already completed to determine what additional testing is necessary to publish an MOT&E Phase II OT report.

SDB II's integration on the F-35 is to occur in two phases. The first phase is intended to provide a limited capability integration, which will be followed by full integration across all variants. In August 2025, DOT&E approved the F-35 United Operational Test Team's (UOTT's) 30R08 OT test plan, which includes OT of the first phase of SDB II integration on the F-35. Delays in the F-35 30R08 software development and integration problems with SDB II prevented the UOTT from conducting any OT on the F-35 in FY25.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX – Tucson, Arizona

TEST ADEQUACY

In April 2025, the Navy completed the two remaining live-fly OT events against moving maritime targets at Point Mugu Sea Range to complete the F/A-18E/F QRA. DOT&E observed these test events, which the Navy executed in accordance with a DOT&E-approved test plan and test plan change. The Navy required a total of nine attempts to accomplish these two test events:

- In November 2023, one attempt was canceled because a bomb rack unit problem caused a hung weapon.
- In December 2023, one attempt was unsuccessful due to weather conditions on the designated test range.
- In February 2024, two attempts were canceled due to unsuccessful loading of the correct cryptographic keys into the weapon. One of these attempts would have been canceled because the FAA did not provide clearance to operate the weapon on the Link 16 network, which is a recurring issue affecting network-enabled weapon testing across the DoW.
- In May 2024, two attempts were unsuccessful due to weather conditions on the designated test range.

- In August 2024, two attempts were unsuccessful, one due to a malfunction on the weapon and one due to 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.
- In April 2025, both test events were completed; only one event was successful.

Due to overland range safety limitations, the maximum employment range used during OT has been below the program's threshold requirement. Other range safety restrictions continue to significantly limit SDB II employment envelopes and F-35 self-lasing. These restrictions prevent testing of SDB II's full operational capabilities.

No OT events with SDB II employed from F-35B or F-35C aircraft occurred in FY25.

PERFORMANCE

» EFFECTIVENESS

DOT&E's July 2020 classified MOT&E Phase I combined OT and live fire test report provided an assessment of SDB II's operational effectiveness as deployed from the F-15E.

The program has not yet demonstrated operational effectiveness on the F-35B or F-35C. As discussed in the FY23 Annual Report, operational users had difficulty employing full SDB II network-enabled weapon functionality on the F/A-18E/F. A developmental test in 2024 on SDB II revealed a targeting software anomaly, which is planned to be resolved in an SDB II software update. The software correction will be verified during OT of the SDB II on the F-35.

» LETHALITY

DOT&E's July 2020 classified MOT&E Phase I combined OT and live fire test report provided an assessment of SDB II's lethality. This assessment is not affected by the platform deploying the SDB II.

» SUITABILITY

DOT&E's July 2020 classified MOT&E Phase I combined OT and live fire test report provided an assessment of SDB II's operational suitability on the F-15E. This report highlighted concerns with cryptographic key loading and mission planning for the SDB II. 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. As noted in the FY24 Annual Report, operational squadrons can now consistently load the correct keys into the weapon and achieve network-enabled weapon functionality.

The program has not yet demonstrated interoperability with the F/A-18E/F, F-35B, or F-35C.

» SURVIVABILITY

DOT&E's July 2020 classified MOT&E Phase I combined OT and live fire test report identified shortfalls with cyber survivability testing, which have not yet been addressed. The testing the Air Force conducted in FY19 was inadequate to fully evaluate cyber survivability. 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 Navy and the program office are working with DOT&E to rectify these shortfalls, to submit an updated cyber survivability test plan to DOT&E for approval, and to conduct additional cyber survivability testing.

RECOMMENDATIONS

As recommended since the FY23 Annual Report, the DoW 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 FAA to develop a timely approval process and reasonable safety measures that will allow the DoW to test network-enabled weapons in restricted airspace.

As recommended since the FY23 Annual Report, the Navy should:

1. Continue to develop and fund an adequate SDB II cyber survivability T&E.

The SDB II Program Office should:

1. Update the FRP TEMP to reflect the updated cyber survivability strategy and threshold platform changes, and submit the updated TEMP for DOT&E's approval.

2. Continue efforts to improve the mission planning process across all platforms, particularly regarding cryptographic data entry, as recommended since the FY23 Annual Report.

T-7A Advanced Pilot Training (APT)

In FY25, the Air Force and Boeing continued T-7A developmental testing (DT), monitored by DOT&E, using contractor-owned and -operated prototype aircraft and Engineering and Manufacturing Development (EMD) aircraft. DOT&E will provide an observation report based on the DT data to assess T-7A progress toward operational effectiveness, suitability, and survivability to support the Milestone C (MS C) decision scheduled for 2QFY26. The program office plans to begin IOT&E in FY27.

SYSTEM DESCRIPTION

The Advanced Pilot Training (APT) system includes the T-7A Red Hawk aircraft and Gound Based Training System (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 system 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 2QFY26 and the full-rate production decision threshold date from September 2025 to 2QFY28.

Boeing delivered the last two EMD aircraft in 1QFY25. To compensate for delay in the MS C decision, the Air Force contracted four additional aircraft that are production-representative test vehicles (PRTV) prior to low-rate initial production. The MS C TEMP is in coordination to support a planned MS C decision in 2QFY26.

The program is scheduled to begin IOT&E in FY27 to support a full-rate production decision in FY29. AETC plans to procure 351 T-7A aircraft, 46 simulators, and associated GBTS for deployment to its five pilot training bases: Joint Base San Antonio-Randolph, Texas; Columbus Air Force Base (AFB), Mississippi; Laughlin AFB, Texas; Vance AFB, Oklahoma; and Sheppard AFB, Texas.

The program office is working with Boeing to contract testing in the transonic and supersonic regions prior to IOT&E. While the APT contract does not require a supersonic trainer, the T-7A is capable of supersonic flight. Student pilots might exceed technical order limits of 0.95 Mach during T-7A designated missions, particularly during the advanced fighter fundamentals course. This will be mitigated by verifying the aircraft's ability to safely reach and recover from speeds exceeding the flight manual limits up to 1.05 Mach.

» MAJOR CONTRACTORS

- The Boeing Company – St. Louis, Missouri
- Saab AB – Linköping, Sweden and Lafayette, Indiana

TEST ADEQUACY

Boeing continued flight testing of two contractor-owned-and-operated prototype EMD aircraft in FY25. DOT&E has continually monitored and periodically observed DT to support an observation report to inform the MS C decision and assess progress toward operational effectiveness, suitability, and survivability.

DOT&E will not use test data from these prototype aircraft in its final evaluation of system performance after IOT&E, as the prototypes are substantially different from the five EMD aircraft contracted. The EMD and PRTV aircraft will be used for government-led DT and operational testing. Boeing's FY25 DT continued to focus on resolving safety-of-flight issues required for airworthiness certification. These issues included the escape system, flight control software, high angle-of-attack portion of the flight envelope, propulsion, noise and vibration, and departure resistance.

Government-led DT in FY25 focused on wing flutter, flying qualities, aerodynamic structural loads, and initial mission systems test points. The program office identified a set of critical test data to assess in order to support the MS C low-rate initial production decision in 2QFY26. These data include high-angle-of-attack testing, structural design limit loads testing, and wing flutter to at least 500 knots calibrated air speed. The majority of the remaining test points in the government DT test plans, which include testing design loads, crew systems, On-Board Oxygen Generation System (OBOGS), and high-angle-of-attack testing, have the potential to drive further software and flight control changes. The program now projects that DT will be complete by 1QFY28, a delay from what was projected in the FY24 Annual Report.

In October 2024, the program conducted a final escape system study phase dynamic sled test, leading to the first escape system qualification tests in April and August 2025. In June 2025, the program completed the second cold and hot weather test event at the McKinley Climatic Laboratory at Eglin AFB, Florida.

The Cyber Approving Official approved the T-7A Aircraft System Interim Authority to Test in March 2025. The program completed a mission-based risk assessment for cyber in June 2025, and completed a sixth adversarial cyber developmental test in the Boeing Systems Integration Laboratory in August 2025.

The Air Force Operational Test and Evaluation Center (AFOTEC) Detachment 5 provided operational feedback throughout Boeing's initial design efforts and early DT. As of FY24, AFOTEC published five periodic reports assessing progress towards operational effectiveness and suitability, with a total of 41 recommendations, 37 of which remain open. No additional periodic reports were completed in FY25. DOT&E concurs with AFOTEC's assessments and recommendations.

PERFORMANCE

» EFFECTIVENESS

Insufficient data are available at this time to provide an assessment of operational effectiveness of T-7A. 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. In FY26, DOT&E will provide an observation report based on DT data to assess progress toward operational effectiveness and inform the MS C decision.

» SUITABILITY

Insufficient data are available at this time to provide an assessment of operational suitability of T-7A. The program continues to work through known suitability limitations, most notably regarding the aircraft escape system, logistics supportability issues, and Automatic Ground Collision Avoidance System (AGCAS).

As reported in the FY22 – 24 Annual Reports, the original T-7A emergency escape system did not meet minimum safety requirements for the Air Force's airworthiness certification. The current design began qualification testing with two high-speed sled tests of the canopy and ejection sequencer, and to date the Air Force has completed 17 of 22 dynamic test events. The program must successfully complete a total of five qualification sled test events under varied conditions before the escape system can be certified for airworthiness and IOT&E.

The program office also continued to make progress on the T-7A on Board Oxygen Generation System (OBOGS). The T-7A OBOGS DT will collect data over 10 ground and 100 hours of flight test events, including high and sustained-g maneuvering. 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.

In FY26, DOT&E will provide an observation report based on DT data to assess progress toward operational suitability and inform the MS C decision.

» SURVIVABILITY

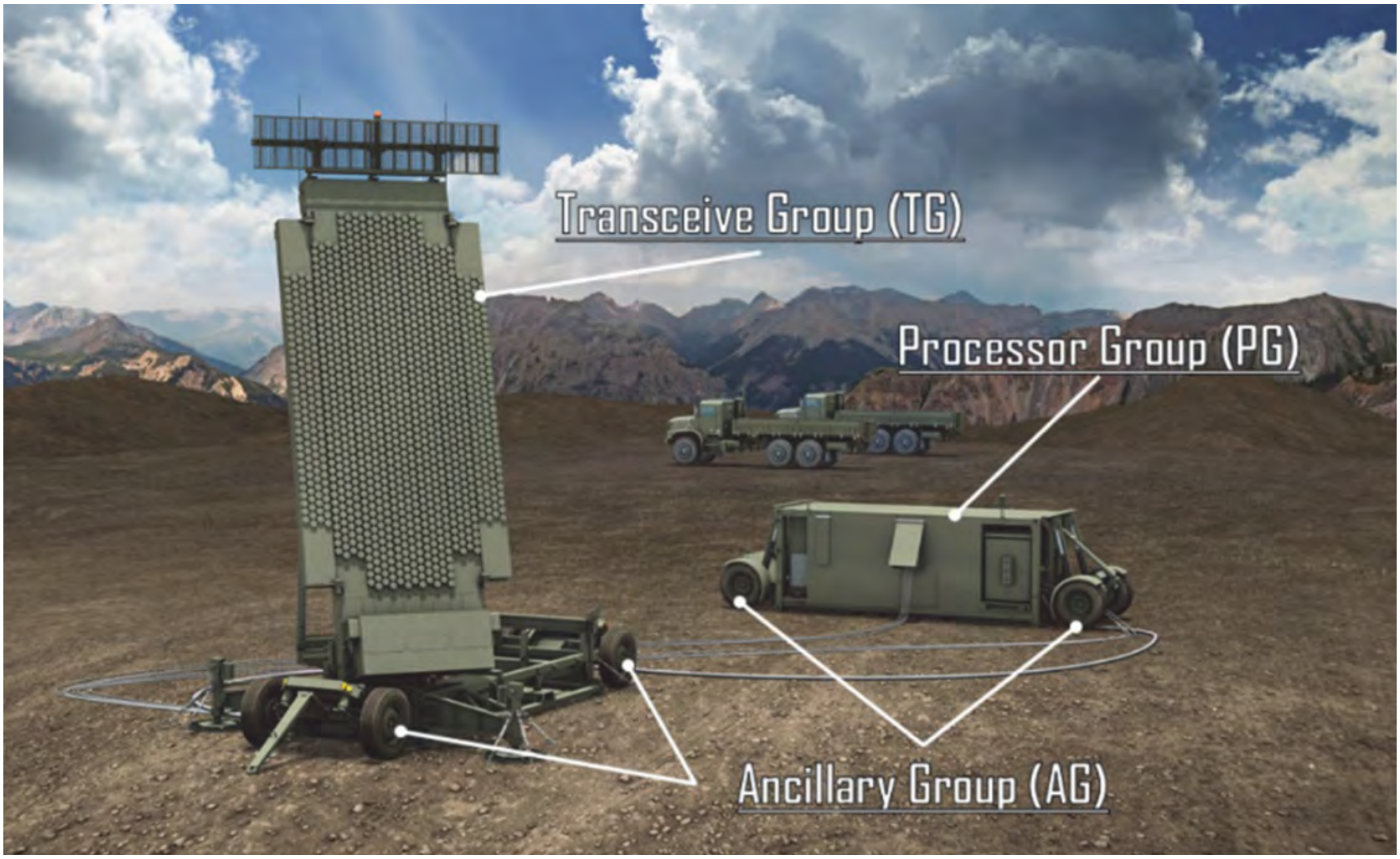
Insufficient data are available at this time to provide a survivability assessment of T-7A. In FY26, DOT&E will provide an observation report based on DT flight and cyber test data to assess progress toward operational survivability and inform the MS C decision.

RECOMMENDATIONS

As recommended in the FY24 Annual Report, 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 the 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)



During 3QFY24, the Air Force started and then paused formal government-led developmental testing (DT) of the Three-Dimensional Expeditionary Long-Range Radar (3DELRR), to allow Lockheed Martin to troubleshoot 3DELRR system performance and reliability issues. The Air Force then restarted government-led DT in 3QFY25 and began an operational assessment (OA) in June 2025. The Air Force has delayed the start of 3DELRR IOT&E from 1QFY26, as reported in the FY24 Annual Report, to 3QFY26.

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 beamforming 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 to 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 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 (MCA) program in 1QFY27 to support the production and fielding of the remaining full operational capability TPY-4 systems. The planned MCA transition in 1QFY27 represents a delay of approximately one year.

» MAJOR CONTRACTOR

- Lockheed Martin Corporation – Syracuse, New York

TEST ADEQUACY

The Air Force had planned to complete an OA of the 3DELRR in FY25 by collecting data during government-led DT, but the Service paused government-led DT for most of FY25, as Lockheed Martin continued to troubleshoot 3DELRR performance and reliability issues. The Air Force started an OA in June 2025, delaying the originally planned OA completion date by more than a year.

The Air Force plans to use integrated testing at every opportunity and resource tests for near-peer, threat-representative targets. Dedicated IOT&E is expected to start in 3QFY26.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E will provide an assessment of 3DELRR's progress towards operational effectiveness, suitability, and survivability, once the Air Force executes the OA that is now expected to be completed in 3QFY26.

RECOMMENDATIONS

The Air Force should:

1. Plan and resource for appropriate threat representative targets, as recommended in the FY22 – 24 Annual Reports.
2. Provide DOT&E with an updated 3DELRR OA and IOT&E test schedule to account for the change in testing timelines.

This page intentionally left blank.

Space Force Programs

This page intentionally left blank.

Global Positioning System (GPS) Enterprise

In December 2024, DOT&E approved the IOT&E test plan for the Next Generation Operational Control System (OCX) Blocks 1 and 2. IOT&E for OCX Blocks 1 and 2 has begun, with the cooperative vulnerability and penetration assessment (CVPA) performed in September 2025. Also in September 2025, the Military GPS User Equipment (MGUE) Increment 1 program completed integrated developmental test (DT)/operational test (OT) as installed on the MQ-1C Gray Eagle unmanned aerial system. DOT&E will publish classified test reports on OCX Blocks 1 and 2 and MGUE Increment 1 in FY26.

Though the GPS Enterprise was removed from oversight in July 2025, some of the specific program elements that enable the GPS Enterprise will remain on DOT&E oversight. DOT&E removed GPS III and MGUE Increment 2 from oversight, as the former has stabilized and the latter is covered by other programs on oversight.

SYSTEM DESCRIPTION

The GPS Enterprise is a satellite-based global radio navigation system of systems, operated by the Space Force, that provides accurate and secure positioning, navigation, and timing (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 military user equipment segment includes the MGUE, which is intended to modernize military GPS receivers, including the ability to receive and use the more secure Military Code (M-code) signal.

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 enable military users to access the 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 algorithm 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 military user equipment segments. In August 2021, DOT&E approved the Enterprise TEMP Revision C that encompasses the three segments of GPS. In FY26, the Space Force plans to draft the Enterprise TEMP Revision D, to address updates to OCX.

- **GPS III Satellite** – An Acquisition Category (ACAT) IC program that achieved Milestone C (MS C) in January 2011. The last of the ten GPS III satellites, Space Vehicle 10, was made available for launch in December 2022. Since 2018, the Space Force has successfully launched eight GPS III satellites and plans to launch the remaining two satellites in FY26. The two most recent satellite launches in FY25 demonstrated the Space Force's ability to complete high-priority launches on a rapid timescale to achieve a broader goal of tactically responsive space operations. In July 2025, DOT&E removed GPS III from oversight because program development has stabilized and there are no significant planned upgrades or OT activities.
- **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 conduct cyber operational testing of Block IIIF satellites in FY26. The Space Force plans to launch the first GPS IIIF satellite in FY27 and operationally accept it in FY28.
- **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 GPS III satellites and provide core M-code capability from the existing GPS constellation while maintaining previous civilian and military services. OCS AEP had been considered part of the GPS Enterprise, which DOT&E removed from oversight in July 2025 because it was not specific to programs of record. OCS AEP development has stabilized and no longer requires DOT&E oversight.
- **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. The Space Force accepted the system from the development contractor in July 2025. OCX will replace OCS AEP following a successful constellation transfer that the Space Force currently plans to execute in FY26, followed by operational acceptance. DOT&E approved the IOT&E test plan for OCX Blocks 1 and 2 in December 2024, and the CVPA cyber test plan in September 2025. Continued delays to OCX put U.S. warfighters and allies

at risk, because full M-code has not deployed to the field for use in operations.

- **OCX 3F** – A tailored ACAT II program that builds on the software delivered by OCX. Contingent on successful OCX deployment, the subsequent OCX 3F upgrade will allow OCX to support launch as well as command and control 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, schedule slips to OCX correspondingly affect operational acceptance of OCX 3F 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. The MGUE Increment 1 program delivered an interim functional aviation/maritime receiver card in September 2022. The program continues to resolve deficiencies related to integration with the lead maritime platform, the Arleigh Burke-class destroyer, and plans to operationally test MGUE aboard the ship in FY27. In September 2025, the U.S. Army Special Operations Command conducted an integrated DT/OT of the aviation/maritime receiver card embedded within the MQ-1C Gray Eagle unmanned aerial system. Gray Eagle does not pass data to GPS-guided weapons, so future testing of MGUE Increment 1 will be required as configured on a weapons platform like the B-2 aircraft. The Space Force expects to transfer the program to the Air Force in FY26.
- **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 Application-Specific Integrated Circuits (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. DOT&E removed MGUE Increment 2 from oversight in July 2025, because the MSI receiver is already covered by existing testing programs and the handheld does not require oversight.

» 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)

Military User Equipment 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

In March 2025, DOT&E funded an assessment of OCS AEP through the Cyber Assessment Program to assess the current cyber defense posture of the GPS control segment. Testing included vulnerability identification, penetration testing, and an assessment of the defensive monitoring of OCS AEP. These results will be included in the overarching cybersecurity reporting.

In September 2025, in accordance with the DOT&E-approved cyber test plan, the Space Force began to conduct the CVPA of OCX Blocks 1 and 2, which DOT&E observed. The CVPA will complete in FY26 and will be followed by an adversarial assessment (AA). DOT&E will evaluate the cyber survivability of OCX Blocks 1 and 2 in a classified IOT&E report using data from the CVPA and AA, as well as data from the OCS AEP cyber assessment for comparison purposes.

The Space Force delayed OCX testing of command and control of the four-satellite mini-constellation until FY26, due to program schedule delays. The Space Force still plans to complete this limited test ahead of the full IOT&E, beginning later in FY26.

In September 2025, the U.S. Army Special Operations Command conducted an integrated DT/OT of MGUE Increment 1 as configured on Gray Eagle, in accordance with a DOT&E-approved test plan. DOT&E observed the event to assess MGUE Increment 1's operational effectiveness and suitability in this specific configuration. Additional testing is still required on a maritime platform, as well on an aviation platform that incorporates a GPS-guided weapon, such as the B-2. In FY26, DOT&E will report on MGUE Increment 1 operational testing on Gray Eagle following completion of data analysis.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

There are insufficient data at this time to assess OCX's operational effectiveness and suitability. DOT&E will provide these assessments in a classified IOT&E report, following completion of testing, expected in FY26.

DOT&E continues to analyze data from the MGUE Increment 1 integrated DT/OT and will assess MGUE Increment 1's progress towards operational effectiveness and suitability in a classified report in FY26.

DOT&E has no updates to previous operational effectiveness and suitability findings for other GPS programs, as they did not undergo OT in FY25.

» SURVIVABILITY

There are insufficient data at this time to assess OCX's cyber survivability. DOT&E will provide this assessment in the classified IOT&E report, following completion of all testing. The cyber survivability assessment will utilize data from the CVPA and AA, as well as data from the OCS AEP cyber assessment for comparison purposes.

DOT&E has no updates to previous survivability findings for other GPS programs, as they did not undergo OT in FY25.

RECOMMENDATION

The Space Force and Air Force should:

1. Fund and plan MGUE Increment 1 OT that integrates the maritime/aviation receiver card with a platform that employs a GPS-guided weapon system, like the B-2.

Space Command and Control System (Space C2)

The Space Command and Control (Space C2) program continues to progress toward the system and capability maturity necessary to retire the Space Defense Operations Center (SPADOC) system. The scope of an FY25 operational utility evaluation (OUE) was reduced to capabilities that were ready, but testing produced adequate data for DOT&E to assess that Space C2 is progressing towards operational effectiveness and suitability determinations for most planned capabilities. Cyber survivability testing was planned for FY25, but the draft adversarial assessment plan was inadequate, and no revised plan was submitted for DOT&E's approval. DOT&E intends to publish a classified OUE report in 1QFY26. More Space C2 OT&E, including cyber survivability testing, is needed to draw conclusions on operational effectiveness, suitability, and survivability.

In FY25, Space C2 restructured into two independent programs, Atlas and Kronos. In July 2025, DOT&E separated the two programs on the oversight list and will produce separate annual report entries for Atlas and Kronos going forward.

SYSTEM DESCRIPTION

The Space C2 system uses a commercially supported platform to access data and provide services for user applications that enable command and control operations. Space C2 uses a hybrid of cloud and on-premises hardware 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):

- LOE 0: System Engineering, Integration, and Test
- LOE 1: Platform, Infrastructure, and Data

- LOE 2: Space Domain Awareness (SDA) Software
- LOE 3: Theater Support Software
- LOE 4: Space Defense Software

The LOEs deliver capabilities across the following broad categories:

- **SDA Software** focuses on modernizing SDA astrodynamics toolsets by building a system of applications that create an operational picture of the space domain to inform warfighter decisions. This includes Theater Support Software, which 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.

These capabilities enable the missions of Space Force's Space Operations Command (SpOC)'s Mission Delta 2 (SDA), Space Delta 5 (Combined Space Operations Center), and Space Delta 15 (National Space Defense Center). Since FY22, Space C2 development efforts have focused primarily on delivering capabilities to replace the legacy SPADOC system with a modernized and integrated SDA system.

MISSION

Space Force Guardians will use Space C2 to provide a wide range of space defense and SDA command and control to facilitate timely, quality battlespace decisions by DoW 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 Mission Delta 2's 18th Space Defense Squadron, Space Delta 5 supporting the Combined Space Operations Center, Space Delta 15 supporting the National Space Defense Center, and other command and control centers.

PROGRAM

The Space C2 program was initiated as a Development, Security, and Operations (DevSecOps) pathfinder in 2019 with the goal of sustaining current operations while developing new capabilities that would enable the decommissioning of SPADOC no later than 2022. After not achieving that goal by FY22, the Space C2 program used the last three years to refocus its capability development to accelerate delivery of Advanced Tracking and Launch Analysis System (ATLAS) capabilities that were critical to enable the decommissioning of SPADOC, while deemphasizing the delivery of non-critical applications.

SpOC operationally accepted ATLAS in September 2025. The Space Force's operational testing, followed by system upgrades and a trial period, informed the operational acceptance decision. However, the Space Force is not yet ready to decommission SPADOC.

In May 2025, Space C2 restructured into two independent programs: Atlas, which contains the SDA program components, and Kronos, which contains the space defense and theater support program components. The two independent programs will develop their own T&E strategies and will be separate but related acquisition efforts moving forward. Thus, in July 2025, DOT&E separated the programs on oversight and will have separate annual report entries for Atlas and Kronos going forward.

Together, these two programs will fulfill the overarching Space C2 requirements and execution of the Space C2 LOEs:

- Atlas will deliver SDA-associated software (LOE 2); system engineering, integration, and test capabilities (LOE 0); and platform, infrastructure, and data needs (LOE 1). The Atlas program will be executed by SpOC's Mission Delta 2 to support integration of SDA operations, sustainment, and capability development.
- Kronos will fulfill all remaining Space C2 program efforts, including those identified in theater support (LOE 3) and space defense (LOE 4), as well as associated efforts to address platform, infrastructure, and data needs (LOE 1). The Kronos program will be executed by Systems Delta 85.

Both Atlas and Kronos use the software acquisition pathway (SWP) and are in varied phases of the SWP. In May 2025, Atlas was approved for entry into the SWP execution phase and Kronos was approved to enter the SWP planning phase. Atlas entered the execution phase of the SWP, following completion of entrance criteria previously approved for Space C2 in FY21 by the OUSD(A&S). Both programs were also tasked to provide DOT&E an updated T&E Strategy to address approval caveats that accompanied the previous T&E Strategy in FY23. A T&E Strategy update remains outstanding and is expected in FY26. A separate Kronos T&E Strategy is being developed.

Atlas entered a trial period in August 2025 to demonstrate that its capabilities were mature enough to declare initial operational capability to support program continuation decisions mandated by Section 1607 of the NDAA for FY24 and to enable future decommissioning of SPADOC. Based on the results of that trial period, the SpOC commander operationally accepted the system.

» MAJOR CONTRACTORS

Space C2 is comprised of a multitude of contracts and contractors developing capabilities, including:

- L3Harris Technologies, Inc. – Colorado Springs, Colorado
- Omitron, Inc. – Colorado Springs, Colorado
- Palantir Technologies, Inc. – Denver, Colorado
- Parsons Corporation, Space Operations Division – Centreville, Virginia
- Systems Planning and Analysis, Inc. – Alexandria, Virginia

TEST ADEQUACY

The Space C2 program conducts quarterly SDA capability integrated tests (SCITs) intended to produce usable data for both the developmental and operational testing communities. FY25's SCIT-10 was the first SCIT to produce operational test data, becoming the first installment in an incremental operational test campaign scoped to the capabilities necessary for SPADOC decommissioning. The SCIT scope was intended to be an OUE that included multiple applications, such as ATLAS, within the Space C2 program. The scope of the OUE was reduced by the Space Force because no capabilities were fully developed. DOT&E observed the test and found that, for the remaining scope, testing was in accordance with the DOT&E-approved test plan. While data collected were adequate for DOT&E to determine that Space C2 is making progress towards operational effectiveness and suitability, not all planned objectives were fully achieved. ATLAS, as tested, did not contain the minimum viable capability necessary for SPADOC decommissioning. Testing also revealed deficiencies consistent with system immaturity. Several of the required minimum viable capabilities required to replace SPADOC functionality were not completed in time for the OUE and will need to be operationally tested as the capabilities mature. Further details will be included in DOT&E's classified OUE report, planned for 1QFY26.

The OUE mitigated previously identified limitations regarding the operational relevance of the test environment. The program maintained a stable software baseline prior to and throughout testing to allow for continuous evaluations. Mission Delta 2 staffed trained operators, with access to appropriate documentation, throughout the SCIT at the level needed for nominal operations. Operators reported their perceived workload as they completed various tasks.

A cyber survivability adversarial assessment (AA) was planned for FY25; however, the initial draft test plan DOT&E received had shortcomings, and no revised plan was submitted for approval. To inform the operational acceptance and system updates, the Space C2 program conducted an assessment based on the unapproved plan. They do not intend to conduct an AA in FY26 but have committed to seek DOT&E approval of the test plan whenever they do.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

The Space C2 program has advanced the maturity of ATLAS, improving its capabilities. Further testing will be needed to fully characterize Atlas's and Kronos's operational effectiveness and suitability.

» SURVIVABILITY

Insufficient data have been collected to inform an assessment of operational survivability for the individual Space C2 programs. For ATLAS, data from a future AA will complement data from the cooperative vulnerability and penetration assessment conducted in FY24.

RECOMMENDATIONS

Consistent with the recommendations in the FY24 Annual Report, the Space Force should:

1. Continue focused efforts on further development and adequate operational testing of SDA capabilities to enable the decommissioning of SPADOC.
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. Develop and submit test plans and overarching T&E strategies for DOT&E approval with sufficient time for coordination.

Space-Based Infrared System (SBIRS) Survivable Endurable Evolution (S2E2)

In December 2024, the Space Force completed IOT&E of Space-Based Infrared System (SBIRS) Survivable Endurable Evolution (S2E2), and in March 2025, DOT&E published a classified S2E2 IOT&E report. In April 2025, Space Force's Space Operations Command declared operational acceptance of S2E2. DOT&E removed the S2E2 program from oversight in July 2025, given the completion of IOT&E and reporting to inform operational acceptance.

SYSTEM DESCRIPTION

The S2E2 is a transportable ground station that integrates a SBIRS Mobile Ground Terminal and a Universal Ground Nuclear Detonation Detection Terminal. It processes data from both SBIRS and nuclear detonation detection systems to transmit messages to consumers. S2E2 replaces the legacy Mobile Ground System.

MISSION

Commanders will use units equipped with S2E2 to provide missile warning and nuclear detonation detection capability in contested and degraded environments.

PROGRAM

The S2E2 system is a modernization upgrade activity under the SBIRS Acquisition Category IC Major Defense Acquisition Program. DOT&E placed S2E2 on oversight in 2018. In October 2024, DOT&E approved the IOT&E test plan without requiring a DOT&E-approved TEMP. In April 2025, the Space Operations Command declared operational acceptance of S2E2. DOT&E removed the S2E2 program from oversight in July 2025, following the completion of IOT&E and reporting to inform operational acceptance.

» MAJOR CONTRACTORS

- Lockheed Martin Space Systems – Sunnyvale, California
- Sandia National Laboratories – Albuquerque, New Mexico

TEST ADEQUACY

The Space Force completed IOT&E of S2E2 in December 2024, in accordance with the DOT&E-approved test plan. DOT&E observed the test. DOT&E's classified March 2025 IOT&E report informed the Space Force's decision to operationally accept S2E2 in April 2025.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E's assessment of S2E2 operational effectiveness, suitability, and survivability is classified. Details can be found in the in the March 2025 IOT&E report.

RECOMMENDATION

The Space Force should:

1. Address all recommendations in DOT&E's classified March 2025 IOT&E report.

Weather System Follow-on – Microwave (WSF-M)

In FY25, the Space Force conducted three operational test events for the Weather System Follow-on – Microwave (WSF-M): the operational utility evaluation (OUE) completed in March 2025, the cooperative vulnerability and penetration assessment (CVPA) in April 2025, and the adversarial assessment (AA) in August 2025. The OUE and CVPA supported the Space Force's decision to operationally accept WSF-M and declare initial operational capability (IOC) in April 2025. The OUE, while limited in scope, allowed DOT&E to evaluate progress toward system operational effectiveness, suitability, and survivability. The FOT&E, planned for FY26, should provide the Space Force with adequate data for a full evaluation supporting a full operational capability (FOC) decision.

In July 2025, DOT&E removed the WSF-M program from oversight after the system completed the OUE and CVPA, as the satellite successfully demonstrated its on-orbit IOC.

SYSTEM DESCRIPTION

The WSF-M program is composed of three segments:

- The space segment consists of one Low Earth Orbit (LEO) weather satellite and one replenishment satellite, each equipped with a passive Microwave Imager (MWI) sensor and an Energetic Charged Particle (ECP) sensor. The WSF-M satellite hosts the ECP sensor as a government-furnished equipment developed by the Air Force Research Laboratory.
- The ground segment consists of the Satellite Operations Center, operated by the Naval Research Laboratory out of Blossom Point Tracking Facility (BPTF), in Blossom Point, Maryland. The ground segment also produced the software for processing MWI sensor data and the mission-unique software for command and control.
- The launch segment consists of the launch vehicle, launch support facilities, and launch services managed by the Space System Command's Assured Access to Space Program Office.

MISSION

The Space Force intends to use WSF-M to mitigate three DoW-identified capability gaps in space-based environmental monitoring: ocean surface vector winds, tropical cyclone intensity, and LEO ECPs. WSF-M also provides partial capability for three other gaps: snow depth, soil moisture, and sea ice characterization. The system replaces the microwave component of the DoW's aging LEO weather satellite enterprise.

PROGRAM

WSF-M is an Acquisition Category IB Major Defense Acquisition Program. DOT&E placed WSF-M under oversight in 2012. The first satellite successfully launched in April 2024.

The first WSF-M satellite achieved IOC in April 2025 and is currently providing data to operational users. In WSF-M's IOC configuration, the Navy's Fleet Numerical Meteorology and Oceanography Center (FNMOC) and Space Force Direct Readout Terminals (DRTs) receive WSF-M data. The WSF-M program competed its MWI sensor calibration and validation on the first satellite in June 2025 to support the system FOC in FY26.

When WSF-M reaches FOC, it will also provide data to the Air Force's 557th Weather Wing (557 WW). WSF-M will provide data to additional Service DRTs (under separate acquisition efforts) when they are available to receive the data, including the Marine Corps' Meteorological Mobile Facility Next Generation and the Navy's SMQ-11 (shipboard) and FMQ-27 (shore).

DOT&E approved the WSF-M pre-IOC TEMP in July 2023. In July 2025, DOT&E removed the WSF-M program from oversight, as the satellite successfully demonstrated its on-orbit IOC and the remaining activities no longer require DOT&E oversight.

» MAJOR CONTRACTOR

- BAE Systems, Inc. – Broomfield, Colorado

TEST ADEQUACY

The Space Force's 17th Test and Evaluation Squadron (17 TES) conducted an OUE of WSF-M from January – March 2025, at both BPTF and FNMOC. 17 TES was unable to conduct the OUE in accordance with the DOT&E-approved test plan due to a lapse in the authority to operate at the BPTF. The lapse paused testing for three days; however, this did not affect the test objectives or the adequacy of the OUE. Following the pause, 17 TES shifted the test toward observing operations and stopped directing operator actions. DOT&E did not observe the OUE but monitored it through the Space Force's daily test status updates. The OUE included program elements necessary to inform the Space Force's IOC decision. It focused on the on-orbit characteristics of the satellite, sensors, and data transmission process rather than the quality of the sensor data or of the subsequent weather products and forecasts.

17 TES, with the support of the 346th Test Squadron, conducted a cyber CVPA of WSF-M in April 2025, in accordance with the DOT&E-approved test plan. DOT&E observed the test. 17 TES, with the support of the 177th Information Aggressor Squadron, conducted an AA of WSF-M in August 2025. As WSF-M was removed from the DOT&E oversight list prior to the AA, the test plan was approved by Delta 12.

The OUE and CVPA were adequate for DOT&E to evaluate progress toward operational effectiveness, suitability, and survivability, which DOT&E will publish in a FY26 test report.

Once the 557 WW and representative DRT are ready to receive WSF-M data, FOT&E will focus on evaluating whether WSF-M effectively integrates into the DoW weather enterprise to mitigate the environmental monitoring capability gaps. As described in the DOT&E-approved TEMP, the Space Force will conduct an FOT&E to continue the evaluation of the system's operational effectiveness, suitability, and survivability. The FOT&E planned for FY26 should provide the Space Force with adequate data for a full evaluation.

PERFORMANCE

» EFFECTIVENESS

The WSF-M satellite demonstrated the capability to measure microwave and ECP activity on orbit and distribute the measurements to BPTF, and the microwave data further to FNMOC. Detailed findings can be found in DOT&E's forthcoming FY26 OUE test report.

17 TES identified two notable system deficiencies during the OUE, although both were already documented as limitations in the DOT&E-approved OUE test plan:

- WSF-M did not have a backup operations center in place if BPTF became non-mission capable. The WSF-M Program Office has funded plans of action to provide a minimum viable product Continuity of Operations Plan (COOP) to support the first WSF-M satellite. The COOP architecture is developed, and the Space Force expects completion by FY27; however, it will not be available in time to support FOT&E.
- BPTF could not distribute WSF-M ECP data in a manner usable by the 557 WW, which is the primary DoW ECP-data end user. For WSF-M ECP data to be used operationally, the data must be transferred to the Unified Data Library (UDL). During the OUE, the ECP data could not reach 557 WW through the UDL, but the WSF-M Program Office has since funded and implemented a solution. Currently, WSF-M's ECP data are being generated at BPTF and are available on the UDL for 557 WW to retrieve. FOT&E will reevaluate this capability.

» SUITABILITY

The OUE produced initial data on system reliability, availability, and maintainability (RAM) and data on usability from a survey of six operators, maintainers, and end users. The survey responses were mostly positive, with some critiques of training materials. The initial RAM data indicated that BPTF had challenges consistently contacting the satellite during its allotted contact timeframes. BPTF identified the cause as latency when issuing requests to contact, stemming from slower copper data lines. BPTF upgraded to faster fiber-optic data lines, which may improve the contact success rate. The improved contact success rate has not been validated through FOT&E.

» SURVIVABILITY

Cyber survivability findings from the WSF-M CVPA in April 2025, supported execution of the AA in August 2025.

RECOMMENDATIONS

The Space Force should:

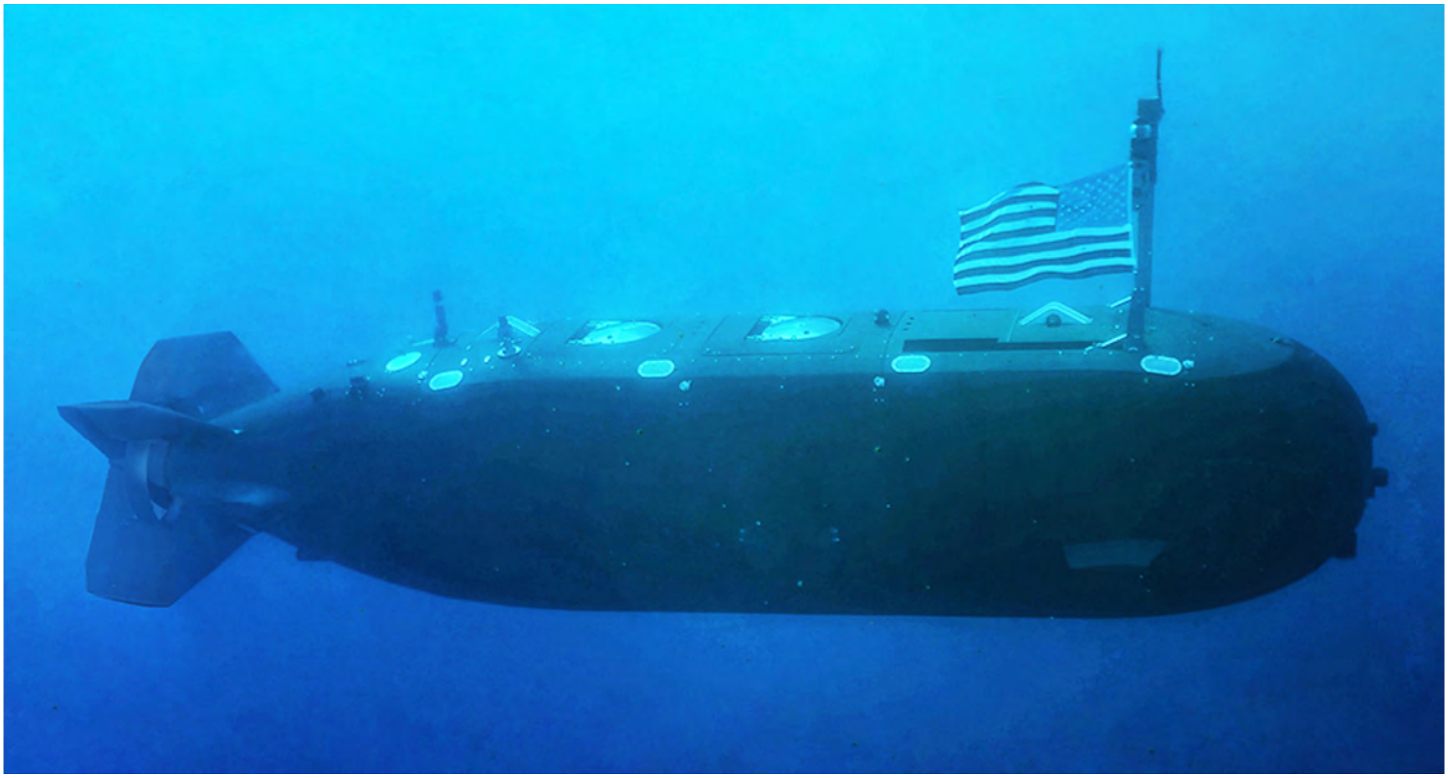
1. Ensure the WSF-M FOT&E includes FNMOC, 557 WW, and representative DRTs and that it covers the complete, end-to-end view of WSF-M data integration with the DoW weather enterprise from sensor data collection to weather products and forecasts.
2. Collect additional RAM data and sample a broader selection of survey respondents, including weather product consumers, during FOT&E, to support a full evaluation of operational suitability.
3. Reevaluate issue items from the OUE, such as the satellite contact success rate.
4. Implement a WSF-M COOP capability.
5. Ensure BPTF can transmit WSF-M ECP data to the 557 WW in an operationally usable manner.
6. Address all recommendations in the DOT&E's forthcoming OUE test report.

This page intentionally left blank.

U.S. SPECIAL OPERATIONS COMMAND PROGRAMS

This page intentionally left blank.

Dry Combat Submersible (DCS)



Dry Combat Submersible (DCS) FOT&E 2 started in July 2025 to test the platform's Integrated Bridge System (IBS). Cyber survivability testing was not performed in FOT&E 2, which DOT&E recommends performing in FY26. DOT&E will publish a classified FOT&E report following completion of cyber survivability testing.

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 has delivered three DCSs for SOF. The Navy completed the FOT&E 1 of the DCS in April 2024. DOT&E published a classified DCS FOT&E report in October 2024. The Navy started the FOT&E 2 on a new DCS IBS, the Platform Integrated Control System (PICS), in July 2025, and DOT&E will publish a second classified

FOT&E report after it completes cyber survivability testing.

» MAJOR CONTRACTOR

- Lockheed Martin Rotary and Mission Systems – Riviera Beach, Florida

TEST ADEQUACY

In July 2025, the Navy's Operational Test and Evaluation Force commenced a FOT&E 2. Testing focused on evaluating a new IBS for DCS, PICS, and was conducted in accordance with a DOT&E-approved test plan and with DOT&E observation. Cyber survivability testing of PICS is recommended at a separate event. DOT&E will publish a classified FOT&E report when cyber survivability testing completes.

PERFORMANCE

» EFFECTIVENESS

Operational effectiveness of the new IBS for DCS, PICS, is still being assessed. Previous assessments of DCS operational effectiveness were provided in the classified IOT&E and the FOT&E 1 reports of October 2023 and October 2024, respectively. DOT&E will address any updates to the operational effectiveness assessment in a second classified FOT&E report.

» SUITABILITY

DCS remains below the suitability threshold for some missions. Insufficient data are available from the FOT&E 1 to change the assessment from DCS IOT&E. Details are in the classified 2023 IOT&E report.

» SURVIVABILITY

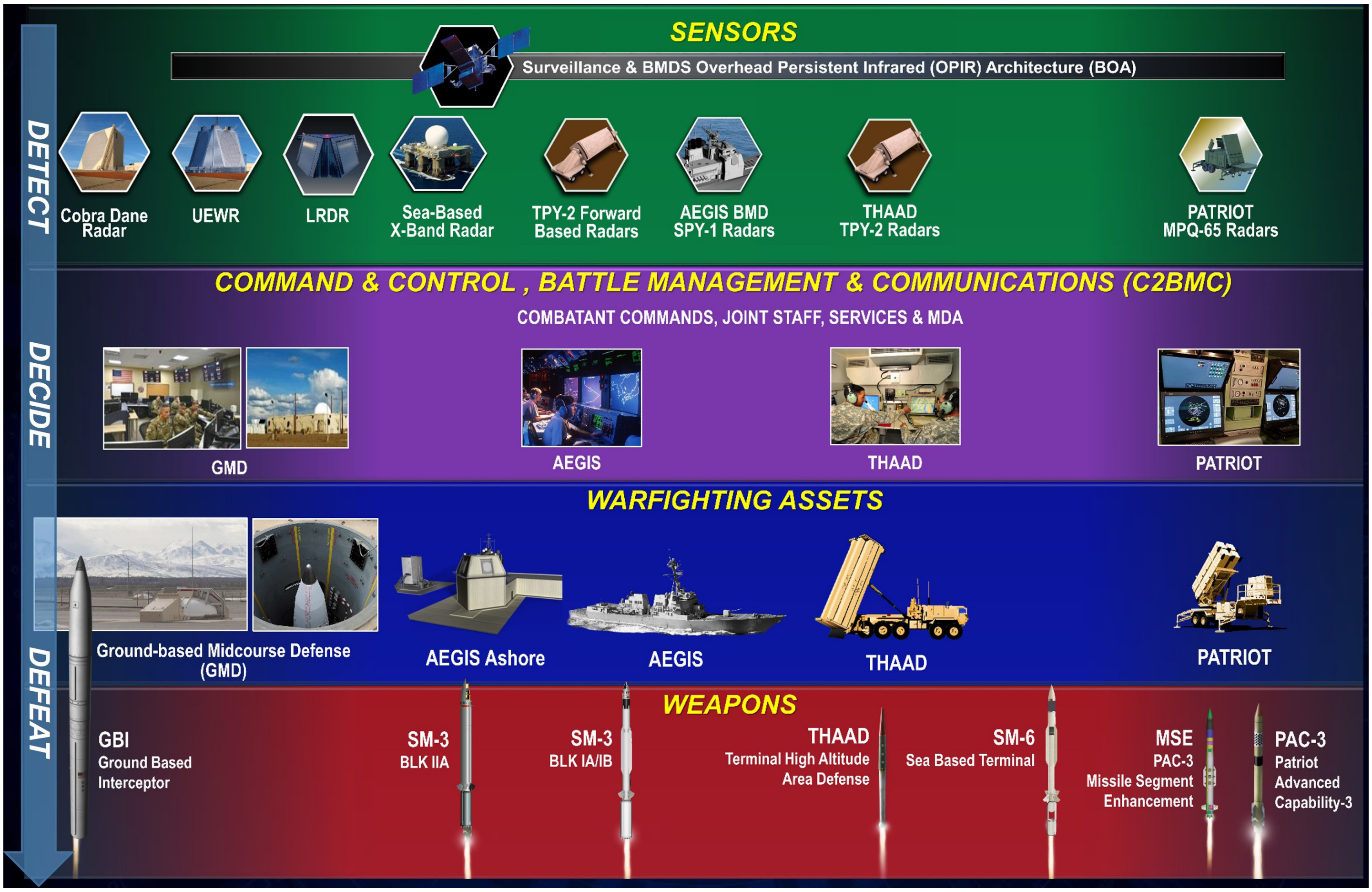
Cyber survivability of the new DCS IBS, PICS, will be assessed in the classified FOT&E 2 report following completion of testing.

RECOMMENDATIONS

USSOCOM should:

1. Continue to address the recommendations in the classified 2023 and 2024 IOT&E and FOT&E reports.
2. Perform FOT&E 2 cyber survivability testing on PICS.

MISSILE DEFENSE SYSTEM



BMD – Ballistic Missile Defense
BLK – Block
GBI – Ground-Based Interceptor
LRDR – Long Range Discrimination Radar
MPQ – Mobile, Position Locating Special Purpose
SM – Standard Missile
SPY – Surface Ship Radar Surveillance
THAAD – Terminal High Altitude Area Defense
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 employing simple countermeasures and with ranges greater than 3,000 kilometers, 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 from a small number of medium- or intermediate-range ballistic missile (MRBM or IRBM, respectively) threats with ranges less than 4,000 kilometers, and from 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 FY25, the Missile Defense Agency (MDA) flight tested or demonstrated in real-world events four significant new MDS capabilities:

- Ability of the Long Range Discrimination Radar (LRDR) to acquire and track a ballistic missile threat complex and report those data to the Command and Control, Battle Management, and Communications (C2BMC) system
- Sustained regional/theater operations in a wartime environment during the 12-day war between Iran and Israel.
- Initial ability of the Aegis Guam System (AGS) with an AN/TPY-6 radar to detect, track, engage, and intercept a MRBM target using a Standard Missile (SM)-3 Block IIA guided missile.
- Ability of Aegis Ballistic Missile Defense (BMD) to detect, track, and conduct a simulated engagement against a maneuvering hypersonic missile using its Sea-Based Terminal (SBT) Increment 3 capability.

DOT&E will provide additional information and recommendations in the classified DOT&E FY25 Assessment Report on the MDS to be published in February 2026.

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 seven 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, IRBM, and a limited number of LRBM 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 MDA and its international partner, the Japan Ministry of Defense, are proceeding with the Northrop Grumman Corporation's interceptor concept to continue development of the GPI.
		AGS[a]: Land-based Aegis BMD variant that will help defend Guam from ballistic and hypersonic threats using SM-3 and SM-6 guided missiles and data from on-island radars.	
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]:** 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 extends Aegis threat detection ranges and provides 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. **AN/TPY-6 Radar[a]:** S-band single-face transportable phased-array radar currently on Guam for potential inclusion in the Guam Defense System. Developed using the same technology as the LRDR.	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. **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. Prototype satellites participated in FY25 testing. **DSS[a]:** Space sensor that will track and discriminate objects in all phases of flight in support of the MDS. Currently in development. **PWSA[a]:** Network of space sensors and communication satellites to provide global communication and persistent fire control quality data of advanced missile threats, including hypersonic missile systems.		

Table 1. Elements of MDA's Missile Defense System, continued

Type	U.S. Homeland Defense	Global Regional/Theater Defense	Hypersonic Defense
C2	**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 and AN/TPY-2 (FBM) radars, and it 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.

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; C2 – Command and Control; C2BMC – Command and Control, Battle Management, and Communications; DSS – Discriminating Space Sensor; FBM – Forward-Based Mode; GMD – Ground-based Midcourse Defense; GBI – Ground-Based Interceptors; GPI – Glide Phase Intercept; 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; LRBM – Long-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; PWSA: Proliferated Warfighter Space Architecture; SBIRS – Space-Based Infrared System; SBT – Sea-Based Terminal; SBX – Sea-Based X-band Radar; 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, allies, and friends 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 six of its seven weapon elements (all but Patriot), most of its sensor architecture, and its command-and-control element. A subset of the MDS elements will comprise the Guam Defense System architecture. In FY25, the DoW began initial planning and development of the Golden Dome for America architecture, which will also include multiple elements of the MDS. In 2002, the Secretary of Defense granted the MDA nonstandard acquisition authorities for the MDS, which 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 MDA maintains responsibility for integrating all elements into the MDS whether or not the MDA developed the element. The MDA publishes a test plan update 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, which DOT&E reviews. DOT&E disapproved IMTP Version 26.1 in December 2024 because of a lack of flight test resources for future tests. In FY25, the MDA began revising the overall test approach, moving toward a high-cadence test program to address next-generation missile defense needs. This restructuring includes changes to the IMTP development process as well as many test event modifications and additions. DOT&E will review these ongoing changes throughout FY26.

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 achieved a conditional Milestone C and major capability acquisition program designation in February 2025. DOT&E approved the LTAMDS TEMP in March 2025. LTAMDS-specific test activities and assessments are provided in the LTAMDS article in this Annual Report.

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 Upgrade, five Upgraded Early Warning Radars (UEWRs), LRDR, and the Space-Based Infrared System (SBIRS) constellation. More details on SBIRS testing and assessments are in the SBIRS Survivable Endurable Evolution (S2E2) article in this Annual Report. The Air Force completed development and initial operational testing for the first three sensor systems prior to them becoming Space Force assets. The MDA completed development and initial operational testing for LRDR in FY25, and the Space Force anticipates operationally accepting LRDR in early FY26.

» MAJOR CONTRACTORS

- The Boeing Company
  - GMD Integration, Test and Readiness: Huntsville, Alabama
- Lockheed Martin Corporation
  - Aegis BMD, AAMDS, Aegis SBT, AGS, AN/SPY-1 radar, LRDR, AN/TPY-6, and Glide Phase Intercept (GPI) Weapons System: Moorestown, New Jersey
  - C2BMC: Huntsville, Alabama and Colorado Springs, Colorado
  - Next Generation Interceptor All-Up Round 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 missile: 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, and LTAMDS: 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 and DSS through Prototype Demonstration Phases: Fort Wayne, Indiana

TEST ADEQUACY

The MDA IMTP documents planned flight, ground (e.g., hardware-in-the-loop), and cyber survivability testing in support of operational capability declarations, as well as for the verification, validation, and accreditation of associated M&S. In FY25, the MDA conducted testing in accordance with the IMTP, although some events experienced technical and programmatic delays. Table 2 outlines the flight, ground, high-fidelity M&S, and cyber survivability test events that the MDA performed or participated in during FY25. 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. FY25 Missile Defense System Testing

Date	Test	Mission Area	Description
October 2024	GTD-08b (USNORTHCOM/ USINDOPACOM)[a,e]	Homeland Defense and Regional/Theater Defense	The MDA and the MDS OTA conducted this DT/OT using operational assets and HWIL test assets supporting MDS-level interoperability assessments in USNORTHCOM/USINDOPACOM geographic regions, with new Aegis BMD and AN/TPY-2 (FBM) functions.

Table 2. FY25 Missile Defense System Testing, continued

Date	Test	Mission Area	Description
October 2024	Cyber Test-08b Part 2 (N/I)[a,d]	Homeland Defense	The MDA conducted a CVPA and AA on the LRDR and C2BMC Spiral 8.2-5.1 as configured for USNORTHCOM defense, to assess cyber survivability via a CVPA and AA events.
December 2024	FEM-02[c,d]	Regional/Theater Defense	The MDA demonstrated an initial AGS capability with an AN/TPY-6 radar to detect and track an MRBM target, and to engage and intercept the target in the midcourse phase of flight using an SM-3 Block IIA guided missile. This was the first BMD event executed from Guam.
December 2024	Joint Flight Campaign Resolve[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.
January 2025	Hypersonic Test Bed-2[c,e]	Hypersonic Defense	The MDA and NSWC-PH conducted this experiment to collect data on the hypersonic environment. An HBTSS observed the rocket-launched hypersonic vehicle.
February 2025	GTI-08b Part 2 (USNORTHCOM/USINDOPACOM)[c,e]	Homeland Defense	The MDA conducted this DT/OT using HWIL test assets supporting MDS-level assessments of updates that were implemented to address findings from the FY24 GTI-08b test.
February 2025	Glory Trip 252[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.
March 2025	FTX-40[a,d]	Regional/Theater Defense	The MDA and Navy demonstrated an Aegis SBT Inc 3 capability to detect, track, and conduct a simulated SM-6 engagement against a maneuvering hypersonic target.
March 2025	GTI-101 (USEUCOM/USCENTCOM)[a,e]	Regional/Theater Defense	The MDA and the MDS OTA conducted this DT/OT using HWIL test assets supporting MDS-level assessments in USEUCOM/USCENTCOM geographic regions, with new Aegis BMD and AN/TPY-2 (FBM) functions.
April 2025	GTI-108 (THAAD)[a,e]	Regional/Theater Defense	The MDA conducted this DT using HWIL assets supporting MDS-level assessments in USCENTCOM geographic regions, with a focus on interoperability within new THAAD operational laydowns.
April 2025	Joint Flight Campaign-4[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.
April — May 2025	UEWR Clear AOC Upgrade[a,e]	Homeland Defense	STARCOM conducted M&S OT on the UEWR at Clear Air Force Base, to evaluate the operational effectiveness, suitability, and survivability, after installation of the AOC upgrade.
May 2025	At-Sea Demonstration/Formidable Shield-25[c,e]	Regional/Theater Defense	NATO forces executed a series of live fire IAMD exercises to build joint interoperability and demonstrate joint command and control in complex integrated air and missile defense scenarios. Two Aegis BMD destroyers detected, tracked, and engaged ballistic missile targets with SM-3 Block IA interceptors during the exercises.
May 2025	Glory Trip 253[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 2025	Live Radiate-26a[c,e]	Space Domain Awareness	The MDA conducted this event to assess MDS tasking and LRDR capability in support of the USSPACECOM space domain awareness mission while maintaining missile defense surveillance.

Table 2. FY25 Missile Defense System Testing, continued

Date	Test	Mission Area	Description
June 2025	FTX-26a[a,e]	Homeland Defense	The MDA demonstrated the LRDR's ability to acquire, track, and report missile data of an ICBM-representative target to C2BMC and GMD, which simulated an intercept.
June 2025	PCSB-1.0 DT Flight Test[c,e]	Regional/Theater Defense	The Army demonstrated the capability of the Patriot system, using PCSB-1.0, to search, detect, track, classify, engage, and kill a maneuvering surrogate ABT equipped with electronic attack using a PAC-3 MSE effector.
July 2025	Cyber Test-08b Part 2 (N/I) for AN/TPY-2[e]	Homeland Defense and Regional/Theater Defense	The MDA conducted a CVPA and AA on the AN/TPY-2 CX 5.0 software configuration on an operational radar to assess cyber survivability.
July 2025	UEWR Fylingdales CVPA[a,e]	Homeland Defense	STARCOM conducted a CVPA on the UEWR at RAF Fylingdales in the UK, to assess its cyber survivability from insider and nearsider threat postures.
August 2025	GTI-107 (USNORTHCOM)[a,e]	Homeland Defense	The MDA conducted this DT/OT using HWIL test assets to support MDS-level assessments in USNORTHCOM geographic regions with a focus on new LRDR capabilities.
September 2025	SBT Inc 2 M&S OT Runs for Record, Phase 3A Part 2[a,d]	Regional/Theater Defense	The MDA executed and delivered endgame and lethality results for a set of high-fidelity M&S OT runs for record to assess Aegis SBT Inc 2 organic engagement performance against select ballistic missile threats.
September 2025	SBT Inc 2 M&S OT Runs for Record, Phase 3C Part 1[a,d]	Regional/Theater Defense	The MDA executed and delivered Aegis Weapon System results for a set of high-fidelity M&S OT runs for record to assess Aegis SBT Inc 2 organic engagement performance against select ballistic missile and hypersonic threats.

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; ABT – Air-Breathing Threat; AGS – Aegis Guam System; AN/TPY - Army Navy/Transportable Radar Surveillance; AOC – Advanced Object Classification; BMD – Ballistic Missile Defense; C2BMC – Command and Control, Battle Management, and Communications; CVPA – Cooperative Vulnerability and Penetration Assessment; DT – Developmental Test; FBM – Forward-Based Mode; FEM – Flight Test Experiment Aegis Weapon System; FTX – Flight Test Other; FY – Fiscal Year; GMD – Ground-based Midcourse Defense; GTD – Ground Test Distributed; GTI – Ground Test Integrated; HBTSS – Hypersonic and Ballistic Tracking Space Sensor; HWIL – Hardware-in-the-Loop; IAMD – Integrated Air and Missile Defense; IBCS – Integrated Battle Command System; Inc – Increment; LRDR – Long Range Discrimination Radar; M&S – Modeling and Simulation; MDA – Missile Defense Agency; MDS – Missile Defense System; MRBM – Medium-Range Ballistic Missile; MSE – Missile Segment Enhancement; NSWC-PH – Naval Surface Warfare Center, Port Hueneme; OT – Operational Test; OTA – Operational Test Agency; PAC – Patriot Advanced Capability; PCSB – Patriot Component Software Build; RAF – Royal Air Force; SBT – Sea-Based Terminal; SM – Standard Missile; STARCOM – Space Training and Readiness Command; THAAD – Terminal High Altitude Area Defense; UEWR – Upgraded Early Warning Radar; UK – United Kingdom; 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

In FY25, the MDA also conducted an extensive analysis on MDS performance in real-world events. The analysis has proven highly valuable in assessing system performance, developing software and concept of operations improvements, and identifying features that should be added to the test program.

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 DOT&E in completing a comprehensive assessment of the MDS. Specifically:

- 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 faster than the pace of flight test target and ground test high-fidelity M&S threat model development. The MDA should also continue investigating parametric targets so the extent of potential threat variations can be explored quickly and methodically.
- Independent accreditations of M&S used in ground tests and high-fidelity analyses are needed to ensure M&S can adequately represent current threat missile capabilities, including electronic attack, countermeasures, 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, such as validation of post-intercept debris models and an accredited model for Patriot. Also, as threat and system model capabilities become more complex, the MDA has sometimes struggled to maintain a real-time test architecture that can handle this complexity. The MDA partially addressed this increase in complexity in FY25 by performing a risk reduction event preceding the current ground test campaign, which allowed the MDA to identify many integration problems before formal testing began. Integration will remain an ongoing concern as more complex capabilities are added to the MDS, such as the Next Generation Interceptor (NGI) and the Glide Phase Intercept (GPI). Finally, as a complement to the real-time testing, the MDA had been developing an End-to-End Digital Integrated System-Level Simulation, which was an MDS-level high-fidelity digital modeling architecture needed to assess effectiveness of the MDS. In FY24, the MDA removed funding from the effort, and no funding was restored in FY25. The 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 delays in other non-cyber tests, element unavailability, or elements that the MDA later deems untestable in their current configuration. The MDA, in coordination with the Services and MDS OTA, should continue to work to overcome these test planning challenges. Additionally, MDA and OTAs should continue to aggregate element-level cyber survivability data to support MDS-level cyber survivability assessment.
- Flight and ground test programs and high-fidelity M&S analyses at both the MDS- 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 since the DOT&E FY22 Annual Report, the MDA often designs flight tests to demonstrate a specific new capability rather than for operational realism. Operationally realistic intercept flight tests are necessary to provide: (1) needed referent data to support verification, validation, and accreditation 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.
- In coordination with DOT&E, the Guam Defense System Joint Program Office (JPO), Army, Navy, and MDA continue efforts to develop a T&E concept for the Guam Defense System, which is intended to provide persistent, 360-degree, layered, and integrated air and missile defense. The proposed architecture is made of both new and existing components in close proximity and with overlapping areas of regard, with all components working together to defend against cruise, ballistic, and hypersonic missile threats. This architecture presents a significant integration and test planning challenge. The JPO has enumerated significant data gaps that need to be filled to adequately inform the warfighter of system capabilities for interoperability and engagement planning. Test data should be collected through ground testing, digital M&S, tracking exercises, and intercept flight testing. Comprehensive suitability and cyber tests are also needed. The JPO is facing significant test resource shortfalls to close these data gaps.

- Flight and ground test infrastructure modernization efforts are needed to increase range capability and throughput to meet the projected increase in the tempo of missile defense testing. Developing and maintaining more long-range flight test corridors and mobile data collection assets will be essential to testing going forward. Progress was made in FY25, when the MDA received funding for the full replacement of a major test resource ship needed for adequate flight testing, and partial funding for a second ship and shipboard radar. The MDA intends to budget the additional required funds in future Program Objective Memorandum submissions. The MDA's current acquisition plan calls for full operational capability of the ships in FY30 and FY31. This funding of the ships resolves one of the major reasons DOT&E disapproved IMTP 26.1.

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 FY25, the MDA demonstrated new capabilities of LRDR and C2BMC when the radar successfully acquired, tracked, and reported a missile complex to C2BMC. GMD used the LRDR and C2BMC data to simulate an engagement.

» 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.

Fielded Aegis BMD variants continue to demonstrate 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. Aegis BMD destroyers engaged Iranian ballistic missile threats targeting Israel in both FY24 and FY25. In December 2024, the MDA demonstrated, for the first time, that the initial build of the AGS has a capability to intercept a ballistic missile using radar data from a single-face AN/TPY-6 radar. However, further development and testing of that system is needed to integrate it with the broader Guam Defense System, which consists of a number of Service components and addresses a complicated threat set with ballistic, hypersonic, and cruise missiles. Aegis BMD also continues to demonstrate a capability to intercept ballistic missile threats in the terminal phase of flight with its SBT capability with SM-6 guided missiles. In FY26, the MDA plans to conduct first-time flight tests with the new Aegis Flight III destroyer, USS *Jack H. Lucas* (DDG 125), to include an intercept attempt.

The Terminal High Altitude Area Defense (THAAD) system has demonstrated the capability to intercept and destroy ballistic missiles of short- to intermediate-range inside or outside the earth's atmosphere during the terminal phase of flight. In FY25, THAAD participated in the defense of Israel, demonstrating capability against Iranian and Houthi missile threats. However, flight testing and M&S still need to address more complex engagement conditions and raid scenarios. 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 in response to real-world events, but these updates should undergo appropriate operational testing. The THAAD 5.0 build, consisting of new hardware and software, started testing in FY25. 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 surveillance air assets. Patriot systems have participated in the defense of Ukraine against Russian threats. However, DOT&E does not have access to the U.S. Army's data to assess Patriot's performance. In the 12-day war between Iran and Israel, Iran launched a salvo of missiles at Al Udeid Air Base, Qatar, where Patriot showed some capability in defending against a raid scenario. The Patriot program is developing the Patriot Component Software Build 1.0 and will begin operational testing in FY26.

AN/TPY-2 Forward-Based Mode (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, and one or more AN/TPY-6 radars may contribute to the defense of Guam. In FY25, the AN/TPY-2 (FBM) radars continued to participate in the defense of Israel, demonstrating tracking capacity against Iranian and Houthi threats in raid environments. Also in FY25, AN/SPY-1 demonstrated the capability to detect, track, and discriminate a hypersonic vehicle during a live target tracking event. 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. However, USS *Jack H. Lucas*, the first Aegis Flight III destroyer with Aegis Baseline 10 and AN/SPY-6(V)1 radar, did not participate in MDA flight tests in FY25. The AN/TPY-6 radar on Guam detected and tracked a ballistic missile for the first time in FY25.

» HYPERSONIC MISSILE DEFENSE

The MDA collected hypersonic test data throughout FY25 to inform future sensor design, sensor detection and tracking algorithms, and M&S validation. The MDA also conducted ground optical, thermal, and aerodynamic testing to support the development of new technologies and the M&S architecture specifically for hypersonic missile defense. In FY25, results from flight testing and high-fidelity M&S demonstrated an Aegis SBT capability to engage select hypersonic missile threats in the terminal phase of flight. During the flight test, the Aegis SBT capability detected, tracked, and conducted a simulated engagement against a hypersonic target as a risk reduction exercise for a planned live SM-6 intercept of a hypersonic target.

» COMMAND AND CONTROL AND SPACE SENSORS

Almost every test the MDA conducted in FY25 included space sensors acquiring, tracking, and reporting on observed objects. A prototype Hypersonic and Ballistic Tracking Space Sensor (HBTSS) continued data collection on hypersonic targets. 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 FY25, 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 FY25, C2BMC communicated with Space Command and Control (Space C2) for space domain awareness, tasking LRDR and receiving reports back from the radars on resident space objects. In FY25, the MDA demonstrated new capabilities of LRDR and C2BMC when the radar successfully reported a missile complex to C2BMC, which was then sent to GMD. During real-world events, BOA and OPIR assets contributed to situational awareness, and C2BMC relayed threat information between assets in stressing scenarios.

» SUMMARY

DOT&E will provide additional information and recommendations in the classified FY25 Assessment Report on the MDS to be published in February 2026.

RECOMMENDATIONS

The MDA should:

1. Continue to increase the rate of U.S. homeland defense and regional/theater target and threat model development to keep pace with emerging real-world threats, as recommended in the FY23 and FY24 Annual Reports, and continue to pursue the creation of parametric threats in ground testing that allow for threat variations in testing.
2. Continue to prioritize independent accreditation of M&S used in ground tests and high-fidelity analyses and ensure M&S can adequately represent current threat capabilities, electronic attack, countermeasures, post-intercept debris, and realistic raid sizes, as recommended in the FY24 Annual Report.
3. Continue investments in ground test architecture improvements to accommodate more complex threat and system model features, as recommended in the FY24 Annual Report.
4. Fund and develop an MDS-level digital integrated simulation, to allow quantitative assessments of both current MDS capability as well as more complex future capabilities that will require such

a capability, like NGI, GPI, and the Guam Defense System.

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 verification, validation, and accreditation of the models representing post-intercept debris, as recommended in the FY24 Annual Report.
6. Conduct high-fidelity M&S runs for record with independently accredited M&S to assess individual weapon system and MDS-level effectiveness against emerging threats, as recommended in the FY24 Annual Report.
7. Prioritize working within the DoW to ensure test resources are available for the higher cadence and more demanding flight and ground tests planned for the future.
8. Ensure comprehensive cyber T&E plans are created and developmental and operational cyber testing is completed prior to capability delivery of MDS element and interceptor builds to the warfighter, as recommended in the FY24 Annual Report.
9. Conduct routine operational cyber survivability assessments with multiple elements, warfighter participation, and federated M&S accredited for performance, as recommended in the FY24 Annual Report.

The Army, in coordination with the MDA, should:

1. Continue to develop Patriot and LTAMDS models that interface properly with the MDS ground test architecture to address current shortfalls in supporting MDS-level performance assessments. Verification, validation, and accreditation efforts for the models should be fully funded.
2. Coordinate with the Navy and other DoW stakeholders to ensure the test strategy for the Guam Defense System is sufficiently funded to incorporate multi-element interoperability into intercept flight testing, tracking exercises, ground testing, and digital M&S, as recommended in the FY23 and FY24 Annual Reports. Additionally, ensure comprehensive MDS-level suitability and cyber testing is planned.

DOT&E-MANAGED ACTIVITIES

This page intentionally left blank.

Center for Countermeasures (CCM)

In FY25, the Center for Countermeasures (CCM) performed 49 events in support of assessing the following: (1) counter-unmanned aircraft systems (C-UASs), (2) directed energy weapons (DEWs), (3) aircraft- and ground vehicle-based countermeasures (CMs), (4) experimentation initiatives, (5) U.S. Indo-Pacific Command (USINDOPACOM) training exercises, (6) data collection for threat characterization to advance the threat CMs development and testing, and (7) fielding of unique instrumentation for CM testing. CCM also partnered with allies on project arrangements to advance the T&E of infrared (IR) and radio frequency (RF) threat CMs.

PROGRAM OVERVIEW

CCM was established and chartered in 1972 by the Office of the Secretary of Defense to address the emergence of technologically advanced weapons systems, including the rapid development of terminally guided weapons and CMs. CCM operates and deploys mobile instrumentation capable of simulating an array of threats to measure and evaluate the operational effectiveness of CMs employed by DoW and foreign weapon systems. The portability of CCM's unique instrumentation capabilities and personnel provides the agility and efficiency required by DoW to develop and field critical DoW systems 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 by supporting T&E and experimentation activities with portable instrumentation. CCM consistently aligns its mission focus to support current DoW priorities and prepares for future T&E and experimentation with new and emerging technologies. CCM also provides the threat environment for pre-deployment training to ensure warfighters are trained in combat-representative environments.

FY25 KEY ACTIVITIES

» C-UAS T&E

CCM supported the Air Force with demonstrating capabilities in a contested, operationally representative environment to combat ever-evolving UAS threats. The demonstration evaluated the ability to detect, track, and engage with various rocket systems. The test also evaluated the utility terrain vehicle operator safety for alternate systems. CCM contributed to the event by providing certified UAS pilots to demonstrate various tactical capabilities during the exercise.

Decoys Deployed as Targets During Technology Readiness Experimentation (T-REX) UAS Experiment 2025

» DEW T&E

CCM supported the rapid capabilities development and fielding of prototype DEWs and made significant progress in equipping the DoW with the tools and methods needed to adequately test and evaluate the operational effectiveness of DEWs and directed energy (DE)-based CMs. CCM supported nine DE test events for the following programs:

Army Multi-Purpose High Energy Laser (AMP-HEL)

CCM supported the Army Rapid Capabilities and Critical Technologies Office (RCCTO) with conducting two government acceptance tests (GATs) by providing ground-based and aerial-beam characterization target boards. RCCTO used one GAT to evaluate AMP-HEL unit 2 and another GAT to evaluate AMP-HEL unit 3. Additionally, the Palletized High Energy Laser (HEL) 4 system was used in each test to collect risk reduction data for another RCCTO project. The results of this event informed the Army's assessment and provided baseline characteristics of the laser system before delivery.

Probability of Weapon Effectiveness Demonstration

As part of OUSW(R&E)-led efforts, CCM supported two tests with a series of dynamic HEL engagements as part of the Probability of Weapon Effectiveness Experiment 2.0 effort in which a HEL engaged target pods mounted on the wingtips of a BQM-34 drone.

Mjölnir Tactical High Power Operational Responder (THOR)

During the Mjölnir risk reduction test, CCM supported the Air Force by providing the High-Power Microwave (HPM) Beam Evaluation Tool system. The test assessed the Mjölnir's upgrades by using the THOR HPM beam boresight as a testbed.

High Energy Laser with Integrated Optical Dazzler and Surveillance (HELIOS)

CCM supported the Navy with two in-port firing calibration events and one at-sea calibration event for the HELIOS – a 60-kilowatt laser weapon system; sensor suite; and counterintelligence, surveillance, and reconnaissance naval capability. CCM assisted with testing the HELIOS beam director, alignment procedures, equipment operations, and data reduction. The test series was conducted in anticipation of a C-UAS live-fire engagement event.

Defense Advanced Research Projects Agency (DARPA) Persistent Optical Wireless Energy Relay (POWER) Receiver Array Demonstration Program

CCM supported the DARPA POWER Receiver Array Demonstration to showcase an optical power-beaming receiver designed to enable faster and more reliable wireless energy transmission over extended distances. Laser power measurements were collected and provided in real-time at varying distances to compare with the power captured by the receiver array.

» AIRCRAFT AND GROUND VEHICLE PROTECTION SYSTEMS T&E

CCM supported over 25 test events in support of aircraft and ground vehicle 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. CCM supported these events by providing a combination of missile threat simulators, RF threat emitters, and laser systems to assist in presenting a threat environment. CCM also collected data with radiometric instrumentation to characterize CM responses. Testing included the following:

CH-53K King Stallion Aircraft

CCM supported the Navy's H-53 Heavy Lift Helicopters Program Office (PMA-261) with an evaluation of the Large Aircraft Infrared Countermeasures (LAIRCM) Advanced Threat Warning (ATW) system installed on CH-53K aircraft.

MH-139A Grey Wolf Aircraft

CCM supported the Air Force's in-flight demonstration assessing the performance of the AN/AAR-47 Missile Approach Warning System and the AN/ALE-47 Airborne Countermeasure Dispenser System installed on MH-139A Grey Wolf aircraft. CCM also provided threat simulations and static threat seekers to test the system's responsiveness and defensive capability to defeat incoming threats during MH-139A IOT&E events.

Distributed Aperture Infrared Countermeasure (DAIRCM)

CCM participated in the following DAIRCM T&E events:

- CCM supported the Air Force and Joint Special Operations Command's quick reaction capability flight test to evaluate the DAIRCM's performance characteristics in an operational environment.
- CCM supported the Army's 160th Special Operations Aviation Regiment (SOAR) with the evaluation of the DAIRCM's software upgrade installed on MH-6 aircraft. The event was in support of efforts to improve and evaluate system safety, airworthiness, and survivability for a rotary-wing aircraft upgrade.
- CCM supported the Navy with evaluating DAIRCM software integrated into UH-1Y aircraft. Testing produced data to assist the Navy with evaluating the DAIRCM during combat utility helicopter missions.

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

CCM supported the Army's FOT&E to assess the effectiveness of the AN/APR-39E(V)2 radar warning receiver installed on AH-64E aircraft in operationally relevant conditions.

Next Generation Electro-Optical (EO) Distributed Aperture System

CCM supported the Joint Program Office (JPO) in testing the next generation EO Distributed Aperture System missile warning system installed on F-35 aircraft. CCM provided the remote launching of various man-portable air defense system (MANPADS) assets.

Improved Threat Detection System (ITDS)

CCM supported the Army's ITDS program with characterization and data collection for two potential future missile warning system sensors in open-air environments, during the down-selection process. Once the down-selection occurred, CCM supported flight testing to support the Army's evaluation of the ITDS.

Advanced Layered Soft-Kill System

CCM supported the Army's science and technology evaluation of the threat detection and response subsystems installed on a Bradley Fighting Vehicle to ensure that it detected and declared threats as intended.

Common Infrared Countermeasure (CIRCM)

CCM participated in the following CIRCM T&E events:

- In support of the Army's 160th SOAR, CCM supported the software upgrade testing of the CIRCM ATW system, as installed on MH-47G and MH-60M aircraft, to evaluate and improve system performance.
- CCM supported the Army's assessment of the Limited Interim Missile Warning System (LIMWS) CH-47F aircraft's updated sensor fairing integration and sensor coverage regions, to substantiate airworthiness and safety. CCM further supported a flight test to assess the performance of LIMWS software on the CH-47F equipped with updated sensor fairing.
- CCM supported the Army with assessing the CIRCM's ability to slew, acquire, track, and emit laser energy on a threat when provided a threat handoff from the Common Missile Warning System as integrated on a UH-60V aircraft.

» EXPERIMENTATION

CCM participated in five experimentation events that advanced prototyping and facilitated multi-national collaboration and international security.

OUSW(R&E) Joint Rapid Experiment

CCM supported the OUSW(R&E) of Prototyping and Experimentation (P&E) to meet the needs of the warfighter for rapid development of long-range fires technologies and systems, as well as assessing the DoW's ability to address the expanding C-UAS mission with kinetic-kill weapons and DEWs. CCM supported the following:

- **Low-Cost Short-Range Air Defense (L-SHORAD)** – CCM supported the Prototype Integration Experimentation Event, L-SHORAD. This event measured the effectiveness of fusing inputs from multiple passive and active sensors to enhance detection range and track accuracy for identifying and destroying multiple adversary UAS targets.
- **Technology Readiness Experimentation (T-REX) 2025** – CCM supported the T-REX 25-2 event, which showcased industry's emerging technologies, including resilient communications, autonomous systems, and C-UAS capabilities. CCM supported the First-Person-View Top Drone Challenge, which brought together DoW and industry drone technologies and teams to compete in air combat scenarios through multiple target identification objectives. CCM provided inflatable decoys to support real-time visual target acquisition, identification, and recognition techniques across diverse domains and terrains.
- **CRIMSON DRAGON 2025** – CCM supported the prototype live-fire experiment, CRIMSON DRAGON. This live-fire event focused on the sea point of departure defense venues against all-domain maritime air-and-sea threats in an instrumented, relevant, fully informed threat environment and long-range fire solutions against amphibious assault in support of delivering innovative warfighter capabilities.

FALCON PEAK 25.2

FALCON PEAK organizes counter-small UAS (C-sUAS) experiments to gather data and observations on existing capabilities that support North American Aerospace Defense Command (NORAD) and U.S. Northern Command (USNORTHCOM) homeland defense C-sUAS objectives. CCM provided data collection instrumentation to support the assessment of existing C-sUAS capabilities.

Maneuver and Fires Integration Experiment 25

CCM supported the Army's C-UAS experiment with integrated fires to inform the Army Capabilities Development Directorate, Air and Missile Defense Cross Functional Team, Long Range Precision Fires Cross Functional Team, Air Defense Artillery Commandant, and community efforts in identifying critical capability needs for future operations at Fort Sill, Oklahoma. This experiment determined if technologies exist that can address capability gaps and determine the progress of these technologies toward fielding and pursuing technology transformation and innovation for a future force.

» USINDOPACOM FIELD EXERCISES AND WARFIGHTER TRAINING

CCM deployed its instrumentation systems and threat assets – such as a missile simulator, an instrumented MANPADS surrogate system, decoys, and an RF-threat simulator – to support five warfighter training exercises. CCM provided data to the trainers to assist with their evaluation of tactics, techniques, and procedures (TTP) employed by participating units to enhance their survivability in a combat-representative environment.

COBRA GOLD 2025 (CG25)

CG25 is an annual USINDOPACOM and Royal Thai Armed Forces co-sponsored international training exercise conducted in Thailand. It is designed to improve multi-national interoperability, effective planning, and executing complex multi-national operations. In support of improving warfighter survivability and military TTP, CCM provided surface-to-air missile targets for the demonstrated system. Training teams conducted the engagements during the CG25 live-fire events to assess the entire kill chain mission scenario objectives.

GARUDA SHIELD 2025

CCM participated in GARUDA SHIELD 2025, an annual multi-national, Indonesia-led USINDOPACOM military exercise that emphasizes interoperability and multi-domain warfare capabilities through training and cultural exchange. CCM provided several RF threat surface-to-air missile targets for a live-fire engagement to assess kill-chain coordination.

EMERALD WARRIOR 2025

CCM supported EMERALD WARRIOR 2025, an annual exercise led by the U.S. Special Operations Command (USSOCOM) and conducted by the Air Force Special Operations Command. CCM contributed to the command objective by providing a threat environment consisting of RF and IR surrogate threats and targets to support threat identification, reaction, CMs, and evasive maneuvers training.

160th SOAR Exercises

CCM supported two Army 160th SOAR exercises. CCM provided a missile simulator to emulate threat-representative IR missile signatures against a DAIRCM-equipped aircraft.

» THREAT SIGNATURE DATA COLLECTION

CCM collected radiometric data on threat missile and UAS platform signatures and provided the data to model developers for inclusion in their model databases. Advancing modeling and simulation (M&S) is critical for accurately representing adversary threats and for using hardware-in-the-loop testing to evaluate missile warning and CM T&E. CCM supported two threat signature data collection events.

UAS Signature Collection

CCM supported the Army by collecting radiometric data on Groups 4 and 5 UAS engines under various conditions. The UAS signature data will be used in the creation of flight profiles and development of models for M&S evaluation.

Static Motor Burn Signature Collection

CCM supported the Defense Intelligence Agency (DIA) Missile and Space Intelligence Center with collecting threat motor burn data. CCM provided spectrometers and hyperspectral imagers to collect radiometric data from various distances and aspect angles. The collected signature data will be used for future threat M&S development and enhancements.

» TEST INSTRUMENTATION INITIATIVES

CCM continued to enhance and modernize instrumentation and capabilities to meet the evolving demands of T&E. These efforts are critical to accelerating the testing, development, and fielding of CMs needed to survive in increasingly complex, multi-domain environments.

DE-based Projects to Fulfill T&E Instrumentation Capability Gaps

CCM conducted or supported developmental and acceptance testing for the following joint DE T&E tools and instrumentation:

- HEL beam capture and safe heat dissipation instrumentation to provide a backstop for HEL testing.
- UAS-mounted HPM instrumentation for measurement and characterization of HPM beam on target.
- Static beam evaluation tools for providing relative field mapping at source-to-target distances and visual determination of HPM system beam profiles for test decision-making, verification of safety constraints, and compliance with rules of engagement.
- Classes 1 and 2 UAS threat targets for DE and C-UAS experimental prototype demonstrations.

Joint Standard Instrumentation Suite (JSIS)

The JSIS is a collection of instrumentation developed to capture radiometric missile and hostile fire signatures; six-degrees-of-freedom attitude data; and time, space, position information during live-fire events. Data collected by JSIS supports DIA's threat model development for use in missile warning and CM system development and evaluation. JSIS reached its full operational capability and broadened its traditional mission area to begin collecting imagery and scoring data to support C-UAS, one-way attack, and autonomous systems T&E and experimentation events.

» SUPPORTING PROJECT ARRANGEMENT WITH ALLIES TO ADVANCE CM T&E

CCM and the Test and Evaluation Threat Resource Activity (TETRA) continued to support the execution of the Australia, Canada, Great Britain, and United States Airborne Electronic Warfare Cooperative T&E Project Arrangement (Air EW CTE PA), intended to advance and standardize coalition airborne EW T&E capabilities. CCM helped the Air EW CTE PA accomplish the following:

- Completed the Non-imaging Missile Approach Warning System model.
- Conducted a trial in Australia to perform a series of chaff-optimization and RF-jamming technique evaluations.
- Conducted a trial in the United States to perform a battlespace-wide analysis of Blue Force Air EW system of system (SoS) and CMs against sophisticated Red Integrated Air Defense System using newly developed, coherent M&S SoS architectural design.
- Conducted a trial in Canada to test advancements of an EO/IR M&S tool and its integration with the Integrated Threat Analysis and Simulation Environment.
- Conducted the annual collaborative T&E trial to assess M&S blue systems' (aircraft and CMs) abilities to disrupt and/or delay threat early warning, survive pop-up medium-range threats, and conduct and survive a strike mission within a long-range weapons engagement zone.

Cyber Assessment Program (CAP)

In FY25, the DOT&E Cyber Assessment Program (CAP) continued an active program of threat-representative cyber assessments during combatant command (CCMD) and Service exercises, Cyber Readiness Campaigns (CRCs), and targeted special assessments. CAP supported more than 70 assessment events of three types: exercises with cyber-threat representation to identify mission risks and help warfighters train in a threat-representative environment; cooperative events to identify and mitigate vulnerabilities; and focused technology assessments with broad benefits and implications for the DoW. CAP provided resources for DoW Cyber Red Teams (DCRTs) to emulate advanced adversaries, which is essential for CAP to assess warfighter ability to sustain critical missions in a contested environment. This threat emulation also enables warfighters to perform effective mission rehearsals and practice performing missions in degraded environments.

During FY25, DOT&E observed the rapid evolution and deployment of emerging technologies into the hands of the warfighters for experimentation with capabilities that offer new levels of synergy. CAP continued to observe that cross-system and cross-network interdependencies magnify risks from local vulnerabilities and reinforce the need for enterprise-level defensive strategies, robust global identity management, and Zero Trust strategies and technologies. The DoW's increased reliance on cloud and other warfighter-enabling technologies allows unprecedented data sharing and efficiencies, but it has also allowed warfighters to concentrate cyber risks from multiple missions onto a shared infrastructure. New systems being fielded to the tactical edge and to partner networks need continuous vulnerability monitoring in addition to the active and passive defenses across the entire DoW enterprise. CAP is well positioned to assess and help track the evolution of evolving capabilities, and, when appropriate, bring advanced threat emulation into assessments of system and warfighter performance in realistic conditions.

At the same time, the Services and CCMDs are continuing to field new defensive capabilities, including Defensive Cyberspace Operations (DCO) toolkits and sensors. In numerous instances, CAP has partnered with developers and network owners to provide threat-representative assessments that indicate how well these new capabilities detect and characterize a cyber adversary's activities, and that identify new sensor tuning strategies or detection tactics, techniques, and procedures. CAP assessments have also identified – and found remediations for – gaps in post-detection incident reporting, organizational coordination, and responses. Notably, CAP provided six assessment reports to the Joint Fires Network (JFN) program that identified potential vulnerabilities and supported early remediation of problems, accelerating developer exposure to real-world issues and reducing adversary attack vectors. CAP also observed that DCRTs are finding it harder to gain and retain access, and that DCRTs need to be better resourced to increase both their capabilities and capacity to perform mission-enhancing assessment for warfighters.

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.

CAP resources DCRTs to emulate realistic adversaries during major CCMD and Service exercises. DCRTs add required threat realism for assessment venues and help warfighters improve their ability to fight through cyber-attacks and accomplish critical missions.

CAP also provides resources to assessment teams from the operational test agencies (OTAs) and federally funded research and development centers (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 CRCs that include non-exercise events to examine specific elements of warfighter missions and defenses. These CRC events may include pre-exercise DCRT activities to position themselves as a near-peer adversary would, 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 analyses of DoW cyber capabilities via assessments of DCO and Offensive Cyberspace Operations (OCO) of the Services and CCMDs. Through these assessment efforts, DOT&E supports and advocates for improvements in DoW'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 recommend future investments and operations.

FY25 KEY ACTIVITIES

FY25 key activities spanned CCMD Tier 1 exercise assessments and CRCs, Service-level campaigns, and special assessments focused on warfighter priorities and emerging cyber-threat technologies and challenges.

» CCMD ASSESSMENTS

In FY25, CAP conducted CRCs culminating in exercise assessments at multiple CCMDs, with a focus on the Joint Staff–led ELITE CONSTELLATION combined exercise. CAP conducted at least some assessment activity at every CCMD, with classified results provided to the network or mission owners, and partnered to identify remediation options when appropriate. DOT&E assessed each CCMD's ability to react and respond to cyber threats while sustaining operational mission requirements. CCMDs remained cautious with exercise injects that carry higher risk to training objectives, but they continued to allow controlled, low-impact effects to emulate realistic threat scenarios. CCMDs remained receptive to CAP's mission assurance focus, particularly the emphasis on creating realistic contested cyber environments to generate assessable impacts to missions.

CRCs also included technical assessments of mission partner environments, air defense capabilities, tactical communications (unclassified and classified), enterprise data stores, C2 networks, and more at the request of the respective CCMDs. CAP provided vulnerability results to the system and network owners and partnered with them to identify remediations or mitigations.

When conducting technical and mission assurance assessments, CAP often observed gaps in cyber intelligence fusion and cyber incident reporting and response processes. Findings, process improvements, and mitigations in these areas remain vital to improving the overall cyber warfighting posture of the DoW. In FY25, CAP observed and reported deficiencies in the reporting and classification of shipboard cyber incidents, in cross-Service cyber intelligence dissemination within CCMD areas of responsibility, and in operational cyber incident reporting channels for highly classified or sensitive networks. The DoW is acquiring various tools to help provide cyber situational awareness and unified C2. CAP will continue to monitor these tools as they are developed and deployed.

Observations during multiple exercises also revealed gaps in the processes to deploy Cyber Protection Teams, disseminate cyber reporting and intelligence, and perform overall C2 of cyber forces. To address these findings, CAP partnered with DoW Cyber Defense Command (DCDC) to execute the Cyber Maneuver, Operations, and Combat Knowledge Wargame (CMOCKW), which focused on the DoW's operational decision-making in cyberspace. DCDC used the output of CMOCKW to help refine their decision support matrices, identify gaps in education and planning, and revise their operational approach.

In planning for FY26 assessments, CAP continues to emphasize greater realism, operational relevance, and mission impact analysis.

» SERVICE ASSESSMENTS

Air Force

In FY25, DOT&E completed a multiyear assessment of the Air Force research and development (R&D) mission, with a focus on the Air Force Network (AFNET) and Air Force Network – Secret (AFNET-S) within a specific Air Force complex. CAP assessed the risks of cyber threats to the Air Force R&D mission during the competition and steady-state phase that precedes direct conflict, identified data exposure vulnerabilities, and partnered with the Air Force for remediation.

Prior to expanding the deployment of the Air Force's Enterprise-Information Technology (IT)-as-a-Service (EITaaS) system from the initial bases to the entire Department of the Air Force (DAF) enterprise, 16th Air Force (16AF) sought DOT&E's input to determine the associated risks. The outcome of this assessment informed the 16AF Commander's approval of the expansion of EITaaS to the entire DAF enterprise.

CAP partnered with the Air Force Operational Test and Evaluation Center for Air Force-focused enterprise assessments to ensure that data from CAP assessments are provided to stakeholders across the T&E community.

Army

In FY25, CAP, in cooperation with the Army Test and Evaluation Command (ATEC), engaged with the U.S. Army Pacific, U.S. Army Japan, 1st Corps, and 25th Infantry Division to catalog major warfighter concerns and plan assessment events focused on the cybersecurity of the Army SIPRNet at the tactical edge. Future assessment events will focus on these assets.

Beginning in FY25 and continuing into FY26, CAP and ATEC are also conducting a full-spectrum threat assessment of the Army T&E enterprise to ensure that systems and data are appropriately protected throughout the T&E process. The assessment will include physical security, network evaluation, personnel security evaluation through a phishing assessment, and mission assurance and operational security evaluations. The Army will be the first Service to conduct a full-spectrum threat assessment on its own T&E enterprise.

Navy

In FY25, CAP partnered with carrier strike groups and amphibious ready groups to conduct multiple assessment events during composite training unit exercises (C2X), all of which included vulnerability and DCO assessments based on cyber effects integrated into the C2X pre-deployment training needs. With the embedded Navy Cyber Defense Team and standard operating procedures, CAP observed Navy ships reporting an increased number of cyber incidents when they were exposed to DCRT cyber-threat events. CAP attributes this positive increase in reporting to ships utilizing the embedded Navy Cyber Defense Team and the preplanned responses that the defenders disseminate prior to each assessment.

The Navy plans to employ additional network monitoring and DCO tools in FY26. The use of these tools and their contribution to continued improvements in incident response will be a partial focus of future CAP assessment events.

Space Force

As the Space Force has established more internal cyber-focused capabilities, CAP has partnered with the Service to conduct assessments and develop plans for future CRCs. Partners include Space Delta 6, the 33d Range and Aggressor Squadron, the 392nd Combat Training Squadron, space systems program offices, and Space Force leadership personnel.

FY26 events will focus on Space Force–identified systems of interest, including support systems for nuclear command, control, and communication (NC3), support to CCMDs, and capabilities for the cyber defense of industrial control systems.

» SPECIAL ASSESSMENTS

CAP performed the following special assessments in FY25 in collaboration with the USW(R&E), U.S. Cyber Command (USCYBERCOM), DCDC, U.S. Strategic Command (USSTRATCOM), the DoW Chief Information Officer (CIO), the DoW Chief Digital and Artificial Intelligence Officer (CDAO), the Defense Information Systems Agency, and the Department of Energy's Sandia National Laboratories:

- JFN assessments
- Non-kinetic effects (NKE) assessments
- NC3 assessments
- Assessments of artificial intelligence and machine learning (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.

JFN Assessments

In FY25, CAP conducted and published six independent cyber assessments to identify and mitigate vulnerabilities in collaboration with OUSW(R&E). These included assessments during major theater exercises aligned with JFN objectives. Building on the success of these objectives in last year's VALIANT SHIELD 2024, this year included an assessment during joint exercises in 2025. CAP also participated in JFN Experiment 24.12 and Experiment 25.05, which validated the military utility of the JFN V1.0 capability for U.S. Indo-Pacific Command (USINDOPACOM) and provided results that facilitated cross-domain solution approval.

Beyond these events, CAP maintained a strong partnership with the JFN Program Office at all levels of capability management. CAP assessments continue to inform and strengthen the cybersecurity posture of the JFN, which USINDOPACOM has designated as a priority warfighting capability.

NKE Assessments

NKE includes OCO, space effects, radio frequency-enabled cyber operations, and Joint Electromagnetic Spectrum Operations (JEMSO). In FY25, CAP assessments of NKE supported the USINDOPACOM Commander's top-priority mission of counter-command, control, computing, communications, cyber, intelligence, surveillance, reconnaissance, and targeting (C-C5ISRT).

CAP conducted NKE capability assessments on unique systems developed by USCYBERCOM J3 Special Projects, the Air Force, the Navy, and the Defense Advanced Research Projects Agency (DARPA). DOT&E also assessed how some of these unique NKE capabilities are integrated within USINDOPACOM Integrated Joint Fires Rehearsals. In one instance, CAP assessed a first-of-its-kind live fire event in support of a rehearsed Joint All-Domain Operation. Additional assessments examined the integration and synchronization of NKE during exercises, experimental events, and live fire events that supported USINDOPACOM, U.S. European Command (USEUCOM), the Joint Staff's ELITE CONSTELLATION, Joint Special Operations Command, the 160th Special Operations Aviation Regiment, and Army Multi-Domain Task Forces.

CAP partnered with the USSTRATCOM's Joint Electromagnetic Warfare Center to join forces into JEMSO working groups that support the electromagnetic spectrum operations executive committee (EXCOM). The working groups – focused on electronic attack, electronic support, and electronic protection – provided deliverables to the EXCOM that shaped assessment priorities for protecting critical systems and applying JEMSO dominance alongside other non-kinetic capabilities.

In FY26, CAP will continue NKE assessments that support the DoW's top priorities of improving homeland defense and deterring China. These efforts will focus on the missions of missile defense and C-C5ISRT. CAP will continue assessing unique and emerging capabilities and their uses for strategic and operational success. CAP will emphasize operational realism to assist CCMDs in meeting congressional requirements to report on USCYBERCOM capabilities included in Joint Integrated Prioritized Target Lists. CAP will also retain the flexibility to assess emerging changes, such as potential Joint Task Force–Cyber implementations.

NC3 Assessments

CAP and USSTRATCOM continued a partnership for assessing and improving the cyber survivability of the NC3 enterprise. CAP is also assisting USSTRATCOM with assessing future concepts and emerging capabilities. In FY25, CAP conducted ongoing assessments of NC3 sensing and monitoring capabilities, as well as special assessments of NC3 capabilities, and briefed senior NC3 cyber leadership. At the request of STRATCOM senior leadership, CAP will continue supporting key assessments through FY26.

AI/ML Assessments

In FY25, CAP furthered its efforts to develop AI/ML evaluation frameworks and adversarial assessment capabilities. In October 2024, CAP participated in a Naval Surface Warfare Center–Crane event with the Services, academia, FFRDCs, and university-affiliated research centers (UARCs) to pair red and blue AI/ML-enabled capabilities to help the DoW further its ability to fully evaluate the cybersecurity of AI/ML-enabled capabilities. Additionally, CAP hosted three AI/ML working groups with partners from the Services, CDAO, FFRDCs, UARCs, contractors, and academia to review the status of AI/ML assessment methods and tools needed for assessment teams and counter-

AI/ML Red Teams. CAP is engaged with the CDAO, USINDOPACOM, DARPA, and other organizations that desire FY26 assessment support for AI-enabled capabilities.

» SUPPORTING ACTIVITIES

Advanced Cyber-Threat Emulation Capabilities

Realistic, threat-representative cyber adversary emulation is vital for supportable evaluations. Realistic adversary emulation also helps to provide actionable insights for prioritizing mitigations. In response to the FY24 NDAA Section 1507, DOT&E monitors and reports on DCRT capabilities, and in FY25, DOT&E continued to work with the DCRT community through a Capabilities Development Working Group. CAP is focusing on future efforts to expand approved cyber effects within exercises to better replicate advanced threats without creating undue mission risk. That includes enhancing DCRT toolsets – such as cloud-based and AI-enhanced tools, mechanisms for teams to share findings and best practices across Services, and tools for automated data collection and enhanced analysis – and improving mission planning capabilities. CAP has also worked with mission owners to ensure that DCRTs get timely approval for on-network activities, particularly for sensitive networks.

Close Access Team (CAT) Evaluations

CATs perform physical security assessments of secure facilities, revealing how an adversary's physical access to a facility enables follow-on cyber access and puts networks and systems at risk. DOT&E sponsors cyber-enabling CATs as part of holistic CRCs. In FY25, CAP conducted nine CAT missions. These teams identified mission-impacting vulnerabilities at multiple DoW facilities that enabled follow-on cyber access. CAP then worked with the facility owners to understand mission risks and identify mitigations. CAP has also been working with the DCRTs that conduct CAT missions to improve their training and toolsets. In addition, CAP has been working with the teams to improve data collection standards for CATs to document all reconnaissance, daily physical access operations, and DoW systems accessed during missions, so CCMDs have more detailed feedback on physical vulnerabilities that could enable an adversary's cyber ingress.

Commercial and Non-Commercial Cybersecurity Capabilities

In response to the FY23 NDAA Section 1514, the DoW 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, DoW 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 DoW CIO to DOT&E for review to ensure test adequacy.

Cyberspace – Radio Frequency Domain Interactions

In partnership with the Air Force Cyber Resiliency Office for Weapons Systems, CAP conducted events focused on transponder vulnerabilities and how adversaries can exploit cyberspace–electromagnetic spectrum interactions to affect operations in both domains. Many of these events focused on tactical data links and civil data links. CAP continued to collaborate across many partners to expand current capabilities, share information and resources, enhance knowledge management, and continue providing realistic and effective opportunities to research and test evolving threats and remediations.

DCO Capabilities

As the DoW has introduced new technical capabilities for threat sensing across the DoD Information Network, CAP has integrated assessments of these capabilities into CRCs to assess their performance on their intended operational networks. Some of this work has been in the context of NC3 missions under USSTRATCOM, including during GLOBAL THUNDER 2025, in which CAP observed measurable improvements in USSTRATCOM DCO capabilities, particularly in fusing sensor data from multiple NC3 enclaves to inform mission assurance decisions. Additional tool assessments were conducted during shipboard operations at the Navy's C2X. CAP also observed and assessed the operations of newly established Cyber Security Operations Centers.

Persistent Cyberspace Operations (PCO)

CAP continued to mature the PCO concept in FY25. PCO enables more threat-representative cyber emulation through long-duration network assessments and improves the efficiency of DCRTs by focusing their resources on the enterprise level, which in turn helps them support exercise assessments for multiple CCMDs simultaneously. Acting as cyber adversaries, DCRTs leveraged network accesses from CCMDs around the world to posture for and target activity in other areas of responsibility, thereby modeling realistic adversaries. CAP plans similar efforts for multiple CCMD and Service exercises and across the DoW enterprise in FY26.

Purple Teaming Capabilities

CAP continued to mature processes for collaborative purple teaming as part of CRCs. Purple teaming is an industry term for events that combine offensive and defensive tactics in a collaborative environment to identify problems, develop mitigations, and validate those mitigations. In FY25, CAP partnered with multiple stakeholders to conduct cooperative events in which DCRTs uncovered vulnerabilities and stimulated defenders, with information sharing and system owners or Cybersecurity Service Providers making fixes in near real-time. This process has now been conducted at multiple CCMDs, Service-level, and Special Operations venues, with excellent feedback and engagement from local, tactical-level cyber defenders.

Table 1. Summary of CAP FY25 Activities

Type of Event
Physical Security Assessments (9 Events) USA, USAFRICOM, USINDOPACOM, USN (2), USNORTHCOM (2), USTRANSCOM, USSTRATCOM
Assessments of Mission Effects During Exercises (16 Events) USAFRICOM, USCYBERCOM (2), USINDOPACOM (4), USN (3), USNORTHCOM, USTRANSCOM, USSOCOM (2), USSTRATCOM (2)
Cooperative Assessments of Network Security, Purple Team Events, and Tabletop Exercises (12 Events) USA (2), USAF, USCENTCOM (2), USCYBERCOM, USEUCOM (2), USNORTHCOM, USSOCOM (2), USSTRATCOM
Assessments of NKE Capabilities or Fires (12 Events) USCYBERCOM, USEUCOM (2), USINDOPACOM (5), USN, USSF, USSOCOM (2)
PCO (6 Campaigns) USAF, USCENTCOM, USEUCOM, USINDOPACOM, USSOCOM, USTRANSCOM
Assessment of Special Capabilities and Projects (17 Events) AI/ML, Cyber Tools (3), JFN (6), USSPACECOM (2), Other (5)
Acronyms: AI – Artificial Intelligence; JFN – Joint Fires Network; ML – Machine Learning; NKE – Non-Kinetic Effects; PCO – Persistent Cyberspace Operations; USA – U.S. Army; USAF – U.S. Air Force; USAFRICOM – U.S. Africa Command; USCENTCOM – U.S. Central Command; USCYBERCOM – U.S. Cyber Command; USEUCOM – U.S. European Command; USFK – U.S. Forces Korea; USINDOPACOM – U.S. Indo-Pacific Command; 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; USSPACECOM – U.S. Space Command; USSTRATCOM – U.S. Strategic Command; USTRANSCOM – U.S. Transportation Command

International Test and Evaluation Program (ITEP)

In FY25, the Director signed 17 new international agreements. These agreements 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 19 ongoing agreements established with our partners prior to FY25.

PROGRAM OVERVIEW

The United States holds 12 bilateral agreements and two multilateral agreements with international partners. During FY25, discussions continued with additional prospective international partners pursuant to negotiating more bilateral agreements. ITEP was established pursuant to a legislative proposal submitted by DOT&E and enacted into law in 2001. The Secretary of Defense delegated administration of the program to DOT&E in 2003.

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.

FY25 KEY ACTIVITIES

In FY25, the Director signed 17 new international agreements. ITEP also supported 17 previously established agreements. Each agreement is detailed below in alphabetical order by partner country. Bilateral agreements are listed first, followed by multilateral agreements. The 34 agreements in effect during FY25 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 agreement with Australia went into effect in September 2021 and lasts until September 2031.
- The agreement included three new annexes in FY25, which allowed 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 agreement with Australia went into effect in April 2022 and lasts until April 2032.
- The agreement allows Australian Defence Force's personnel to periodically test and evaluate CB agents 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 agreement included one new annex in FY25, which allowed the Australians to conduct additional testing.

3. Electronic Warfare Operational Test 2016 RUTF PA

- This agreement with Canada went into effect in March 2020 and expired in October 2025.
- The agreement between the United States and Canada allowed the at-sea T&E of the electronic warfare (EW) suites fitted in Canadian Navy ships, where the United States simulated anti-ship missile attacks to validate the Canadian Softkill System.

4. SIMULATION DISPLAY (SIMDIS™) Sustainment for Sensors, Weapons, Analysis and Tactical Display Developments RUTF PA

- This agreement with Canada went into effect in March 2020 and lasts until October 2029.
- The agreement 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 is being evaluated for use in operational analyses for tactical development and platform procurement programs.

5. Combat Hammer Omnibus RUTF PA

- This agreement with Canada went into effect in November 2006 and lasts until November 2026.
- The agreement addresses operational effectiveness and suitability testing of all aspects of the CF-18 air-to-ground weapons system.

6. Her Majesty's Canadian Ship (HMCS) Windsor Testing RUTF PA

- This agreement with Canada went into effect in April 2022 and expired in April 2025.
- The agreement covered testing of the Mk 48 Mod 7 Advanced Technology Torpedo as well as the combat systems of HMCS Windsor.

7. Crash Truck Foam Test (CTFT) Project Equipment Transfer (PET)

- This agreement with Canada went into effect in October 2022 and expires in October 2026.
- 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.

8. The Canadian Forces Electronic Warfare Support Test and Evaluation (CFEWS T&E) RUTF PA

- This agreement with Canada went into effect in March 2023 and lasts until March 2027.
- The EW software and the Scenario Simulation Controller are part of a U.S. DoW-owned EW and reprogramming software suite managed by the U.S. Navy's Next Generation Electronic Warfare Generation Program Office.

9. Technology Experimentation and Characterization Field Trials (TECFT) RUTF PA

- This agreement with Canada went into effect in May 2023 and lasts until October 2026.
- The agreement 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 this test event.

10. Combat Archer II Omnibus RUTF PA

- This agreement with Canada went into effect in December 2015 and expired in December 2025.
- The agreement addressed operational effectiveness and suitability testing of the Canadian Air Force's CF-18 air-to-air weapon systems using a total system approach which includes man, munitions, and machines.
- The agreement included one new annex in FY25, which allowed the Canadians to conduct additional testing.

11. Reciprocal Use of Test Facilities (RUTF) Project Arrangement (PA) Concerning Electronic Warfare (EW) Operational Test (OPTEST) 2016 with Canada

- This agreement with Canada went into effect in May 2016 and lasts until March 2026.
- The agreement 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.

12. Advanced Distributed Modular Acquisition System (ADMAS) Instrumentation Equipment and Material Transfer Arrangement

- This agreement with Germany went into effect in October 2020 and lasts until October 2026.
- The agreement 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. The transfer is valid for three years, and allows Germany to standardize test procedures, data analysis techniques, and T&E methodology for the testing of autonomous robotic vehicles and associated technology.
- The agreement included one new amendment that extended the duration of the PA in FY25 to allow additional testing.

13. T&E of the German Bundeswehr CBRNE Defense TTPs RUTF PA

- This agreement with Germany went into effect in June 2021 and lasts until June 2026.
- The agreement 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 agreement included one new annex in FY25, which allowed the Germans to conduct additional testing.

14. 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.

15. Reciprocal Use of Test Facilities Project Arrangement (RUTF PA) Concerning Test and Evaluation of the German Special Forces Reconnaissance and Combat Vehicle (AGF2)

- This agreement with Germany went into effect in July 2024 and expired in July 2025.
- The agreement allowed the German Army to test their new ground combat vehicle, AGF2, in a variety of climatic conditions.

16. Assault Rifle in Extreme Environments RUTF PA

- This agreement with Germany went into effect in May 2024 and expired in May 2025.
- The agreement allowed the German Bundeswehr to test their new assault rifle in three different environments (desert, cold, and tropical).
- The agreement included one new annex in FY25 to allow additional testing.

17. Reciprocal Use of Test Facilities Project Arrangement Concerning Test and Evaluation (T&E) of the German Special Forces G39 Suppressed Assault Rifle, P14 Pistol, and AG40-4 Grenade Launcher in Extreme Environments

- This agreement with Germany went into effect in May 2024 and lasts until May 2026.
- The agreement enables the German Bundeswehr to test an assault rifle, pistol, and grenade launcher in three different environments (desert, cold, and tropical).
- The agreement included one new amendment to extend the duration and one new annex in FY25 to conduct additional testing.

18. 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 effortis facilitating the demonstration of test capabilities at facilities responsible for testing autonomous systems' mobility and weapon systems performance.

19. Reciprocal Use of Test Facilities Project Arrangement Concerning Netherlands F-35 Follow-On Operational Test and Evaluation

- This agreement with the Netherlands went into effect in May 2024 and lasts until February 2034.
- The agreement evaluates the operational effectiveness, suitability, survivability, lethality, and vulnerability of the capabilities for the Netherlands Ministry of Defence F-35 Air System in an operationally realistic environment.

20. Test and Evaluation (T&E) of the Netherlands Ministry of Defence Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) Defence Tactics, Techniques, And Procedures (TTPs) RUTF PA

- This new agreement with the Netherlands went into effect in October 2024 and lasts until October 2029.
- The agreement allows the conduct of testing on the dissemination signature recognition and identification TTP.
- The agreement included one new annex in FY25 to allow additional testing.

21. Over-the-Horizon Weapon System Reciprocal Use of Test Facilities Project Agreement

- This agreement with Norway went into effect in April 2024 and lasts until April 2026.
- The objective of the Over-the-Horizon Weapon System RUTF PA is to test and evaluate two U.S. Over-the-Horizon Weapon System encanistered missile-test assets.

22. Oceanographic and Acoustic Systems (OAS) Reciprocal Use of Test Facilities Project Agreement

- This agreement with Norway went into effect in September 2023 and lasts until September 2027.
- The agreement permits T&E of U.S. DoW oceanographic and acoustic systems aboard a Norwegian Ministry of Defense (NO MOD) vessel in Norwegian waters. The U.S. DoW and NO MOD is leveraging the unique traits of the Norwegian waters and a NO MOD vessel under NO MOD command to: (1) determine the viability of U.S. DoW oceanographic sensors to capture sub-mesoscale and other oceanic motions, and (2) determine the capabilities of U.S. DoW 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. DoW oceanographic and acoustic equipment during three sea trials.

23. MAB 2, Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Defense Tactics, Techniques, and Procedures (TTPs) Test and Evaluation (T&E)

- This new agreement with the United Kingdom went into effect in April 2025 and lasts until April 2030.
- The objective of this MAB 2 CBRNE TTP RUTF PA is to test and evaluate the MAB 2 CBRNE defense TTP for response through the execution of threat representative scenarios in an operationally realistic environment.
- The agreement included an annex to allow testing that was completed in FY25.

24. 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 agreement with the United Kingdom went into effect in January 2021 and lasts until January 2031.
- This agreement has enabled the development and testing of partner defense TTP against CBRNE threats. The U.S. Army 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.
- The agreement included one new annex in FY25 to allow additional testing.

25. T&E of Protective Ensembles Using the Porton Man Test Fixture CTE PA

- This agreement with the United Kingdom went into effect in May 2020 and lasts until May 2027.
- The agreement 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 T&E PA supports U.S. DoW requirements to protect personnel from chemical and biological threats.

26. TOR for Live Fire WG

- This WG with the United Kingdom went into effect in October 2010 and expired in 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.
- The WG exchanged in-theater incident data for combat and tactical wheeled vehicle as well as live fire test and evaluation (LFT&E) data to inform realistic conduct of ongoing and future LFT&E in their respective nations as well as establish a common understanding of LFT&E test procedures.

27. Integrated Air and Missile Defense (IAMD) Testing Reciprocal Use of Test Facilities (RUTF) Project Arrangement (PA)

- This agreement with the United Kingdom went into effect in November 2012 and lasts until November 2027.
- The agreement with the United Kingdom permits large-scale missile defense tests every two years, including the latest in the series, Formidable Shield 2025 (FS25). In May 2025, the Maritime Theater Missile Defense Forum participated in Naval Striking and Support Forces NATO exercise FS25. The purpose of FS25 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 forum events, FS25 increased coalition interoperability and joint capabilities through complex scenarios designed to meet tomorrow's air defense and ballistic missile defense challenges.

28. Counter-Laser Directed Energy Weapons (CLDEW) RUTF

- This agreement with the United Kingdom went into effect in April 2023 and lasts until April 2027.
- 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.

29. L163A1 Electronic Time Fuzes for Artillery Equipment and Material Transfer Arrangement (E&MTA)

- This E&MTA with the United Kingdom went into effect July 2025 and lasts until January 2027.
- The E&MTA allows the U.S. Army to test, evaluate, and analyze the interoperability between the United Kingdom Ministry of Defence L163A1 fuzes and U.S. DoW artillery munitions.

30. Weapons Effects Against Structural Targets 2 (WEST2) RUTF PA

- This PA with the United Kingdom went into effect August 2025 and lasts until August 2028.
- The PA allows the U.S. Army to test and evaluate specified structural targets when impacted by penetrating weapons.

31. 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.

32. Tactics Validation and Operational Readiness Assessment RUTF PA

- This agreement with Australia, Canada, and the United Kingdom went into effect in August 2023 and lasts until August 2026.
- The agreement allows the evaluation of the effectiveness of the defensive tactics of the 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.

33. Aircraft Electronic Warfare Cooperative T&E Project Arrangement

- This agreement with Australia, Canada, and the United Kingdom went into effect in May 2016 and lasts until August 2026.
- Activities and plans for the coming years under this agreement are described in detail in the Center for Countermeasures section of this Annual Report.

34. F-35 Follow-on Operational Test and Evaluation Cooperative Test and Evaluation Project Arrangement

- This agreement with Australia and the United Kingdom went into effect in October 2023 and lasts until October 2033.
- The agreement allows cooperative FOT&E of the F-35 air systems. It will support the contributing participants' continued efforts to evaluate the operational effectiveness, suitability, survivability,

lethality, and vulnerability of F-35 air systems in operationally representative environments. The contributing participants, under the F-35 FOT&E PA, are also evaluating 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 FY25, the Joint Aircraft Survivability Program (JASP) made significant advancements in the Survivability and Lethality of Aircraft in a Tactical Environments (SLATE) simulation environment, including the release of version 1.2, the integration of BlueMax for rotary-wing simulations, and the development of small-arms engagement capabilities, all aimed at improving combat effectiveness analysis for a broad user base. JASP enhanced simulation interoperability and reusability by integrating proven SLATE capabilities into the two-sided Agile Combat Effects Library (ACEL). By implementing a Micro API – a subset of ACEL's Application Programming Interface (API) – JASP enabled external simulation frameworks like Advanced Framework Simulation, Integration and Modeling (AFSIM) to directly access and utilize ACEL's simulation capabilities. This strategic move minimizes redundant development efforts and lowers T&E costs for the entire DoW.

JASP actively addressed emerging threats through projects such as the Intelligent Countermeasure Control (ICC), which uses machine learning (ML) and reinforcement learning (RL) to enhance missile warning systems, and through the development of models and data for long-range air-to-air missile (AAM) detection and tracking.

JASP also enhanced aircraft vulnerability assessment and force protection capabilities through improvements to the Combat Assessment Tool (CAT), development of a plugin for AFSIM to assess weapon impact effects, and the advancement of the Next Generation Fire Model (NGFM) to improve the accuracy of ballistic vulnerability assessments during live fire testing.

In FY25, the Joint Combat Assessment Team (JCAT) strengthened its capabilities through enhanced assessor training (including a new focus on emerging threats and national technical means tools), engagement with U.S. Indo-Pacific Command (USINDOPACOM), and development of a new concept of operations (CONOPS) that utilizes intelligence tools for near real-time forensics of aircraft combat damage in contested environments.

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 modeling and simulation (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 DOT&E.

In January 2003, the Joint Aeronautical Commanders Group signed a new charter establishing JASP to replace the JTCG/AS, while expanding the charter to include the JCAT.

In 2005, the Service aviation systems commands (U.S. Army Aviation and Missile Command, 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 (TTP).
- 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 inform 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.

FY25 KEY ACTIVITIES

» ADVANCING THE CAPABILITY AND CREDIBILITY OF JOINT AIRCRAFT COMBAT EFFECTIVENESS TOOLS

JASP's SLATE tool provides a two-sided combat simulation with "First Look," "First Shot," "First Kill" capability across the survival/kill chain. SLATE supports two-sided multi-domain combat engagement analysis from one-on-one to several-on-several players. 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 in-flight aircraft and weapons players leverage high-fidelity authoritative models, simulations, and data to provide users with credible analytical products.

In February 2025, the Defense Systems Information Analysis Center released SLATE version 1.2 as a controlled unclassified information (CUI) and classified application. SLATE includes an intuitive interface enabling a broad user base from the science and technology, acquisition, and operational communities. The SLATE Operational View is shown in Figure 1.

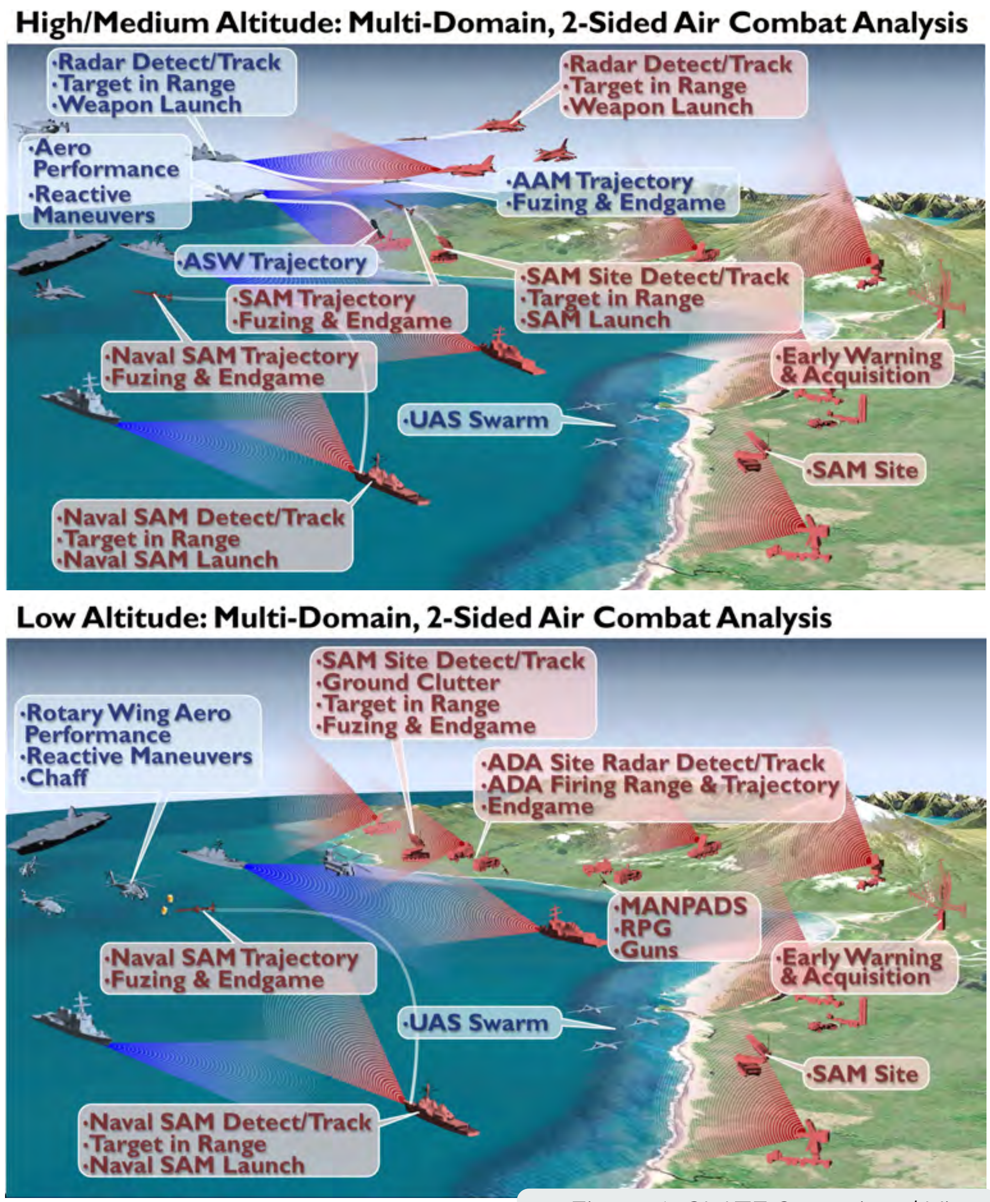


Figure 1. SLATE Operational View

Acronyms: 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

SLATE leverages the Hybrid Integration and Visualization Engine (HIVE) framework to enable multi-domain two-sided combat analyses with a growing suite of capabilities and data. The HIVE integration framework enables fast implementation and testing of authoritative simulations and data from the intelligence community and system program offices. While most of the SLATE/HIVE development effort is focused on providing analytical capability with system models and data, some effort is dedicated to enhancing and maintaining the user interface and experience. SLATE includes interactive, virtual range, and constructive batch capabilities utilizing appropriate types of terrain for advanced displays and simulation effects.

During FY25, the development team implemented and updated SLATE capabilities supporting four key user communities: LFT&E, operational squadrons, RDT&E, and test and training ranges.

LFT&E Simulation Support

SLATE is evolving to support LFT&E. Integrating and fusing multiple simulations delivers a more complete evaluation capability that requires less time from analysts and lowers the cost to meet T&E objectives.

One M&S shortfall for LFT&E has been rotary-wing aircraft and small-arms (projectile flight path) engagement simulation within a combat scenario to assess aircraft lethality and survivability. To resolve this shortfall, JASP completed development of the aero-engine performance (BlueMax) rotary-wing capability. In FY25, JASP released BlueMax version 7.3 with improved flight path stability for rotary-wing aircraft, updated user interface, and was migrated into SLATE. JASP also developed and implemented in SLATE a small-arms (projectile flight path) simulation and ballistic engagement by air and surface threats. The resultant capabilities support a diverse set of combat evaluations within SLATE, including lethality and survivability T&E metrics.

Figure 2 shows the SLATE user's geographical displays for a rotary-wing aircraft's maneuvering flight path with a gunner aiming and firing projectiles into a complex scene and target, combined with terrain imagery. The simulation determines projectile flight paths towards target(s) and resultant engagement lethality.

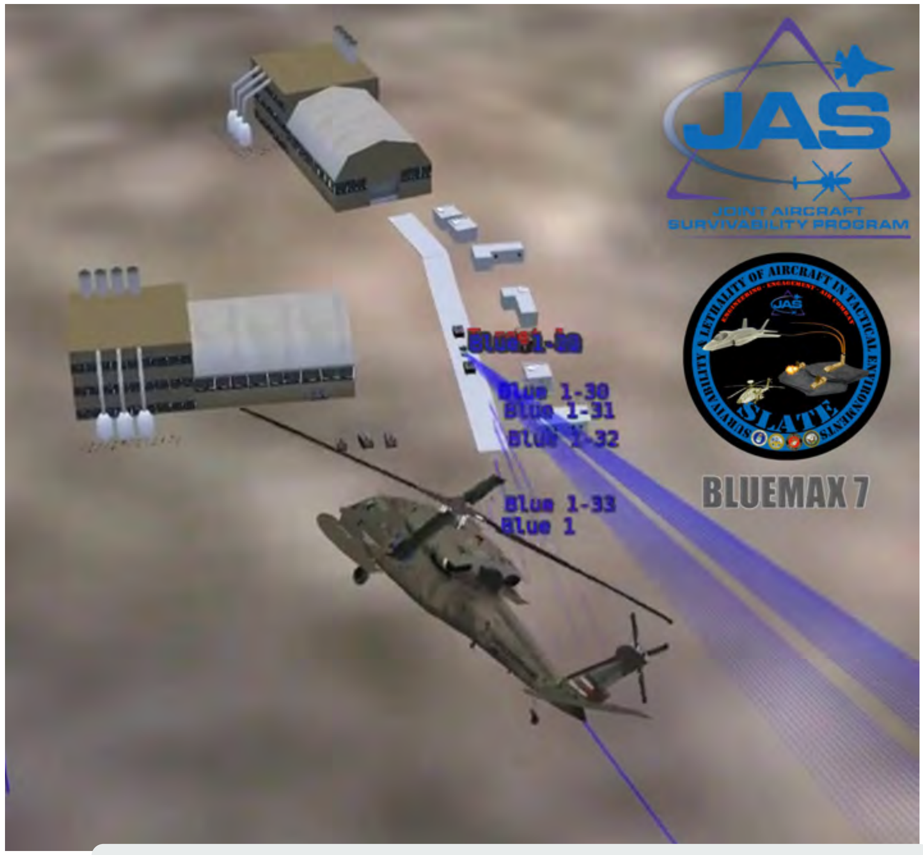


Figure 2. SLATE Rotary-Wing Aircraft Small Arms Engagement

Operational Squadron Tactics Simulation Support

In FY25, JASP continued to develop, expand, and maintain capabilities supporting multi-domain combat simulations within SLATE. Coordinated efforts ensure that once SLATE/HIVE simulation applications are verified and tested with authoritative data, the Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) migrates these capabilities quickly into ACEL. ACEL is a major component of the JTCG/ME Joint Anti-Air Model (JAAM) application which will field a major release in early FY26. JAAM's use of ACEL/ACEL API simulation and data enhances M&S quality and timeliness of delivering suitable simulations to operational warfighters. JAAM user requirements then inform the long-lead development activities for SLATE/HIVE.

RDT&E Simulation Support

JASP supported ongoing ACEL/ACEL API and Micro API development. FY25 efforts expanded upon the FY24 successes of integration of ACEL capabilities via a Micro API for the aircraft aero-engine performance within AFSIM to also address AFSIM needs for surface to air missile simulations. These Micro APIs can be leveraged by other external simulation frameworks. The Micro APIs enable standardized access to the authoritative simulations, for sharing and reuse across the DoW, improving the consistency of analysis, avoiding M&S duplication, and reducing T&E costs.

Test and Training Ranges Simulation Support

Late in FY25, the Test and Training Range at Nellis Air Force Base requested JASP support to manage the replacement of a legacy HIVE-supported application called Aggressor View (AV). AV supports test range real-time kill removal evaluations. SLATE/HIVE, AV/HIVE, and JAAM/ACEL/HIVE capabilities will be refactored into a new simulation called JAAM Live/Virtual/Constructive (LVC). The initial JAAM LVC simulation will be completed late in FY26. The long-term goal is to provide JAAM LVC to TTRs and training squadrons across the DoW, improving aviator TTP development and training capabilities, while reducing duplicative, inconsistent, and expensive efforts.

» 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 to manage major M&S tools used to estimate air combat effectiveness and survivability against an array of operationally representative kinetic threats. The toolsets include the multiple domain two-sided air combat simulation SLATE, the vulnerability analysis code Computation of Vulnerable Area Tool (COVART), along with its supporting penetration and fire prediction codes Projectile Penetration, Fast Air Target Encounter Penetration, and the Next Generation Fire Model (NGFM).

In FY25, JASP initiated an effort to define requirements and write a development plan for a "few-on-few" multimode threat engagement simulation, leveraging existing best-of-breed M&S tools, and capable of evaluating and optimizing aircraft countermeasure (CM) effectiveness. In this case, multimode is defined as threats with sensors that include electro-optical, infrared (IR), and radio frequency wavelengths.

In 1QFY26, this project will deliver the development plan for a tool that will allow engagement simulation of threats that operate in some or all of these wavelength bands. The simulation must operate at fidelity levels high enough to develop and optimize CM devices and techniques.

In FY25, JASP continued to develop tools for cyber and high-energy-laser (HEL) non-kinetic threats. JASP added cyber survivability evaluation capability to the Cyber Operations and Lethality Effectiveness tool (COLE). Specifically, JASP:

- Integrated new cyber risk calculation methods and automated cyber-attack path builder tools.
- Added support to ingest Cameo data, to improve the efficiency of creating and updating system network models.
- Led mobile training team events for Army and Air Force cyber T&E organizations.
- Presented COLE cyber survivability M&S capabilities for aviation at national aircraft cyber and survivability events.
- Supported the Navy's P-8A Poseidon and Army Special Operations Aviation Regiment's MH-60L/M Black Hawk program offices with system model development and cyber survivability analyses. 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.
- Concluded a two-year effort to achieve interoperability of HEL-relevant M&S toolsets for practical HEL survivability analysis. The final report, detailing associated processes, metrics, and supporting test data will be released in 1QFY26. The effort identified data voids, M&S capability limitations, and other factors limiting platform-level survivability analysis. JASP will use this information to develop a comprehensive M&S suite for aircraft HEL survivability analysis.

» COLLECTING AND ANALYZING U.S. AIRCRAFT COMBAT DAMAGE AND LOSSES USING THE JCAT

In FY25, JASP continued to enable aircraft combat damage incident reporting through the JCAT. The JCAT is heavily engaged with USINDOPACOM operational commanders on combat data collection and is leveraging operational exercises to improve data collection and training. The JCAT graduated 32 assessors, increasing the ready bench actively supporting fleet exercises and ready to support combatant commands at every echelon. 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 DoW critical data to address aircraft survivability gaps.

JCAT fully incorporated a third phase of the aircraft combat damage assessment training course, with two new objectives:

- First to provide students with situational awareness of the current and emerging threats in particular areas or responsibility and a basic understanding of naval aviation missions, capabilities, and TTP.
- Second to provide hands-on instruction in the use of national technical means tools, to include a practical exercise.

Figure 3. Phase 1 JCAT Students Learning About the Aviation Survivability Equipment on the AH-64E

JCAT continued development of a new CONOPS utilizing U.S. Code, 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. Through the use of Joint T&E Program funds, they were able to mature and codify CONOPS by supporting test at TALISMAN SABRE 25 and NORTHERN EDGE 25. Figure 3 shows JCAT assessors participating in NORTHERN EDGE 25.

» DELIVERING INNOVATIVE SURVIVABILITY ENHANCEMENT FEATURES

Threat Detection and CM Technologies

Recent conflicts have demonstrated that simultaneously engaging an aircraft with multiple heat-seeking missiles can overwhelm existing defenses and significantly reduce platform survivability. ICC, a JASP project focused on addressing this problem, combines advanced ML and RL concepts to improve the performance of two-color IR (2CIR) missile warning systems in multi-threat engagements. The project combines (1) ML algorithms for improved threat identification, (2) advanced optimization schemes for more robust CM design, and (3) RL training frameworks into a unified design methodology that yields CM systems capable of intelligently prioritizing and deploying limited CM resources in stressing engagements. Beyond addressing the concern of airborne platforms that are simultaneously targeted by multiple threats, ICC also shows improved performance in single-threat engagements.

Over the past three years, the ICC effort has generated several accomplishments within each of the three main research thrusts:

- First, it developed sequential ML algorithms that require less time than in-service algorithms to more accurately identify known threat signatures in a large validation set of simulated engagements. Results indicate that further maturation of these techniques for transition to in-service missile warning systems is warranted.
- Second, the multi-objective jam code design framework has been used to generate, over the course of days, jointly effective codes that are more capable of defeating targeted threats than deployed threat-specific codes developed, over the course of years, by subject matter experts. These jointly effective codes have been validated both in the lab and in simulation and have been prioritized for further development and eventual deployment in the field.
- Finally, trained RL agents have been shown to improve platform survivability in large ensembles of simulated multi-threat engagements by appropriately targeting the laser jammer against

threats according to descending order of danger to the aircraft. Conversely, a naïve baseline jammer allocation policy fails to adequately address all threats in a large fraction of the engagements using the same simulated scenario ensemble.

Overall, the ICC project has delivered several notable successes, which bode well for maintaining U.S. superiority in stressing aerial engagements.

Technological advancements have created emerging threats that push the envelope of long-range detection and tracking. JASP is addressing those issues through development of three projects: (1) Detection of Long-Range AAM Threats, (2) Post Burn-Out (PBO) AAM Tracking, and (3) PBO Signature Capability for Enhanced Missile Signature (E-MSIG).

- The Detection of Long-Range AAM Threats project is intended to establish a validated model for IR signature of the plume, specifically resulting in an updated model for source radiant intensity of an AAM, which will in turn provide the basis for establishment of the detection range of deployed IR sensors against this class of emerging threats.
- The PBO AAM Tracking project is intended to provide modeled signature data for long-range AAMs during the post-motor-burnout phase of flight. This signature data will be used to define required specifications for optical systems, to allow the tracking of these threats after motor burnout and to enable the timely and effective deployment of CMs to defeat these threats. This project will support the tracking capabilities of currently fielded technologies, as well as the ideal and required sensor characteristics to enable the highest likelihood of tracking these threats post-burnout.
- The PBO Signature Capability for E-MSIG project will leverage data from the Detection of Long-Range AAM Threats and PBO AAM Tracking projects to implement the PBO E-MSIG model. E-MSIG models provide obscuration of the plume signature by the missile hardbody but do not model the PBO signature of the hot missile hardbody after burnout. Missile warning and IR CM systems do not have adequate PBO signatures to develop terminal phase detection, tracking, handoff, classification, and CMs.

In FY25, the project teams successfully completed simulation and flight tests to collect data in support of the project goals.

Aircraft Force Protection

VulnView is a visualization tool that allows users to interrogate aircraft platform and threat models for vulnerability analyses with COVART analysis results, and it also houses the Combat Assessment Tool (CAT). The JCAT uses CAT to visualize engagement conditions and identify probable threats in aircraft combat damage assessments. In FY25, JASP added usability features to CAT that aid JCAT and the entire aircraft survivability assessment community. These features include integration with the JASP-funded COVART API, limited support for BRL-CAD files (an Army-based platform geometry modeling environment), animation development, and Microsoft tablet support.

With JASP funding, the Naval Air Warfare Center Weapons Division, in coordination with the U.S. Army Combat Capabilities Development Command (DEVCOM) Analysis Center, developed a new plugin for the AFSIM, to utilize the Advanced Joint Effectiveness Model (AJEM) for assessing the effect of a weapon impact on an aircraft during simulated engagements. The plugin compiles weapon and target states for each engagement during a simulation run and inputs these data into AJEM through the model's application programming interface. AJEM in turn uses the provided data to evaluate what damage levels the aircraft has suffered. Based on AJEM's results, the plugin applies the appropriate kill type(s) to the aircraft. In turn, this allows analysts to more accurately determine aircraft casualties and incorporate loss of aircraft functionality into simulated engagements.

Aircraft Survivability T&E

The NGFM is an ongoing, JASP-coordinated joint-Service collaboration to strengthen the integrity of ballistic vulnerability assessments in LFT&E programs through more accurate fire ignition analyses. This model provides a credible physics-based tool capable for rapidly assessing dry bay fire ignitions, underpinning DOT&E's independent assessments and congressional reporting on acquisition programs covered under section 4172 of title 10, U.S. Code.

The NGFM effort is focused on the following key areas: energy deposition, fuel deposition, model validation, and model management. In FY25, NGFM testing was executed by the Air Force's 704th Test Group's Aerospace Survivability and Safety Office, the Air Force Life Cycle Management Center, and U.S. Army DEVCOM Analysis Center, capturing characterization data for warhead fragment flash and hydrodynamic ram, key variables in evaluating projectile impact conditions needed for a fuel fire ignition source. The Defense Systems Information Analysis Center released NGFM version 2.0 in June 2025.

Figures 4 and 5 show the cavitation bubble produced by a fragment or projectile entering a fluid filled tank, a key fluid-structure dynamic event in predicting fire ignition. Figure 6 shows the critical moment when energy (from a fragment flash) and fuel (from the hydrodynamic ram) coincide and are most likely to ignite into an onboard fire.

The follow-on project, NGFM 2.x, builds on the existing model foundations to expand NGFM's empirical database, enabling aircraft dry bay ignition predictions across a wider range of operationally relevant conditions. Additionally, it will apply physics-

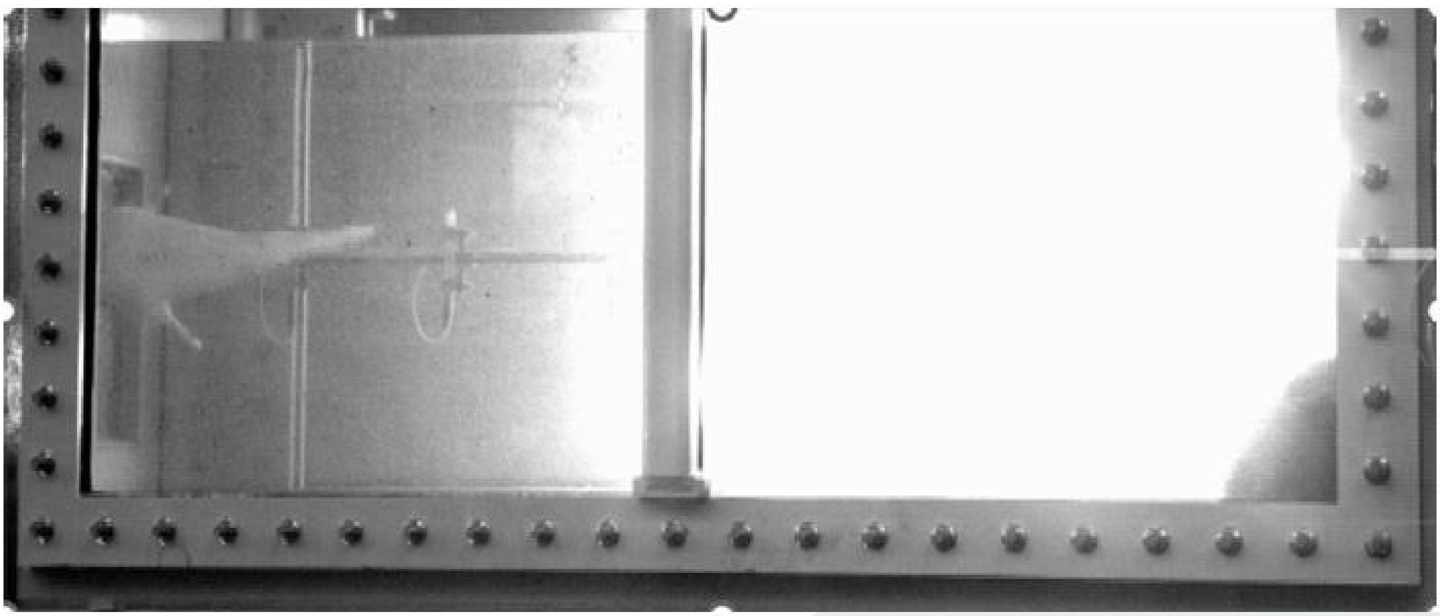


Figure 4. Fuel Cell Post-Impact Fluid Cavitation

Figure 5. Fuel Cell Post-Impact Fluid Cavitation Secondary View

Figure 6. Fuel Cell Post-Impact Back-Face Flash and Exit Wound Spurt

based modeling and ML methods to probe the underlying fluid-structure dynamics of hydrodynamic spurt events and enhance the robustness and accuracy of data reduction processes.

Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) Program

In FY25, the Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) program leveraged modern software development methods to enhance the capability, user experience, and integration of weaponeering tools with greater efficiency and effectiveness. JTCG/ME weaponeering tools and data supported over 500 kinetic strike packages comprised of multiple unique weapon-target pairings. Some of the most visible FY25 strikes included approximately 3,600 unique weapons employments between Operation Poseidon Archer, which took place between January 2024 – May 2025; Operation Rough Rider, which took place between March – May 2025; and Operation Midnight Hammer in June 2025.

PROGRAM OVERVIEW

Chartered in 1968, the JTCG/ME program was established as the Department's focal point for munitions effectiveness information. Its mission began with the development of Joint Munition Effectiveness Manuals (JMEMs) – the sole source of non-nuclear weapons effectiveness data and methodologies for the DoW. These manuals serve as the "how-to" guides for employing kinetic and non-kinetic offensive capabilities, directly enhancing combat readiness, operational effectiveness, efficiency, and survivability.

JMEMs provide critical data in three key areas:

- Weapon characteristics – to quantify damage-producing mechanisms and munition reliability.
- Target vulnerability – to assess how susceptible a target is to specific weapon damage mechanisms.
- Delivery accuracy – to measure a weapon system's ability to place munitions on a target.

Today, JMEMs have transitioned to kinetic and non-kinetic tools used in operational weaponeering, and collateral damage estimation (CDE) in direct support of multi-domain operations, mission planning, and training to support combat operations at the speed, scale, and precision required to prevail in a major theater war.

These tools are used by joint and Service planners in force-on-force effect estimations, mission area analysis, requirements studies, and weapon procurement planning and by the Service acquisition community in performance assessments, analyses of alternatives, and survivability enhancement studies. Key tools and capabilities include:

- Digital Imagery Exploitation Engine (DIEE) – National Geospatial-Intelligence Agency (NGA)-validated mensuration tool that generates precise 3D coordinates for coordinate-seeking weapons. DIEE streamlines Advanced Target Development (ATD) through:
  - Geographically locating and characterizing the target.
  - Weaponeering the target using JMEM Weaponeering System (JWS) – A weaponeering tool that predicts lethal effects and provides warfighters with probability of kill data.
  - Performing target coordinate mensuration.
  - Determining CDE and Risk Estimate Distances – Critical for ensuring the safety of civilian and friendly forces during "danger-close" weapons employments, using the Digital Precision Strike Suite Collateral Damage Estimation (DCiDE) tool.
  - Producing and outputting graphics to the appropriate databases.
- Joint Anti-Air Model (JAAM) – A tool designed to enable air combat tactics, techniques, and procedures (TTP) development for operations at test and training ranges. JAAM is used daily across the DoW for planning and debriefing air combat operations.
- Non-kinetic weaponeering, battle damage assessment (BDA), and targeting workflow tools – These tools estimate lethal effects for advanced systems, including directed energy weapons (DEW), cyber, electromagnetic spectrum (EMS) fires, and maritime targets. They also support BDA and streamline targeting workflows to enhance operational efficiency. Specific tools include:
  - Joint Laser Weaponeering Software (JLaWS)
  - Joint High Power Microwave (HPM) Applied Weaponeering Knowledge Software (JHAWKS)
  - Cyber Operations Lethality and Effectiveness (COLE)
  - Joint Electronic Attack Prediction (JEAP)
  - Maritime and High Energy Laser (HEL) Target Damage Cards
  - Maritime Combat Effectiveness (MaCE)
  - Integrated Naval Simulation for Threat Effects
  - Joint Battle Damage Assessment Repository (JBAR)
  - Joint Target Intelligence Modernization (JTIM) Workflow Application for Recording Production and Targeting History (WARPATH)

The JTCG/ME program also oversees the Joint Live Fire (JLF) program, which plays a critical role in the survivability and lethality analytic community. JLF delivers infrastructure, models, simulations, and data to support the testing and experimentation of kinetic and non-kinetic systems in operationally relevant contexts. This ensures a consistent foundation for LFT&E and the development of 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 joint force and 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 oversees 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.

FY25 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 18,000+ accounts, spanning the following entities:

- DoW Service members
- Joint Staff/CCMDs
- Multiple coalition partners
- Acquisition community
- T&E enterprise
- Intelligence Community
- National Laboratories

In FY25, JTCG/ME fielded updates to improve product accuracy and efficiency in support of operational warfighters. Specifically:

- JTCG/ME has continued to improve the efficiency and effectiveness of the JTIM program by developing, standardizing, and integrating the ATD federated workflow management tool, WARPATH, and further the connection with battle damage assessment tool, JBAR. 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 continued to apply modern software development methods to enable continuous and incremental improvement in capability, user interface, and experience of tools, including JWS, JAAM, COLE, and JEAP.
- JTCG/ME generated seven reach-back packages for weaponeering, CDE, and munition effectiveness assessment in support of FY25 operations.
- JTCG/ME facilitated 24 training classes/events for over 450+ students. Training of integrated product capabilities (DIEE/JWS) continues to enable the operational community to successfully employ munitions while minimizing collateral damage.

» JLF PROGRAM DATA SUPPORT

JLF serves as a cornerstone of the T&E community, providing essential infrastructure, models, simulations, and data to support the testing and experimentation of kinetic and non-kinetic systems in operationally relevant contexts. By delivering a consistent foundation for LFT&E and warfighter tools and techniques, JLF ensures informed decision-making and continuous improvement. In FY25, JLF partnered with naval surface warfare centers, U.S. Army Combat Capabilities Development Command, Sandia National Laboratories, Naval Air Warfare Center, Air Force Research Laboratory, Larence Livermore National Laboratories, Walter Reed Army Institute for Research, Air Force Lifecycle Management Center, Air Force Institute of Technology, and many industry partners to address leading-edge and unique weapon systems development challenges while ensuring that data and characteristics are rigorously analyzed to assess lethality and effectiveness.

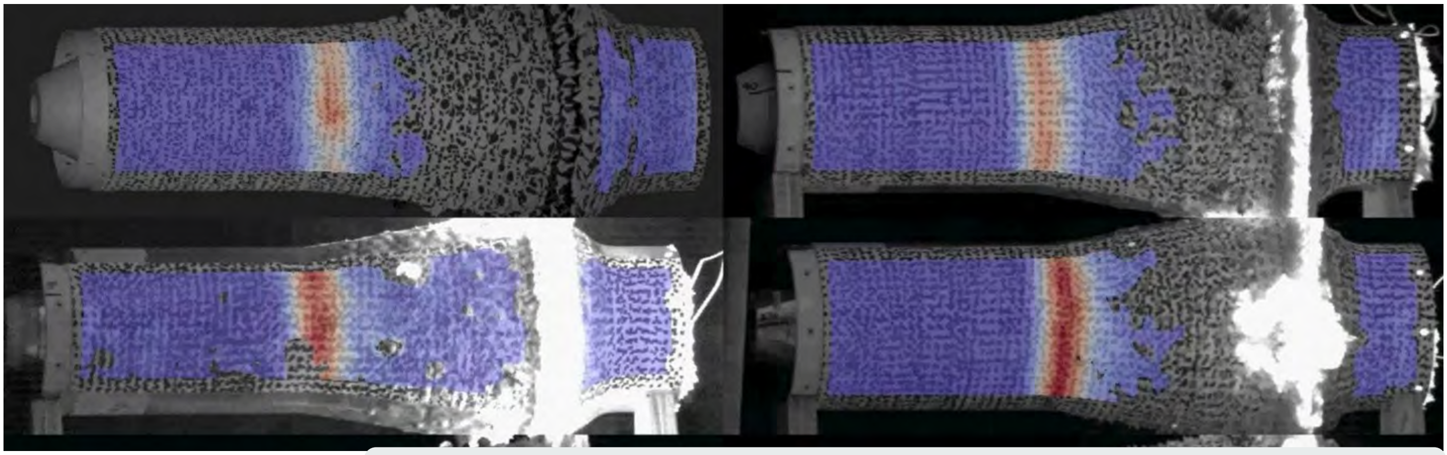


Figure 1. Advanced Warhead Characterization - Digital Warhead Compared to Test

Acquisition Support

JLF provided DOT&E with organic test, data, and modeling and simulation (M&S) capabilities to support T&E requirements – including joint testing that will benefit the entire DoW – emerging/unique testing capabilities and advancing M&S in preparation for Title 10 statutory required evaluations.

In FY25, JLF conducted testing and data collection to update methodologies and create new assessment tools. JLF successfully finalized comprehensive documentation outlining the digital engineering process for munition warhead characterization (as shown in Figure 1). This process is designed to support and enhance the JTCG/ME in its efforts to standardize and improve warhead performance evaluation across the DoW.

Expanding on previous Advanced Warhead Characterization (AWC) test successes, JLF executed over 60 behind armor debris experiments with optical fragment tracking for kinetic energy penetrators. They enhanced optical fragment tracking techniques and updated methodology that can reduce live fire costs by up to 30 percent.

As part of Active Protection System (APS) M&S capability enhancements, JLF expanded shaped charge jet vulnerability and lethality analysis to include multiple fragment impacts. JLF funded the development of methodologies to model damage to rocket-propelled grenades and anti-tank guided missiles from APS countermeasures, and updates to the Advanced Joint Effects Model (AJEM) damaged jet methodology for advanced scenarios. These efforts further improved the effectiveness and fidelity of APS evaluations.

Additionally, JLF improved the modeling of dismembered (misaligned) warheads by collecting test data for existing gaps (as shown in Figure 2) and then used the date to improve the End Game Model's methodology.

Vulnerability analyses depend on accurately defined damage criteria for critical components to predict the probability of kill at the component, system, and target levels. To support this, JLF conducted a series of tests to evaluate fragment penetration into wiring and wire bundles (shown in Figure 3), aiding in the development and validation of component damage criteria.

In FY25, JLF advanced its Traumatic Brain Injury (TBI) initiatives. JLF partnered with Walter Reed Army Institute of Research (WRAIR) to develop a preliminary dose-

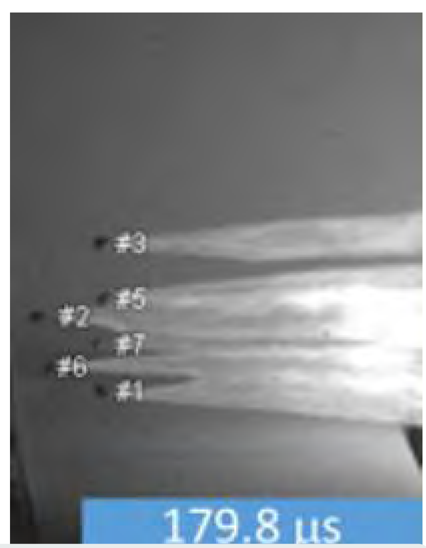


Figure 2. Dismembered Warhead Projectiles

Figure 3. Wire Bundle Target Examples Before and After Test

response curve to establish thresholds for low-level, repeated blast exposure from weapons firing (shown in Figure 4). This curve is set to be integrated into the health hazard assessments used by DOT&E to evaluate weapon safety.

Operational Suppport

JLF provided JTCG/ME with an organic test, data, and M&S capability to support warfighter requirements. This includes joint testing that will improve M&S capabilities foundational to operational tools, quick reaction testing to meet critical operational requirements, and advancing M&S in preparation for integration of fielded weapon systems into JTCG/ME operational tools.

In FY25, the JLF executed aluminized high-explosive blast experiments to validate and improve late-time blast effects M&S methodologies developed under the JLF Phase I - Aluminized High Explosive Modeling and Simulation Program. Figure 5 shows an example of the blast experimentation. This comprehensive program enables more accurate fast-running models and lethality assessments, allowing the weaponeering community to precisely evaluate the impact of enhanced-effect aluminized explosives on lethality.

To support injury risk assessments as part of JTCG/ME's CDE efforts, JLF continued collaboration with the University of Virginia (UVA) to develop an initial TBI risk model for large, acute blast event exposures to inform Danger Close calls (i.e., risk to friendly troops) for close air support and fires support missions. JLF delivered an initial software capability, with verification and validation planned for FY26.

Within the scope of non-kinetic capabilities, JLF tested and generated target vulnerability packages to assess the lethality and effectiveness of HEL and HPM weapons, accounting for threat vulnerabilities through high-fidelity and empirically based analyses. Figure 6 shows an HPM test fixture.

JLF investigated the kinetic effects that can penetrate shielding and make target components more vulnerable to HPM weapons. This involved conducting simulations and testing of attenuation through shields with relevant fragment holes and patterns to evaluate frequency susceptibility against relevant components.

JLF partnered with the Air Force Institute of Technology to include the Weather Integration Prototype (WIP) system in DoW field tests, tested WIP updates, and generated atmospheric and performance data sets for the Directed Energy community to provide improved real-time path characterizations for laser weapon systems and battlespace management applications. This work resulted in a Realtime Weather Sensor Package (shown in Figure 7) recommendation for ranges to accurately capture HEL effectiveness.

Full-Spectrum Survivability

In FY25, the JLF provided DOT&E with a surge capability to develop and implement tools, processes, and methods to enable credible full-spectrum survivability and lethality evaluations across the acquisition lifecycle, including operations and sustainment. This one-year surge effort focused on three operationally relevant scenarios: (1) weaponeering in multi-domain operations to support the commander's intent, (2) full-spectrum survivability to inform acquisition decisions, and (3) full-spectrum lethality to inform acquisition decisions. Deliverables from the JLF full-spectrum analysis surge will transition to DOT&E and JTCG/ME to improve system evaluation and warfighter capabilities across multiple, collaborative domains.

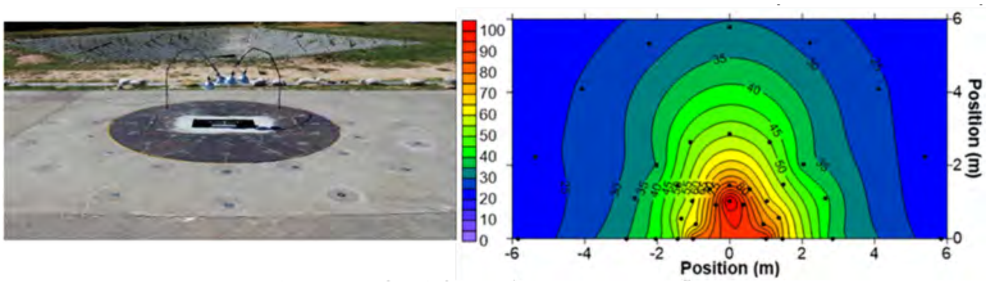


Figure 5. Blast Pad facility (left) and example of pressure impulse data (right)

JLF advanced full-spectrum analysis capabilities by transitioning the Full Spectrum Survivability Tool to the lethality domain, delivering an updated graphical user interface (GUI) for scenario definition, and evaluating transition partners. Additionally, JLF completed initial research and modifications to integrate radio frequency connections between devices into COLE through the Cyber Link Effects Analysis for Radio Systems (CLEARS) project, enabling comprehensive analysis of wireless systems within the full spectrum framework depicted in Figure 8.

JLF expanded LLNL's Eucalyptus, a failure analysis logic tool. Eucalyptus generates system fault trees based on component and location variability. The fault tree is generated using engineering principles and outputs a visual representation of the layout (as shown in Figure 9), to support multi-domain effects and integrated the capability to model uncertainty of component location. Enhancements included the following: performance improvements, faster computations, improved test suite, and ability to generate a single executable file.

As part of the FY25 focus on enabling credible full-spectrum survivability and lethality evaluations across the acquisition lifecycle, JLF developed and delivered a proof-of-concept analysis demonstrating dynamic integration

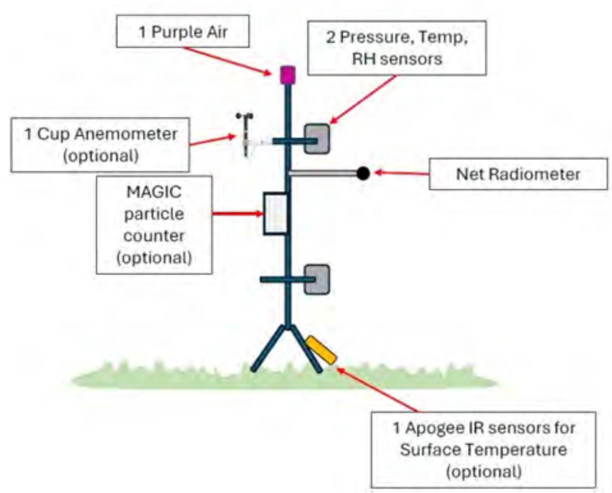


Figure 7. Realtime Weather Sensor Package

Figure 8. CLEARS Concept

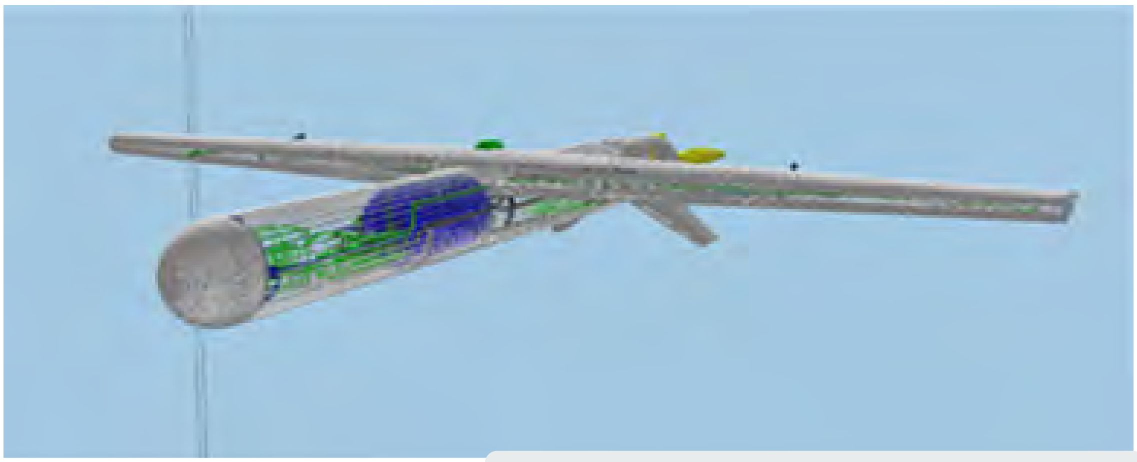


Figure 9. Eucalyptus Component Representation

between force-on-force level modeling with engineering level ballistic modeling. This effort included adjustments to human behaviors to reflect the reduced functionality of a vehicle. This final demonstration of full-spectrum survivability directly supports the JLF's operational priorities, including multi-domain weaponeering, survivability-informed acquisition decisions, and lethality assessments.

Knowledge/Data Management

Data is the foundation of acquisition and operational decision-making, with digital transformations playing a critical role in accelerating development, analysis, and production processes. JLF prioritizes validated data as the cornerstone of every project, ensuring accuracy and reliability to support informed decisions.

In FY25, JLF transitioned and expanded data repositories to enhance the archival, review, and accessibility of lethality and vulnerability data, methodologies, and documentation. Key updates include the following:

- HEL Repository – JLF was the transition partner for the OUSW(R&E)-developed repository for HEL component-level testing, supporting test planning and M&S development.
- JBAR – JLF integrated test data into JBAR and added a user interface, enabling warfighters to search and access videos and data from test events (shown in Figure 10).
- Service-Specific Repository (SSR) – JLF developed and deployed a target vulnerability data repository shared across the DoW acquisition community. The SSR connects directly to the JTCG/ME target development and approval

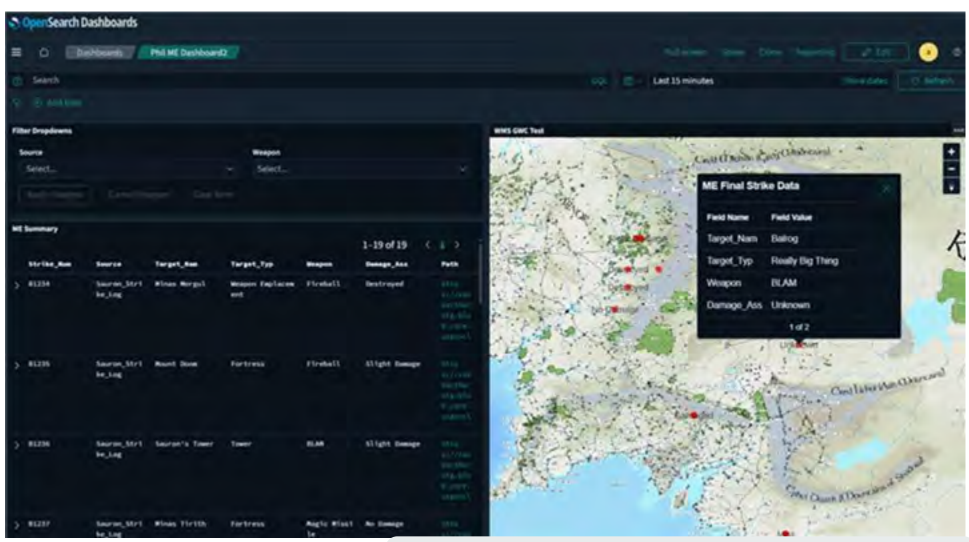


Figure 10. JBAR Screenshot User Interface

process and is accessible on both NIPRNet and SIPRNet.

These advancements ensure that critical data are readily available to improve lethality and survivability evaluations and to inform decision-making.

JLF remains an essential contributor to the T&E and warfighting communities, delivering innovative capabilities, tools, and data to advance all-domain survivability and lethality evaluations of DoW systems. Through rigorous testing, M&S, and analysis in operationally relevant environments, JLF continues to enhance JTCG/ME effectiveness estimates for both kinetic and non-kinetic systems. These efforts ensure that the DoW is equipped with the insights and tools necessary to maintain a decisive edge in modern warfare.

» ADVANCING THE CAPABILITY, EFFICIENCY, AND ACCURACY OF TARGET DEVELOPMENT TOOLS

ATD

DIEE is a vital software program for the targeting enterprise at the global level. It provides digital solutions to the essential Joint Targeting Cycle functions for the U.S. and coalition partners.

DIEE's intel and targeting capabilities transform workflow inefficiencies into automated and integrated solutions within one ecosystem. DIEE's critical targeting functions apply across the targeting spectrum and address basic, intermediate, and ATD. Key functions include the following:

- Target Coordinate Mensuration – Ensuring precise geolocation of targets.
- Weaponeering Methodologies – Utilizing the JWS for optimal weapon selection.
- CDE – Leveraging the DCiDE tool to assess effects and minimize risks.
- Targeting Graphics Production – Creating high-quality visual aids for operational planning.
- Combat Assessment – Evaluating mission effectiveness and refining restrike strategies.

FY25 accomplishments include extending DIEE's interoperability with the rest of the targeting enterprise to enable federation of target development. This includes interoperability with key systems such as the Machine-assisted Analytical Rapid-repository System and WARPATH.

Additionally, the fielding of Tactical DIEE versions 3.0.1 and 3.1 introduced several enhancements, including:

- Modernized integrated database updates for improved data management.
- 3D point mensuration capability for precise geospatial analysis shown in Figure 11.
- DCiDE updates aligned with Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3160.01E standards for CDE.
- Graphic generation updates compliant with CJCSI 3370.01D for targeting visuals.
- Initial release of maritime target damage cards to support maritime operations.
- The first iteration of the integrated JWS capability.

The development of Enterprise DIEE, a Public Key Infrastructure (PKI)-enabled and cloud-based solution, is underway with capability drops planned for FY26. Specific capabilities being developed include

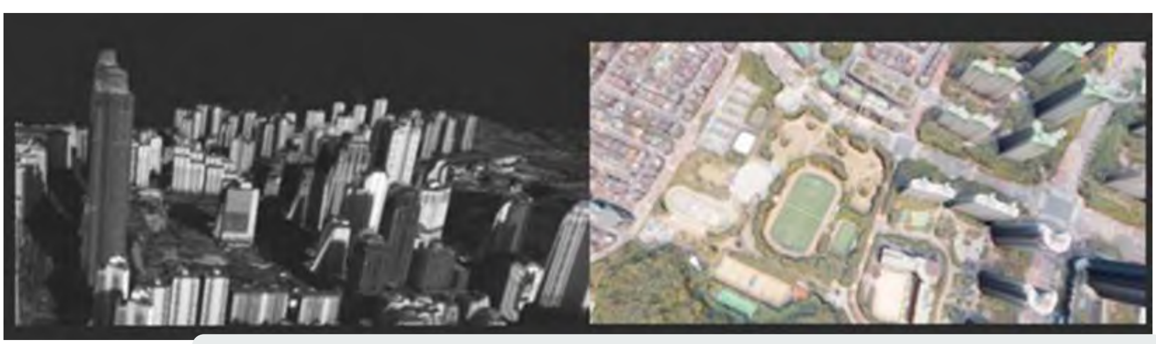


Figure 11. Examples of native 3D imagery analysis and Target Coordinate Mensuration capability no longer requiring additional hardware

interfaces with other Services to conduct basic and intermediate target development as well as support for combat assessment.

As part of the OUSW(I&S) and J-2 JTIM initiative, JTCG/ME initiated the development of a federated workflow management tool, WARPATH. This tool aids in streamlining the targeting, production, and tracking process while reducing duplicative efforts and costs. WARPATH will be a stand-alone 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 FY25, JWS version 2.4.2 was published for foreign disclosure review and accreditation. JWS v2.4.2 provides cyber security updates and enhanced connectivity capabilities with the DIEE application. Development of a follow-on release, JWS v2.5, was also completed. This version of JWS provides a refined data set that allows deployment to additional coalition partners and tightens interactions between the U.S. and foreign partners within joint environments.

The next-generation JWS 1.x plug-in product line will continue the development of weaponeering capabilities, including:

- Support for structural targets (e.g., building cross-section, as shown in Figure 12).
- Enhanced modeling for interior and exterior personnel targets.
- Materiel target analysis.
- Modernized weaponeering support tools.
- Seamless integration with DIEE 3.x.

While initial capabilities are reviewed and tested, future capabilities, to include bridge, bunker, and runway targets are being integrated and prepared for operational weaponeer community review.

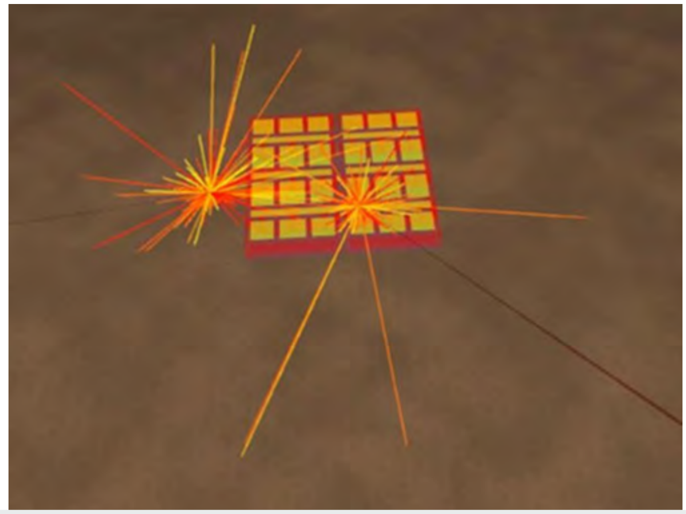


Figure 12. JWS Plug-in 1.x Fragment flyout interaction with cross-section of structural target

CDE

In FY25, JTCG/ME made significant progress toward improving the ability of the DoW and coalition partners to accurately characterize the CDE associated with lethal effects of weapons employments. Specifically, JTCG/ME continued the execution of the multiyear Enhanced Weaponeering and CDE test program to quantify the collateral effects resulting from munitions detonating in the ground or beneath structures. Data sets from the Enhanced Weaponeering and CDE test program were used to develop, improve, and validate methodologies to predict building debris characterization (e.g., fragment distribution, mass, velocity), cratering, soil ejecta, ground shock, and blast pressure for mitigated munitions. These methodologies are used by operational tools, including DCiDE and JWS, to estimate weapon collateral damage and lethality.

In FY25, JTCG/ME conducted multiple tests, shown in Figure 13, to further the understanding of deeply buried munitions and building debris effects, shown in Figure 14, on personnel and nearby structures. These data supported the evaluation of camouflet - formation resulting from below-ground detonations that do not open to the soil surface, as well as the effects of a munition buried beneath a two-story structure. The data enabled the characterization of blast and fragmentation mitigation and the collateral risk from secondary debris. This program has fostered

Figure 13. Buried ordnance test conducted in partnership with the U.S. Army Engineer Research and Development Center at Fort Johnson, Louisiana

Figure 14. Two-story over-burial building debris test conducted in partnership with the U.S. Army Aberdeen Test Center, Maryland

collaboration opportunities among multiple organizations, enabling the collection and sharing of valuable data for other M&S and methodology development efforts.

BDA

JTCG/ME continued the multiyear effort to 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 FY25, JTCG/ME worked with U.S. Central Command (USCENTCOM) to update the JBAR GUI to ensure it meets their operational strike reporting needs. Application programming interface (API) connections were made to the Defense Intelligence Agency's Modernized Intelligence Database and the Air Force's air mission repository MARAUDER to collect mission reports, graphics, weaponeering data, and full-motion video for USCENTCOM and U.S. Africa Command (USAFRICOM). The data were subsequently entered into the JBAR database, making them accessible through queryable web maps.

As part of the JTIM program, JBARs development team is working to make connections to data scraping tools and WARPATH to maintain interoperability and integrate into the National Geospatial-Intelligence Agency Common Operations Release Environment (NGA CORE) cloud environment. Connections to scraping tools will allow for the collection of strike-related information from operational chat logs. WARPATH will receive a strike identification number from JBAR for tracking through the combat assessment process.

Lethal Effect Estimates – Maritime Targets

In FY25, JTCG/ME continued 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 continued to develop and publish updates to the "Maritime Weaponeering Handbook," covering several maritime targets not currently in JTCG/ME inventory. Version 1.3 of the Target Damage Cards software, developed by JTCG/ME will be integrated into DIEE to update the interim maritime weaponeering analysis tool for

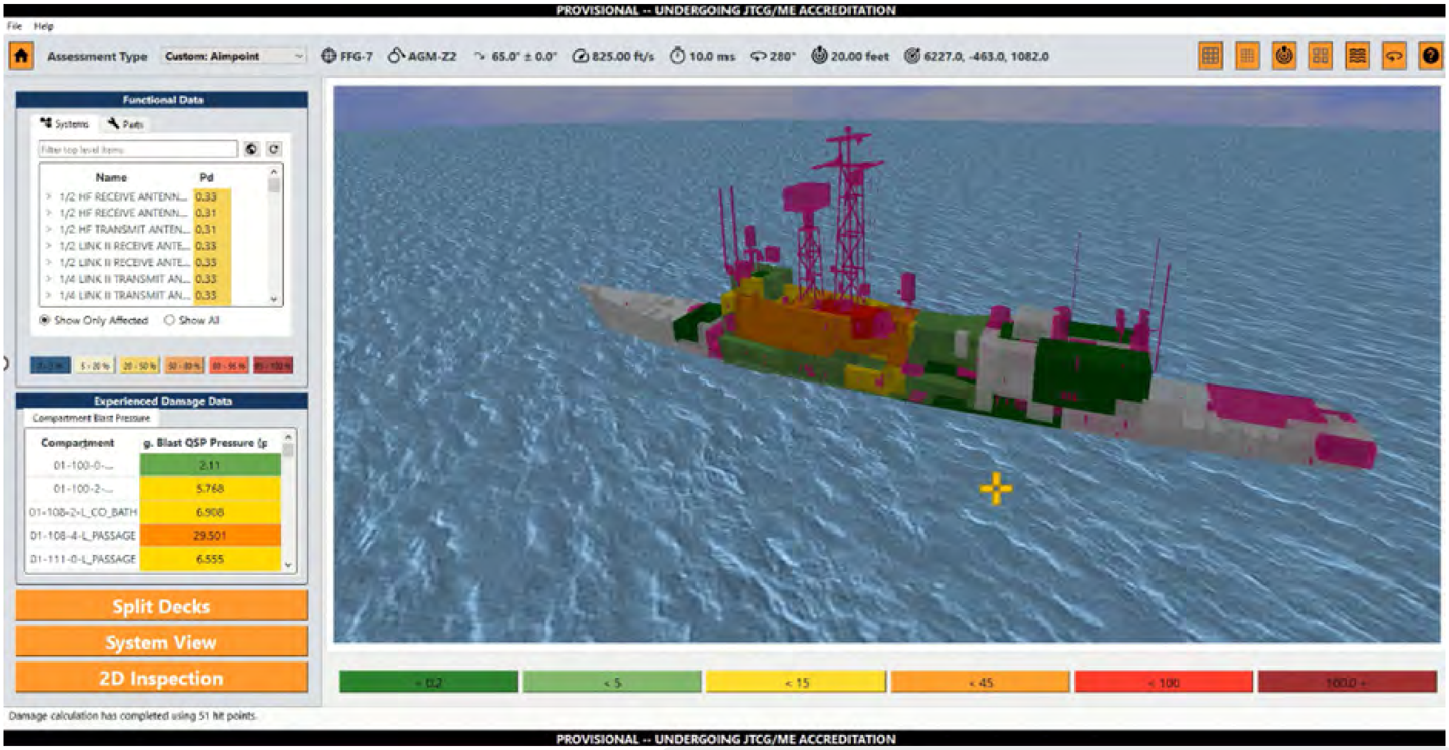


Figure 15. Maritime Target Damage Card visualization tool

surface targets shown in Figure 15, with follow-on versions including subsurface targets.

Development of the MaCE operational weaponeering tool progressed in FY25, adding to the capabilities of Target Damage Cards (shown in Figure 15). Ultimately, MaCE will be integrated into DIEE. MaCE will be able to calculate results on the fly and visualize precalculated data within DIEE.

JTCG/ME continues to execute a collaborative test program that procures data to close knowledge gaps, improve current analytical tools and methods, and develop advanced digital tools required to support the delivery and fielding of weaponeering tools against maritime targets. This includes the Integrated Naval Simulation for Threat Effects, which is 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:

- Submarine Vulnerable Effects Model
- Navy Enhanced Sierra Mechanics
- Dynamic System Mechanics Advanced Simulation

The test program includes methodology development to predict fire initiation within targets and damage due to missile-body debris. JTCG/ME also provided reach-back support for urgent operational user requests and has delivered 29 operational user reach-back packages to date. These efforts increase weapons systems' lethality against foreign maritime threat platforms and will support more effective and efficient survivability evaluation of U.S. ships and submarines for LFT&E programs.

Aircraft and Weapon Tactics

In FY25, JTCG/ME finished the JAAM version 6.0 application, with a planned release early in FY26. The JAAM application is the authoritative, two-sided (e.g., blue and threat), multi-domain combat simulation utilized to underpin common air warfare training and operational tactics. JAAM development leverages an authoritative suite of supplier simulations and data, fused within a common framework. JAAM significantly enhances the lethality of U.S. fighter pilot training by providing accurate assessments rather than assumptions, guesswork, or unverifiable maneuvers. JAAM is critical to warfighters having the weapons and tactics required to win in combat.

Warfighters utilize JAAM version 5.4 daily across 370 sites to enable TTP development and refinement, as well as reinforcement training for air-to-air and surface-to-air threat engagements.

Users across the joint force use JAAM for a breadth of operational requirements:

- Test and training ranges use JAAM to support tactics development, mission rehearsal, debriefing, and reinforcement training for pilots.
- Combat Air Forces and the Navy and Marine Corps air fleets use JAAM to support operational doctrine and technical manual development.
- The Intelligence Community uses JAAM to support tactics analysis.
- The joint fighter integration community utilizes JAAM for cockpit-used data kneeboard devices detailing the timelines approved for efficient and effective tactics.

JAAM leverages both stand-alone and external APIs:

- The stand-alone JAAM version 6.0 application and GUI display show aircraft and weapon flight paths and key tactical events, such as aircraft target detection, weapon launch, weapon seeker activation, weapon performance, aircraft performance, and target intercepted-killed (Figure 16). These graphical displays enable users to critically assess aircraft maneuvers and weapon shots, with high-fidelity, authoritative information.
- The JAAM external API provides the same authoritative results accessible to the warfighter when using JAAM stand-alone. The JAAM API allows interoperability within debriefing tools such as Personal Computer Debriefing System, Live Missions Operations Capability, and Tactical Combat Training System. This interoperability allows JAAM to support event playback using post-event aircraft cartridge data (i.e., time-space-position information data and GPS data).

JTCG/ME developed the new JAAM version 6.x product line to address warfighters' needs for unique large-scale data simulation and ease-of-use workflow. The JAAM 6.x product line uses the Air Combat Effects Library (ACEL) which contains the government-owned framework, Hybrid Integration and Visualization Engine. JAAM leverages collaborative

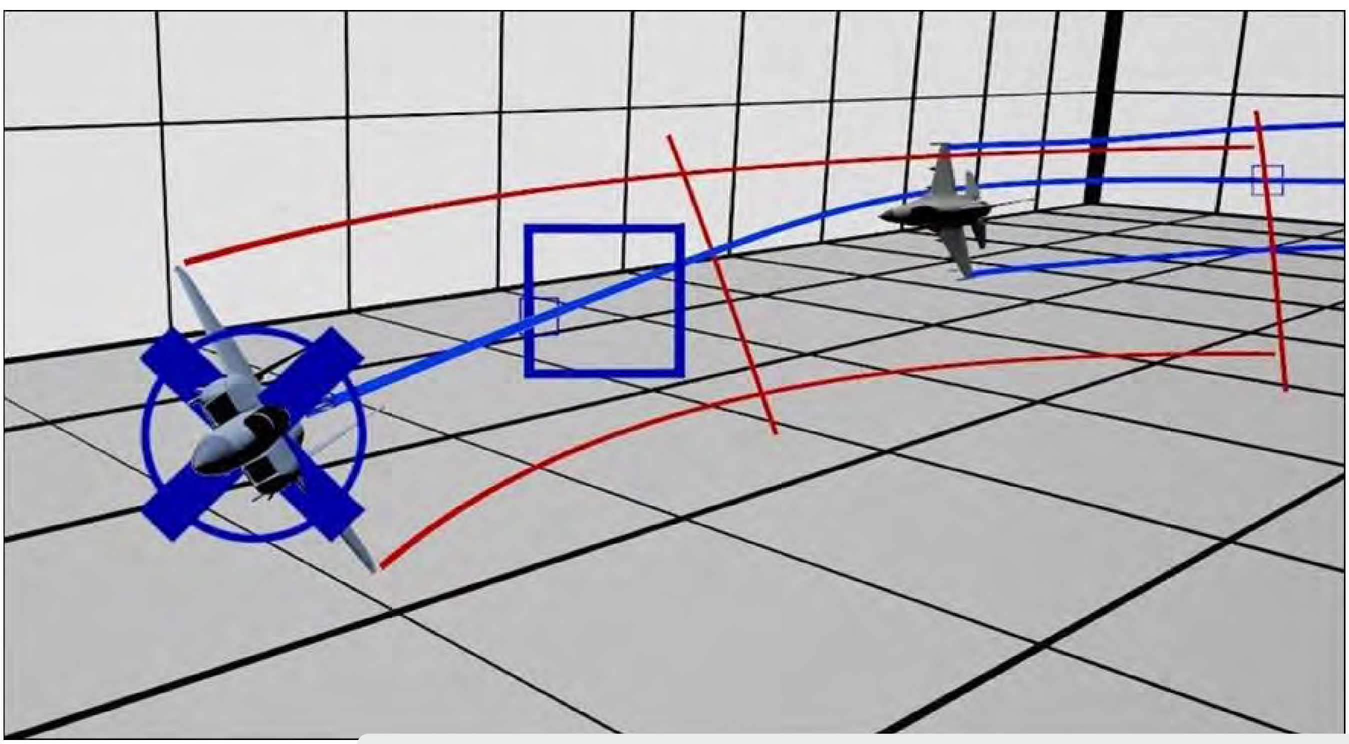


Figure 16. JAAM version 6.0 Interactive GUI showing key simulation events (weapon launch, seeker activation, and intercept/kill)

efforts with the Joint Aircraft Survivability Program (JASP) and intelligence centers to provide users with ACEL's authoritative, high-fidelity simulations and data needed. JAAM's design enhances aircraft survivability and weapons lethality in a multi-domain, contested combat environment.

JAAM version 6.0 enhances productivity and workflow to support large-scale data analytics needed to develop and refine tactics against emerging threats. JAAM's warfighter-friendly parametric GUI, simplifies workflow and increases output options for the warfighter assessing multiple aircraft and weapons with hundreds of thousands of parametric engagement conditions. Data content is user selectable and is available in standard eXtensible Markup Language (XML) and spreadsheet formats, suitable for external data processing. GUI-enabled batch processing increases productivity by removing operator-overhead and instead utilizing the framework to efficiently handle the processor allocation and sequencing within individual engagements. This key capability directly supports efficient tactics development. The new in-line GUI editing eliminates disconnected workflow. The GUI redesign enables growth for additional capabilities such as terrain masking and displays. JAAM version 6.0 will introduce rotary-wing platforms as part of the low-altitude combat scenarios, providing critical value-added insights to warfighters.

Data Management

In FY25, JTCG/ME supported implementation of the DoW Data Strategy. Beyond the previously mentioned JLF knowledge/data management initiative, JTCG/ME expanded the repositories for access of lethality and vulnerability data (e.g. archival, review, and approval) methodology, and documentation. The following four repositories serve multiple user communities with corresponding features and capabilities:

- 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 communities by providing JTCG/ME-approved target vulnerability packages. In FY25, 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, the Joint Effects Library (JEL) is 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 FY25, JTCG/ME incorporated several additional modules into the JEL to support kinetic 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 DoW community. In FY25, 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.
- For the acquisition community, the JLF Secure Targeting Exchange Platform (STEP) is a web-accessible and secure repository for the joint target vulnerability development community. This application provides transparency of target vulnerability development efforts throughout the DoW for cost sharing opportunities. Analysts can use the repository to store, manage, and share target vulnerability data throughout the acquisition community. In FY25, the STEP was enhanced with token-based authentication, improved access controls, and easier loading of large data sets. The product has users in the 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 DoW.

» ENABLING MULTI-DOMAIN SUPERIORITY WITH DEW, CYBER, INFLUENCE OPERATIONS, AND EMS FIRE WEAPONEERING TOOLS

DEW

In FY25, JTCG/ME continued to develop and validate DEW weaponeering tools – JLaWS and JHAWKS – to enable the CCMDs to estimate lethal effects using HEL and HPMs.

JLaWS

JLaWS uses target vulnerability data, weather effects, and optical risk characteristics to provide effectiveness results for solid state laser weapon systems. JLaWS accounts for the effect of weather on laser propagation by automatically downloading location-specific weather files from established services. It 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. Figure 17 shows a JLaWS graphical rendering of a ship-based laser weapon system engagement with an unmanned aerial vehicle target and the spherical zones around the target, as calculated by HELRAT, in which ocular hazards exist.

In FY25, JTCG/ME fielded JLaWS version 2.x and continued development of JLaWS version 3.1.2. The JLaWS version 3.x products will include new weapons, target vulnerability characterization, and enhancements from test and analytical events. Focus areas include validating and verifying both the underpinning methodology and data that support JLaWS, and increased data reviews/approvals for improved capability.

JTCG/ME supplied eight operational threat packages to Commander, U.S. Seventh Fleet (C7F) for a HEL

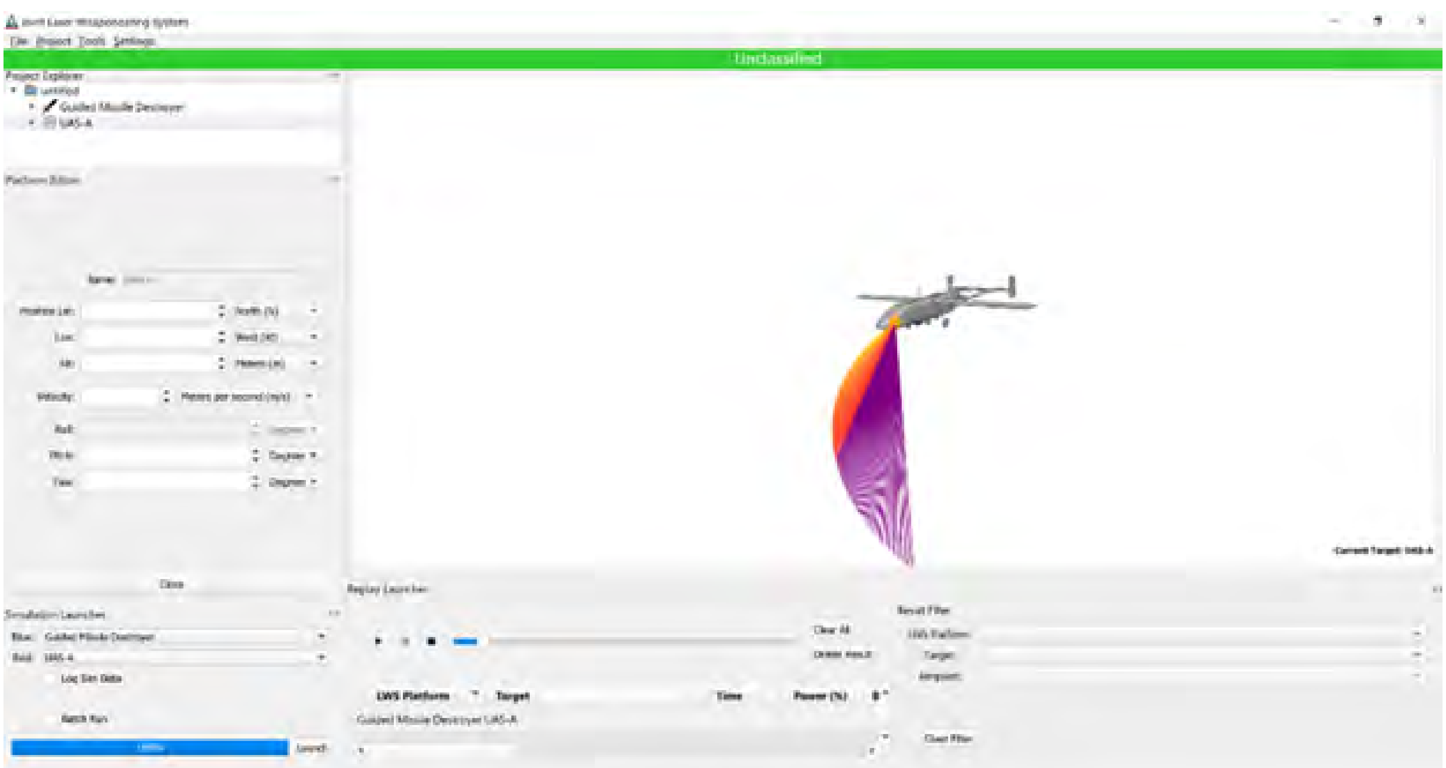


Figure 17. JLaWS Vulnerability Explorer and examples of shot lines

system of interest. In addition, supported operational target card packages, and engaged in multiple warfighter events, allowing critical operator feedback to support weaponeering and CDE for HEL weapon systems.

JTCG/ME's further development and validation of the surrogation tool, Characteristic-based Laser Objective Surrogate Evaluation (CLOSE), allows for subject matter experts to generate efficient, reliable, and tractable HEL surrogate vulnerability packages from an existing assessment database, allowing quick turnaround HEL analyses and studies.

JHAWKS

JTCG/ME continued development of its HPM tools and released JHAWKS version 1.0 Beta for user feedback, with the next release scheduled in FY26. JHAWKS version 1.0 Beta, shown in Figure 18 displays a single drone and a stationary HPM source. This use case allows users to output the overall power directed on target and establishes a foundational minimum viable product that can be expanded to model more mission-relevant scenarios, such as swarm engagements. Additionally, the JHAWKS team developed HPM vulnerability modules (VMs) and refined the HPM VM interface control document, for review and concurrence with the HPM community.

These efforts serve as critical inputs for JHAWKS development.

In FY25, JTCG/ME supported the release of the Effectiveness ToolBox (ETB) 9.0, with significant enhancements in graphics and capabilities that support HPM engagement evaluations as shown in Figure 19. ETB is an advanced engineering-level M&S tool designed to address capability gaps and enable accurate modeling of dynamic HPM engagements, critical for providing reliable JHAWKS inputs and ensuring validated and accurate data are used in operational planning. The ETB 9.0 release marks a significant advancement in HPM modeling capabilities and supports next-generation non-kinetic weaponeering tool development.

COLE

In FY25, JTCG/ME continued developing and fielding cyber JMEM capabilities. COLE is the foundational product, enabling commanders and decision makers at all echelons to generate accredited, quantitative, and predictive effects of cyber operations in joint force operations. COLE provides the user with a cyber operations modeling and analysis capability for offensive cyber operations, T&E of operational systems, and risk assessments of cyber resilient systems. JTCG/ME partnered with JASP and JLF on

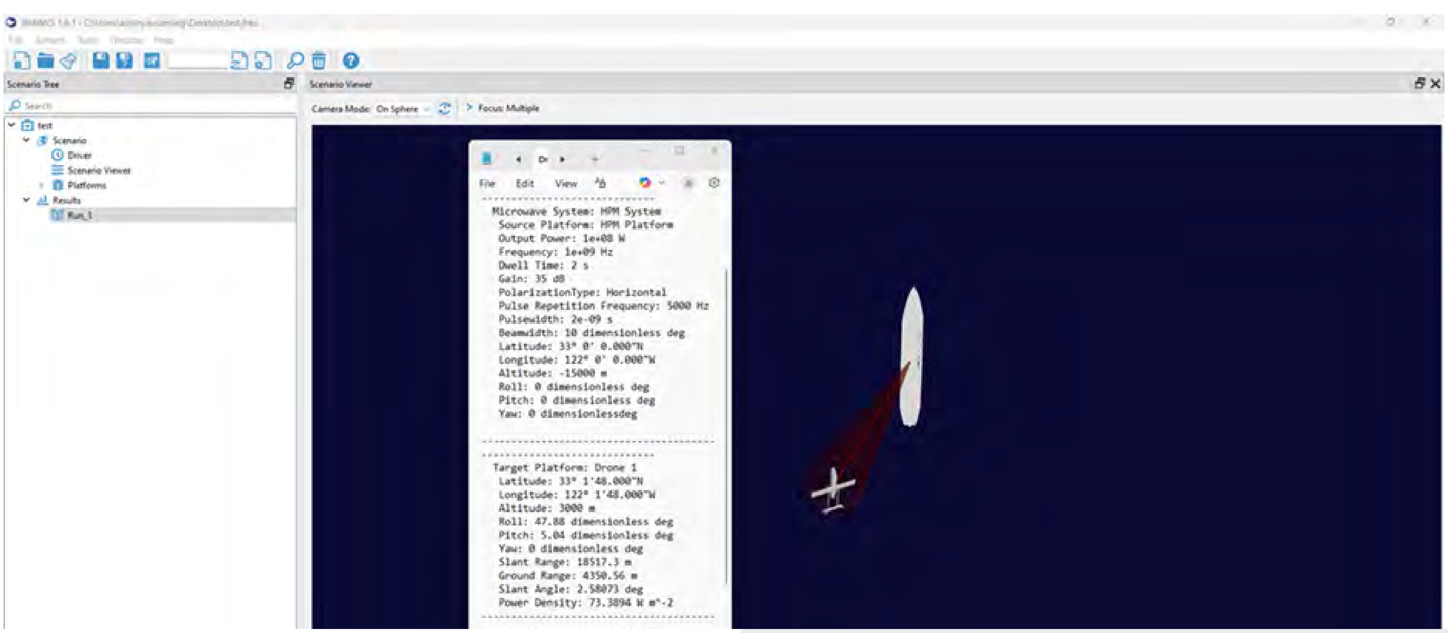


Figure 18. JHAWKS Initialization and Platform Editor

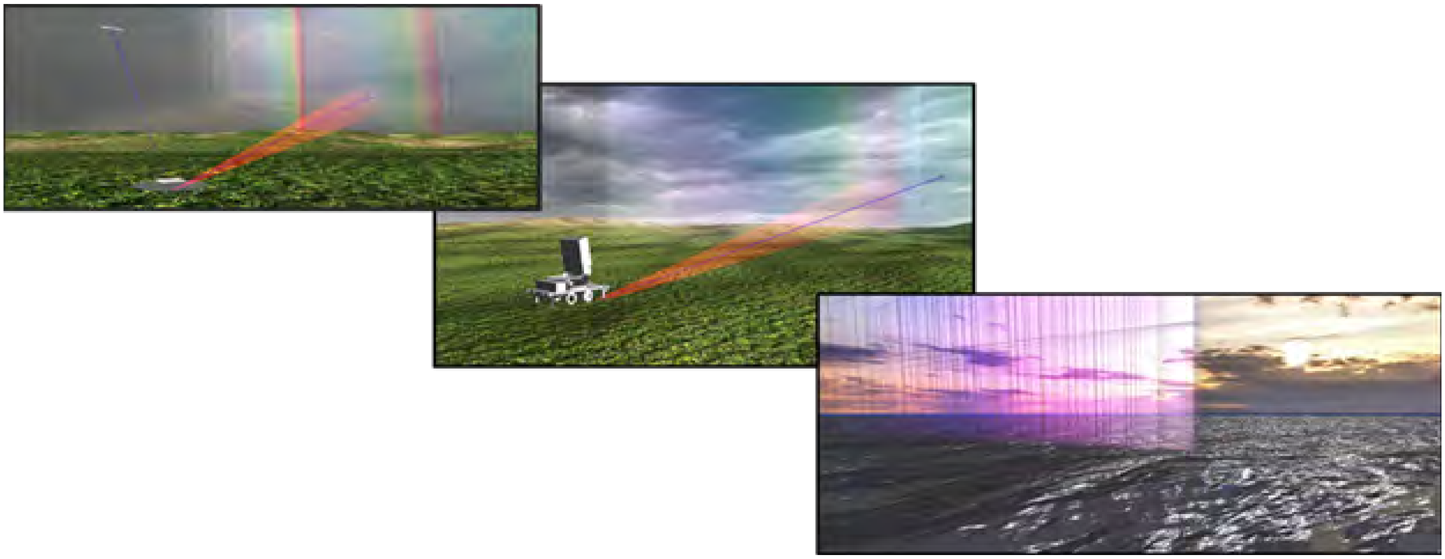


Figure 19. ETB HPM Propagation for Land and Maritime Environments

T&E efforts within COLE, to include Machine Assisted Exploitability Simulation and Testing for Resilient Operations (MAESTRO) and Cyber Automated Threat Discovery and Vulnerability Evaluation Reinforcement (CADAVER) programs.

In FY25, JTCG/ME deployed COLE version 4.1, enabling planning elements to model cyber networks, characterize properties, determine potential network vulnerabilities to cyber capabilities, develop TTP for cyber operations, and develop cyber capability requirements.

Major FY25 COLE achievements included a significant framework update, improvements for increasing automated data ingestion capabilities, including a Software Bill of Materials importer. Enhancements to the attack-path optimizer, which automatically generates possible courses of action, increase the thoroughness of options and speeds analytical efforts via automatic generation and tracking of options. COLE developers also integrated MITRE's D3FEND™ and the National Institute of Standards and Technology's Common Vulnerability Scoring System version 4.0. There were also built-in tool improvements to enable direct and immediate feedback to the COLE requirements and development teams.

JTCG/ME concluded its work with the JASP on the MAESTRO 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. This year's analysis included completion of two aircraft assessments.

JLF concluded its work to develop enhanced vulnerability discovery abilities to assist in rapidly and automatically characterizing, discovering, and reporting cyber vulnerabilities within complex software configurations through the CADAVER program. CADAVER is intended to leverage artificial intelligence and machine learning to allow identification of potential vulnerabilities and to mitigate cyber-attack access points. In FY25, a hardware model was constructed to simulate environmental effects on radio frequency communications. Combined, COLE and CADAVER ensure warfighters have the necessary tools to assess cyber effectiveness and vulnerability using tri-Service-approved data standards and streams.

In FY25, JTCG/ME continued to partner with the DoW Test Resource Management Center, initiating two projects which will carry through FY26. The first, to model and examine the potential for adversary attacks against test facilities, has already generated new models within COLE for removable media and data movement between networks. The second brings modifications to COLE's results page, enabling selected format outputs based on executive-level preferences.

JEAP

In FY25, JTCG/ME continued to develop an EMS fire – electronic attack JMEM, known as JEAP, with the capability to:

- Assess the impact of EMS effects on blue precision-guided weapons and salvos.
- Assess the effects of blue electronic attack capabilities against adversary emitter targets.

Ultimately, these JEAP tools will enable the warfighter to effectively prosecute adversary targets in contested, congested, and constrained EMS operations (as shown in Figure 20).

FY25 efforts included completion of a multi-year radar cross section data re-baseline for use in ACEL-based products for the joint community, as well as model-based systems engineering and data ontology models to support improved relational architecture and data streams for JEAP and Joint electronic warfare planning tools. JEAP also hosted and supported multiple user/supplier engagements within the joint electronic warfare community to underpin product requirements.

Additionally, the JEAP team provided interfaces to GPS operational awareness capabilities, as well as a Joint coordinated effort for enhanced analytical tools for assessing impacts to GPS guidance on weapon delivery and effectiveness based on operational use cases. An initial capability leveraging the GPS Interference and Navigation Tool (GIANT), and one blue high-fidelity weapon trajectory model, with other weapons initiated. JTCG/ME provided short-term support via reach-back to units and will continue to do so, until a more long-term product is fielded. JTCG/ME also supported an API effort to directly ingest high-fidelity models from DoW munition owners into GIANT. This API capability streamlines the ability to add high-fidelity 6-degrees-of-freedom models,

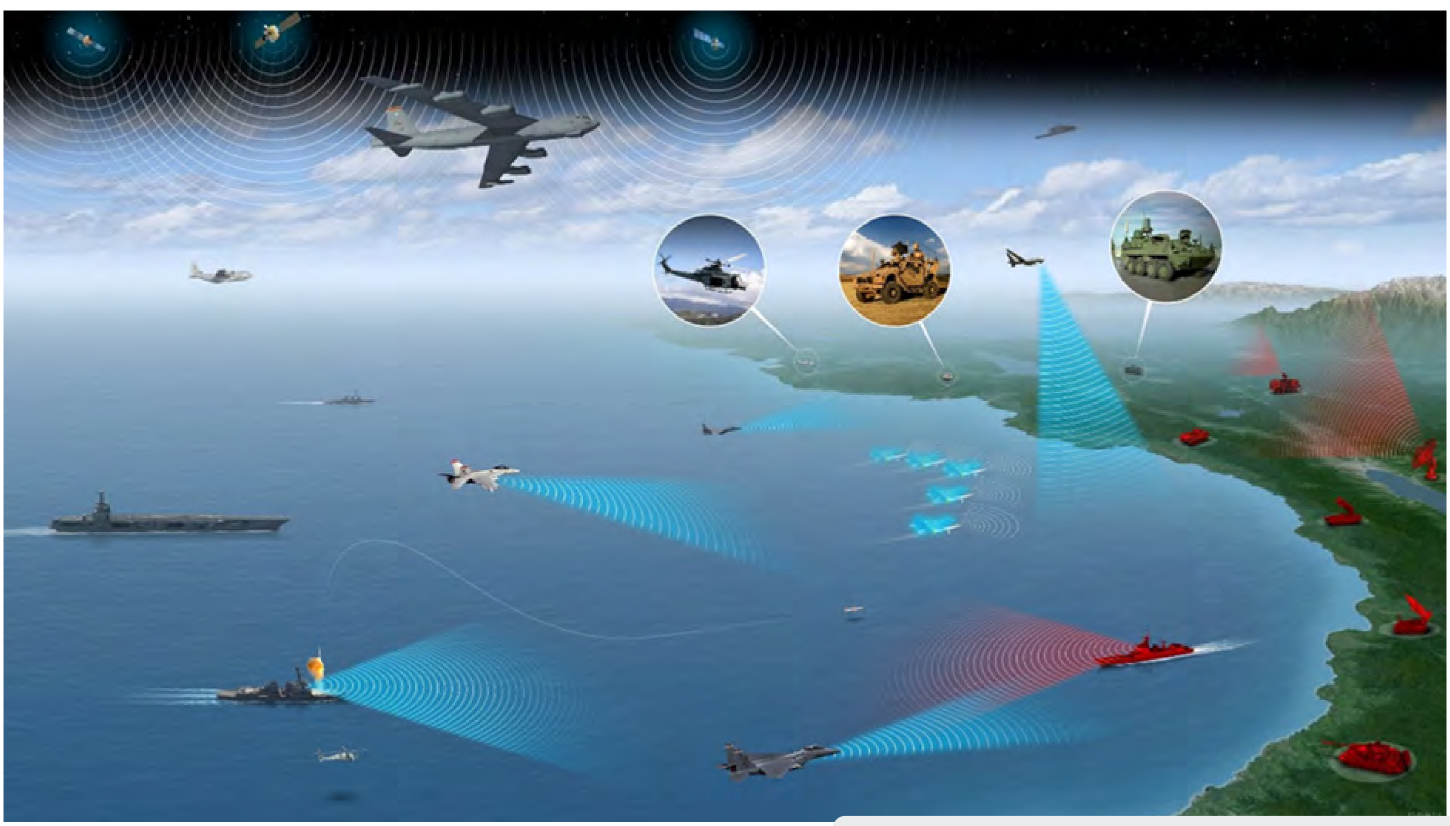


Figure 20. Sample Notional EMS Environment

while protecting proprietary, sensitive information, and thereby expediting and increasing the number of high-priority munitions models within GIANT.

Finally, JEAP developers started executing an integration path into an advanced framework that will dynamically depict high-fidelity electronic attack interactions against threat emitters leveraging ACEL framework. This includes naval surface assets via Navy models, air assets, and Army systems via the Builder software simulation environment. ACEL interfaces were initiated for GIANT, as well as interfaces to enhance visualization capabilities for two high-priority joint air systems.

» SUPPLYING WEAPONEERING TOOLS TO SUPPORT INTEROPERABILITY WITH U.S. ALLIES AND PARTNERS

In FY25, JTCG/ME provided weaponeering tools and data sets in support of training to 14 partner countries under Foreign Military Sales (FMS) or Foreign Military Financing agreements. This included the foreign release of the JWS product or JWS-derived data to approved partners, weapon effectiveness tables, collateral effects radii tables, and ATD 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 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 FY25, JTCG/ME continued 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.

In FY26, JTCG/ME will continue to provide ATD tools, methodology, and data through legally binding security cooperation activities, including FMS, in accordance with multiple laws and policies, which will enable international partners to employ U.S.-purchased and releasable munitions. JTCG/ME will continue to support and deliver JWS version releases and stand-alone Probability of Kill Look Up Tables to key coalition partners in support of current operations under FMS cases. FMS efforts are expected to increase, given new JMEM product lines. In addition, JTCG/ME will continue to support coalition interoperability via information exchange agreements forums.

Joint Test and Evaluation (JT&E)

In FY25, the Joint Test and Evaluation (JT&E) Program completed its shift from legacy test processes to modern and agile approaches for accelerated delivery of solutions to warfighter joint urgent operational needs (JUONs). The JT&E Program managed 14 agile reaction test (ART) projects, while also concluding its final joint test and quick reaction test (QRT) projects. FY25 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 JT&E Program focuses on joint requirements that cannot be economically or effectively tested within each of the individual Services and combatant commands (CCMDs). The Services and 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 protocol 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.

MISSION

The JT&E Program bolsters the warfighter capability by addressing JUON challenges through developing and testing proposed solutions using enhanced assessor methodology synergized with warfighting concept objectives, military exercises, complex mission threads, and kill webs to meet the DoW's strategic objectives.

FY25 KEY ACTIVITIES

In FY25, the JT&E Program Office (JPO) completed its transition from legacy test processes to modern and agile approaches with the conclusion of the final joint test and QRT projects. During FY25, JPO managed 14 ARTs to test and evaluate CONEMPs, CONOPS, and TTP to provide critical solutions to specific warfighter-identified DOTmLPF-P challenges within one year. These ART projects address challenges identified by North American Aerospace Defense Command (NORAD) and U.S. Northern Command (USNORTHCOM), U.S. Central Command, U.S. European Command, U.S. Indo-Pacific Command (USINDOPACOM), U.S. Southern Command, U.S. Space Command, U.S. Strategic Command, Marine Corps and Navy component commands, and OSD agencies.

» DEVELOPING EFFECTIVE CONOPS FOR INTEGRATION OF FIRES AND EFFECTS AT RESOLUTE HUNTER (DECIFER)

JPO chartered the DECIFER ART to develop, test, and validate a cross-functional CONOPS and TTP to codify and accelerate all-domain, human-machine-teamed, end-to-end kill webs and chains. The objective was to validate a standardized joint approach to integrating resilient, all-domain kill webs that hinder the effectiveness of joint fires in the maritime theater of operations. For its first field test, the ART team leveraged exercise RESOLUTE HUNTER 25-2, which is a capstone event for the Naval Aviation Warfighting Development Center's Maritime Intelligence Surveillance and Reconnaissance (MISR) Weapons School. The ART team used the field test data to validate the utility of the TTP to develop and execute effective, integrated, and resilient kill webs. The DECIFER ART will transition the joint MISR TTP – comprised of a mission planning process, coordination cards, and matrix – to the MISR Weapons School when it concludes in 2QFY26.

» GENERATIVE ARTIFICIAL INTELLIGENCE MODELS INTEGRATION (GAIMI)

NORAD and USNORTHCOM recognized that generative artificial intelligence tools, specifically large language models (LLMs), have the potential to help staffs become more efficient by reducing time needed for tasks such as document review. JPO chartered the GAIMI ART to develop and test a set of TTP to provide support and boundaries for staff use of LLMs for summarizing documents. The objective is to provide an LLM TTP to help ensure that time saved with the use of an LLM does not sacrifice output accuracy or introduce risk into the workflow. During FY25, the ART team conducted an observation event to collect data on staff use of a prototype TTP and a field test event to support validation of the TTP. The ART team will transition the GAIMI TTP and associated test products to NORAD and USNORTHCOM when the project concludes in 2QFY26.

» JOINT SUSTAINMENT NETWORK (JSN)

JPO chartered the JSN ART to develop, test, and evaluate TTP comprised of JSN procedures, data architecture, and decision processes that will enable CCMDs to see, understand, direct, and synchronize theater sustainment operations. During FY25, the JSN team engaged with various bureaus, boards, centers, cells, and working groups within USINDOPACOM J4 to understand the types of logistics information leadership requires to support decision-making. The team also observed exercise PACIFIC SENTRY and met with munitions and fuels planners to discuss their requirements. At USINDOPACOM's request, JPO paused the JSN ART in August 2025 to allow for realignment of the CCMD's personnel resources to shifting defense priorities in its area of responsibility.

» JOINT GLOBAL HYPERSONIC OPERATIONAL SENSOR TASKING II (J-GHOST II)

In December 2024, JPO chartered the J-GHOST II ART to refine and test Global Sensor Management CONOPS and real-time TTP for space and ground missile warning, missile defense, space domain awareness, allied, and commercial sensors to detect, task/cue, track, and report. The ART objective is to improve track custody of trans-regional threats. The ART will build on findings and recommendations from the FY24 J-GHOST I QRT and input from subject matter expert working groups for TTP development and refinement prior to field testing in 1QFY26.

» JOINT INTERAGENCY PARTNERSHIPS UTILIZING LOWER 3GHZ SPECTRUM FOR EFFICIENCY (JI-PULSE)

In October 2024, JPO chartered JI-PULSE as a JPO-Direct ART (J-DART) to evaluate proposed spectrum-sharing technologies and techniques capable of supporting commercial spectrum users without compromising DoW mission capabilities in a complex spectrum environment. The J-DART team will plan and execute test activities in coordination with the Services, CCMDs, Joint Staff, OUSW(A&S), OUSW(R&E), DoW Chief Information Officer, industry, and other stakeholders. Additionally, the JI-PULSE J-DART will inform U.S. Government stakeholders of spectrum-sharing interference risks, mitigations, standards, conditions, and future test resource requirements.

» EXPEDITIONARY WARFARE DECISION SYSTEM II (EWDS II)

In May 2025, JPO chartered the EWDS II ART to develop TTP to enhance the ability of joint forces to detect, classify, localize, and track surface and sub-surface threats within an anti-access/area denial (A2/AD) environment using a small-footprint format. The objective is to enable improved expeditionary warfare decision-making in contested environments. In 4QFY25, the ART team convened TTP working groups and a joint warfighter advisory group to gain input from the joint expeditionary community to support drafting and refining the initial EWDS II TTP before field testing in FY26.

» PROJECT VESUVIUS

In February 2025, JPO chartered the Project VESUVIUS ART to develop, test, and evaluate a CONEMP for collaborating with mission partners in the dynamic utilization of robotics and autonomous systems (RAS) through a series of demonstration events. RAS provide significant operational advantages by using kinetic or non-kinetic payloads, providing sensor and track data, and utilizing tactical formations to accomplish specific mission objectives. The ART team is utilizing the demonstration events to examine how the numbered fleets' Maritime Operations Centers could best employ RAS alongside mission partners and joint/allied forces. In 4QFY25, the ART conducted its first field test in coordination with stakeholders to support CONEMP refinement.

» JOINT COMBAT ASSESSMENT TEAM (JCAT) – FORENSIC OPERATIONS AND REMOTE COLLECTION EVALUATION (J-FORCE)

In January 2025, JPO chartered the J-FORCE ART to develop, refine, and enhance modern JCAT TTP. The JCAT collects and analyzes U.S. aircraft combat damage and losses to develop the requirements for joint aircraft survivability solutions that provide force protection and remedy operational shortfalls. The goal of the ART is to support JCAT personnel by incorporating alternate tools and data sources into existing JCAT mission processes for effective conduct of time-critical vulnerability and survivability assessments in A2/AD environments. During FY25, the ART team participated in exercises TALISMAN SABRE and NORTHERN EDGE to gather data for TTP refinement. The J-FORCE ART will transition the final TTP to the Joint Aircraft Survivability Program Office for incorporation into the JCAT Pocket Guide.

» EARLY VERTICAL TAKE-OFF AND LANDING AIRCRAFT DEMONSTRATION (EVADE)

In May 2025, JPO chartered the EVADE J-DART to develop and test an EVADE CONEMP for the use of unmanned aerial systems performing various missions supporting ground forces. During 4QFY25, the J-DART team participated in flight test demonstrations at Webster Outlying Field, Maryland, and mission scenario demonstrations at Grand Sky, North Dakota, to support CONEMP development. Once finalized, the EVADE CONEMP will also serve as a document to inform the Joint Staff J7 Joint Warfighting Concept 3.0 and a future program of record.

» JOINT CONUS DIRECTED OVER-THE-HORIZON RADAR (J-CONDOR)

In June 2025, JPO chartered the J-CONDOR ART to develop, refine, and enhance modern TTP to assist joint forces in mitigating adversary A2/AD strategies and capabilities to maintain freedom of maneuver within designated areas of operations. U.S. Southern Command has undertaken digital enhancement of its CONUS-based high frequency over-the-horizon radar. This technological advancement provides an opportunity to develop TTP against similar adversarial systems. The goal of the J-CONDOR ART is to provide counter over-the-horizon radar TTP to give operational-level commanders greater confidence when employing air and maritime assets in an A2/AD environment. The ART will continue development of specific TTP annexes for the CONOPS previously developed during the FY24 J-CONDOR Joint Test.

» LOW EXPOSURE AIR DEFENSE USING PASSIVE SENSING (LEAD-UPS)

In June 2025, JPO chartered the LEAD-UPS ART to develop a CONEMP to enable kill chains featuring alternate sensors and effectors to support operations with air defense capabilities. The objective is to address the challenge posed by the proliferation of modern, low-cost unmanned aerial systems with the capability to detect and target mobile units using radio frequency and infrared emissions from personnel and equipment. The LEAD-UPS ART team will conduct test activities to develop and refine the CONEMP during FY26.

» NUCLEAR COMMAND, CONTROL, AND COMMUNICATION (NC3) CONDITION RISK CONTROL (NC3CON RC)

In June 2025, JPO chartered the NC3CON RC ART to develop a CONOPS to improve the efficacy of the pre-planned NC3CON RC actions. The intent is to posture the NC3 enterprise according to relative risk and mission assurance requirements. This U.S. Strategic Command requirement was identified based on recommendations from the NC3 Condition Risk Assessment QRT that concluded in February 2025. The NC3CON RC ART team will conduct test activities in FY26 to evaluate the various control measures for meeting the necessary threat-level posture across the NC3 enterprise.

» DELAYED DEPLOYMENT DEVICE – FIEVEL PAYLOAD (DDD-FP)

In July 2025, JPO chartered the DDD-FP ART to develop TTP that support the deployment of space capabilities. Space-based capabilities are essential to modern life and an indispensable component of U.S. military power. Ensuring the availability of these capabilities is fundamental to establishing and maintaining military superiority across all domains and advancing U.S. and global security and economic prosperity. The objective of the ART is to address maintenance, deployment timelines, and deployment coordination as well as define responsibilities and command and control relationships. The ART team will coordinate with the OSW Strategic Capabilities Office and stakeholders to develop, test, and finalize the DDD-FP TTP for transition to the U.S. Space Force in FY26.

» INDOPACOM JOINT FIRES CENTER (IJFC)

In July 2025, JPO chartered the IJFC ART to develop and validate TTP for the IJFC, which is composed of multi-Service/domain specialists from intelligence, fires, space, cyberspace, and information functions. The TTP will support defining roles and responsibilities and integrating diverse disciplines and specialties to incorporate multi-domain planning and execution to enable multi-domain fires. The ART is convening subject matter expert working groups to support TTP development prior to field testing in 2QFY26.

Test and Evaluation Threat Resource Activity (TETRA)






In FY25, 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 DoW systems and services. These critical, cross-Service and multi-domain threat evaluations included, but were not limited to, the contested electromagnetic spectrum (EMS) environment, the use of artificial intelligence (AI) in adversary systems, foreign materiel acquisition and exploitation, and assessments of adversary order-of-battle, capability, concept of operations, and tactics, techniques, and procedures (TTP). TETRA continued 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. TETRA provided management of the development of high fidelity space threat models and counterspace threat surrogates to support OT&E and LFT&E of space systems. TETRA managed 130 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

Established in 2000, TETRA is a joint duty initiative between DOT&E and the Defense Intelligence Agency (DIA). Its mission is to ensure that OT&E and LFT&E programs – as well as warfighter mission planning and training – are grounded in the latest intelligence analysis. TETRA is composed of a multidisciplinary team of DIA analysts, engineers, modelers, and scientists who deliver authoritative, timely assessments of the evolving multi-domain threat landscape to the OT&E and LFT&E Enterprise.

Specifically, TETRA:

- Produces intelligence-driven artifacts, analysis, models, and simulations analyzing current and emerging threats and targets.
- Facilitates the acquisition and exploitation of critical foreign materiel for testing and the development of threat and target surrogates.
- Leads the verification, validation, and certification of threat and target surrogates, encompassing both physical hardware and digital constructs such as models, simulations, and digital twins.
- Leverages emerging scientific advancements and technologies to forecast future threat and target capabilities.
- Explores, develops, and delivers innovative capabilities to DOT&E and the Intelligence Community (IC) to address complex OT&E challenges, including those involving AI-enabled human-autonomous teams and Superteams.

TETRA's integrative role across the acquisition, testing, and intelligence domains ensures tailored intelligence support and specialized products that meet the evolving demands of OT&E and LFT&E.

MISSION

In coordination with the DIA and the Services' intelligence production centers (IPCs), TETRA conducts analysis and supports the delivery of threat and target digital representations, surrogates, and foreign materiel to meet OT&E and LFT&E requirements.

FY25 KEY ACTIVITIES

» INTELLIGENCE ANALYSIS TO SUPPORT OT&E AND LFT&E

In FY25, TETRA improved the capabilities of 77 new and emerging threats and targets to support adequate evaluation of the operational effectiveness, suitability, survivability, and lethality of DoW systems and services. Specifically, TETRA:

- Hosted a Threat Systems Management Office (TSMO) threat surrogate capabilities presentation to DOT&E. This collaborative approach between TETRA and TSMO fused intelligence support with threat emulation assets and capabilities. Discussions improved DOT&E's awareness of TSMO's test asset availability leading to better informed decision-making for threat surrogate selections during operational test design.
- Reviewed live fire test results and analyzed survivability assessment data for an armored combat system, during multiple post-event damage assessment meetings. TETRA experts collaborated with T&E stakeholders to identify known capability gaps to ensure all relevant threats to the program are addressed. Stakeholders focused on systems survivability; threat trends and technologies; and modeling and simulation (M&S) threat emulation capabilities to enhance operational and live fire testing.
- Collaborated with NSA acquisition intelligence analysts to increase threat intelligence support to the Joint Simulation Environment and the Western Test Ranges. Topics included generic level of support NSA provides for a specific customer set, an overview for Future Warfighting Advantage Forum acquisition support efforts, and positioning testing efforts as support imperatives to acquisition efforts.
- Played a key role in advancing critical intelligence support to acquisition initiatives by hosting a workshop to foster collaboration

between TETRA, DOT&E, Joint Acquisition Intelligence for Mission Integration (JAIMI), National Air and Space Intelligence Center, and the Acquisition Intelligence Joint Integration Cell. Additional participants included J2F85 Battlespace Awareness and TETRA's Intelligence Digital Ecosystem (TIDE) development team. Stakeholders discussed JAIMI; Acquisition Intelligence Requirements Enterprise System; and Production Planning, Prioritization and Resourcing Framework tool status, development efforts, and funding pathways. TETRA presented TIDE beta testing results and discussed planned future capability developments. TETRA focused on increasing open collaboration between intelligence support to acquisition providers and consumers to improve utility of the Defense Intelligence Enterprise's threat support for the DoW acquisition community and T&E enterprise.

- Coordinated with Center for Countermeasures (CCM) to support Army Futures Command's threat representation requirements for upcoming testing for the Autonomous Transport System-Vehicle (ATS-V). CCM identified the capability to emulate adversary employment of lasers to degrade ATS-V Light Detection and Ranging sensors during testing. The capability to stress the ATS-V against operationally relevant threats supports assessing its suitability and survivability in a challenging environment.
- Supported a DoW-wide outreach to assess intelligence needs of acquisition-related customers. TETRA responded directly to collaboration opportunities intended for acquisition intelligence professionals and assisted DOT&E to capture Action Officer (AO) views on intelligence support received compared to their intelligence needs. DOT&E feedback helped assess utility of current forms of intelligence so stakeholders can define focus areas for customer adaptation to improve intelligence support processes, products, and delivery methods.
- Contributed to multiple threat working groups and critical threat studies that drive policies and regulations governing intelligence support to DoW 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.
- Delivered tailored threat intelligence support to DOT&E and the Conventional Prompt Strike (CPS) Program Office test planners, providing critical insights for evaluating CPS performance against cyber and kinetic threats in challenging realistic operational environments. TETRA's bespoke intelligence products significantly enhanced the operational and live fire testing capabilities supporting CPS by providing detailed information on potential strategic targets for lethality analyses. Collaborative discussions with DOT&E AOs overseeing related programs facilitated integration of intelligence findings across acquisition program equities. Responsive intelligence support enabled informed decision-making during test design phases, ultimately contributing to avenues that will improve the ability for the DoW T&E Enterprise to adequately assess program operational effectiveness, survivability, and lethality.
- Performed a comprehensive review of the classified Validated Online Lifecycle Threat (VOLT) report for a program under DOT&E oversight to ensure alignment with evolving cyber threats and to address vulnerabilities introduced by emerging technologies such as AI/machine learning (ML), 5G, and cloud infrastructure. This effort directly supports DOT&E's focus on improving cybersecurity and survivability while ensuring the system under evaluation meets rigorous operational resilience standards. By incorporating the latest validated threat intelligence, the revised VOLT informs test planning and risk mitigation strategies to assess the system's ability to withstand cyber threats under operationally realistic conditions while ensuring mission assurance and survivability.
- Delivered critical analytical threat support during the Missile Defense System (MDS) VOLT review ensuring accuracy of the program of record threat document used to guide operational and live fire testing, and drive threat surrogate

development. TETRA identified emergent threats, ensuring the MDS VOLT provides a comprehensive understanding of the evolving threat landscape and anticipated operational environment at distinct timeframes. TETRA worked with DOT&E to address their concerns and capture feedback for the Intelligence Production Center VOLT author to improve VOLT utility. This ultimately improves the ability of DOT&E and the OTAs to adequately assess the program's operational effectiveness, sustainability, survivability, and lethality.

- Hosted a series of AI training and AI Human-Autonomous Teaming (HAT) groups to validate research findings in terms of embedding AI functionality into various threat and Allied team dynamics and interactions. TETRA focused on first understanding DOT&E and IC experiences, challenges, and pain points along with approaches to leverage AI-driven analytics, decision support, and automation to enable AOs to better assess system performance and predict outcomes while optimizing resource utilization. TETRA is actively shaping the future of how AI will be used to support the T&E and IC communities.
- Continued the development of TETRA's TIDE – an AI/ML customizable web-based ecosystem to support trend analysis of threat intelligence data, understanding of AI-enabled and traditional electronic warfare, cyber threat analysis, and many more critical IC analysis functions to maximize AI tools and functionalities inside of the wider TETRA customer base. For example, 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 DoW acquisition systems.
- Provided multiple ongoing DOT&E critical cyber threat assessments for the defense of Guam. Threat assessment support included both DoW-owned/controlled infrastructure as well as critical on-island domestic infrastructure.
- 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.
- Supported multiple Service, Service OTAs, and wider U.S. cyber working groups like the NASA Cyber Threat Working Group to enable access to vital real-world cyber intelligence in the rapidly adapting adversarial cyber threat arena.
- In support of the DoW's CPS program, TETRA provided tailored cyber threat intelligence, delivering critical insights into adversary cyber capabilities that could target CPS-related command, control, and communications infrastructure. This support has enabled threat-informed risk assessments and ensured that CPS system development incorporates realistic, mission-relevant cyber threat scenarios. TETRA's cyber threat contributions have proven instrumental in enhancing test planning, validating system resilience, and informing mitigation strategies aligned with real-world adversary TTP. By integrating intelligence-driven cyber realism into the CPS T&E lifecycle, TETRA significantly elevates the operational effectiveness, survivability, and strategic credibility of this key national defense capability.
- Over the past year, the TETRA team has played a pivotal role in informing DOT&E on the evolving landscape of adversary cyber threats. Through the delivery of over 75 in-depth briefings to DOT&E AOs, TETRA provided timely, threat-informed insights spanning a wide range of cyber topics – including advanced persistent threats (APTs), emerging exploitation techniques, cyber-enabled EW, and radio frequency (RF)-based cyber operations. These engagements have ensured that DOT&E remains aligned with current and projected adversary capabilities while enabling the integration of realistic, intelligence-based cyber

threats into OT planning and execution. TETRA's ability to translate complex cyber intelligence into actionable guidance has been instrumental in shaping test strategies while facing today's evolving cyber threat environment and tomorrow's warfighting systems.

- Assessed threat intelligence, capability, and EW for OT&E of the Next Generation Jammer, EA-37B Compass Call, B-21, and multiple other high-priority air warfare platforms.

» KEEPING PACE WITH EMERGING THREATS AND TARGETS

In FY25, TETRA:

- Researched efforts across 38 AI-enabled EW projects resulting in the generation of 19 reports supporting five key areas: (1) development of threat cognitive EW models by Integrated Product Teams (IPTs); (2) creation of adaptive OT and developmental test (DT) environments; (3) design of test methodologies, data analysis frameworks, and performance metrics; (4) implementation of machine learning operations (MLOps) for rapid reprogramming and online learning; and (5) establishment of policies, processes, and guidance for T&E of AI-enabled systems. These efforts systematically identified and assessed existing tools, methodologies, and processes to address critical challenges in data collection, measurement, and analysis within the EW OT&E community. The final deliverables were consolidated into the Cognitive Electronic Warfare (CogEW) Compendium, which has been distributed to stakeholders across the T&E and IC.
- Continued development of the roadmap to close test capability gaps for the evaluation of U.S. space systems' resiliency against emergent threats. The Space EW and cyber roadmap led to demonstration of progress on potential counterspace EW threats and 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.
- Conducted a comprehensive T&E community survey and delivered a detailed assessment of test capabilities and gaps related to the survivability of uplinks for space assets. Leveraging collaboration with the Space T&E community, TETRA not only identified critical shortfalls in current test infrastructure and methodologies but also developed actionable solutions and investment recommendations to address these gaps.
- Coordinated closely with the U.S. Space Force Operational Test and Training Infrastructure (OTTI) and Intelligence Centers to advance space threat model development. The resulting models are designed to enable rigorous resiliency testing of military satellite communications and tracking, telemetry, and control signals across digital, hardware-in-the-loop (HWIL), and open-air environments – impacting all DoW space programs.
- Partnered with the Space T&E community to assess and address the impact of RF-enabled cyber threats on space assets from multiple attack vectors. TETRA initiated the development of new TTP to support the Space T&E community in countering these emerging threats. These efforts included evaluating current threat models, identifying gaps in test capabilities, and recommending enhancements to modeling, simulation, and test architectures.
- Collaborated with the National Space Intelligence Center (NSIC) to design and advance a Space Object Surveillance and Identification (SOSI) architecture, enhancing space domain awareness and space debris collision avoidance. This partnership focused on integrating authoritative threat models, advanced sensor data fusion, and real-time tracking methodologies to improve the detection, characterization, and monitoring of resident space objects.
- Established the Space T&E M&S Working Group, bringing together representatives from OTTI, NSIC, DOT&E, Missile and Space Intelligence Center (MSIC), National Ground Intelligence Center (NGIC), STARCOM S2, and Test Resource Management Center (TRMC). The group aims

to align M&S efforts across agencies to support operational testing of space systems.

- Launched the Space T&E RF HWIL Community of Interest (COI) to assess test capabilities and gaps in the Space T&E community. This COI addresses uplink survivability and RF-enabled cyber threat simulation, bringing together STARCOM, TRMC, the relevant IPCs, and service test labs to develop threat-representative architectures and validate system-of-systems models.

» 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 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. TETRA facilitated hundreds of 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, certification, 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 FY25, TETRA provided threat intelligence, validation, and certification expertise, as well as oversight, for 14 joint and Service threat validation efforts, including:

- The Navy's Next Generation Electronic Warfare Environment Generator (NEWEG).
- The F-35 and B-21 programs.
- The Next Generation Jammer to develop a method to validate and certify the radar electronic attack countermeasure tools, models, and simulations.
- The Joint Aircraft Mission Survivability Integrated Product Team.
- M&S gaps and verification, validation, and accreditation in support of MDS ground testing.

During FY25, TETRA finalized the development, validation, and delivery 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 FY25, DOT&E and TETRA delivered 21 new LIVE and WEEW systems and 9 new CHIMERA systems for installation at T&E sites and facilities. Moreover, TETRA provided programmatic oversight for MSIC'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 serves as the T&E and IC focal point for critical countermeasure developments as the organizer and lead for the RF and IR Collaboration Control Boards (CCBs). These RF and IR CCBs bring together leaders, technical representatives and developers, and subject matter experts from across the IC, 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 FY25, TETRA continued the 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.

TETRA leads the partnership between the intelligence production centers and the Space Force to produce counterspace threat models supporting OT&E of space systems in the National Space Test and Training Complex. TETRA also leads a focused model development effort for a high priority counterspace threat to facilitate OT of DoW 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 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. This enables realistic testing of blue force systems against complex threats to support F-35, B-21, and other Service warfare programs.

TETRA maintains 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.

» 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 Foreign Materiel Program (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 FY25, TETRA monitored, developed, and coordinated dozens of acquisition efforts. For the second year, TETRA also led Project Doctor Mafia, an essential and very successful Foreign Material Acquisition team, resulting in multiple critical first of kind capabilities for U.S. Service ranges.

TETRA continues to prioritize threat systems that test the vulnerability of U.S. weapon systems such as Active Protection System of ground combat vehicles, GPS-guided weapons, and the F-35 aircraft.

In FY25, TETRA:

- Developed DOT&E's Top 50 FMP Priorities list for FY26 to advocate for funding of FMP community efforts to anticipate, prioritize, collect, and manage FMP activities.

- Led critical foreign materiel acquisition and delivery of essential systems for U.S. support to an ally in a wartime environment.
- Led the reconstituted DoW 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.
- Produced and delivered two first of kind, low cost, high threat representative foreign material targets enabling OT, DT, and training against the most advanced foreign threats at scale and within budget, for multiple U.S. ranges.

APPENDIX

This page intentionally left blank.

Oversight List

This page intentionally left blank.

DOT&E Oversight List as of September 30, 2025

- .338 Norma Magnum Anti-Materiel, XM1224 (.338 NM AM)
- Abrams M1A1 SA; M1A2 SEP; APS
- Advanced Anti-Radiation Guided Missile - Extended Range
- Advanced Anti-Tank Weapon System - Medium (Javelin)
- Advanced Battle Management System
- Advanced Reconnaissance Vehicle (ARV)
- AEGIS Modernization (Baseline Upgrades)
- AIM-120 Advanced Medium Range Air-to-Air Missile
- AIM-260A Joint Advanced Tactical Missile
- Air and Missile Defense Radar (AMDR) / AN/SPY-6
- Air Force Integrated Personnel and Pay System (AF-IPPS)
- Air Force Intercontinental Ballistic Missile Fuze Modernization
- Air Force Next Generation Air Dominance
- Air Operations Center Weapon System Modifications
- Air Warfare Ship Self Defense Enterprise
- 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)
- 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
- CH-47F Modernized Cargo Helicopter
- CH-53K King Stallion
- Columbia Class SSBN - including all supporting PARMs
- Common Infrared Countermeasures (CIRCM)
- Conventional Prompt Strike
- Cooperative Engagement Capability (CEC)
- Cross-Domain Solutions
- 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 Office Solution (DEOS)
- Digital Modernization Strategy (DMS) – Related Enterprise Information Technology Initiatives
- DoD Healthcare Management System Modernization (DHMSM)
- Dry Combat Submersible (DCS)
- E-130J (Take Charge and Move Out) Recap
- E-2D Advanced Hawkeye
- E-7A Rapid Prototyping
- EA-18G - Airborne Electronic Attack
- EA-37B Compass Call Rehost
- Electronic Warfare Planning and Management Tool (EWPMT)
- Enterprise Air Surveillance Radar
- Enterprise Business Systems Convergence
- 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)
- F/A-18E/F Super Hornet Aircraft

DOT&E Oversight List as of September 30, 2025

- F-15EX
- F-22 - RAPTOR Advanced Tactical Fighter Aircraft
- 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
- FFG(62) Guided Missile Frigate
- Future Long Range Assault Aircraft (FLRAA)
- Future Operationally Resilient Ground Evolution Rapid Prototype
- Global Command & Control System - Joint (GCCS-J)
- Golden Dome for America
- Global Positioning System (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
- HH-60W Jolly Green II
- High Accuracy Detection and Exploitation System (HADES)
- Hypersonic Attack Cruise Missile
- Improved Threat Detection System
- Improved Turbine Engine Program (ITEP)
- Indirect Fire Protection Capability Increment 2 (IFPC Inc 2 MTA RP)
- Integrated Air and Missile Defense
- Integrated Air and Missile Defense of Guam
- Integrated Head Protection System (IHPS)
- Integrated Visual Augmentation System 1.2 Rapid Prototyping (IVAS 1.2 RP)
- 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 Transportation Management System
- KC-46A Tanker Modernization
- Key Management Infrastructure (KMI)
- LGM-35A Sentinel
- LHA 6 Flt I and associated PARMs
- Littoral Combat Ship (LCS) Mine-countermeasures (MCM) Mission Package
- Littoral Combat Ship (LCS), FREEDOM and INDEPENDENCE Variant Seaframes
- Long Range Hypersonic Weapon Ground Support Equipment (LRHW GSE MTA RF)
- Long Range Stand Off Weapon
- Lower Tier Air and Missile Defense Sensor
- LPD 17 Flt II
- M88A2 Heavy Equipment Recovery Combat Utility Lift Evacuation System (M88A2 HERCULES)
- Medium Landing Ship
- MH-139A Grey Wolf
- Mid-Range Capability (MRC)
- Military Global Positioning System (GPS) User Equipment Increment 1

DOT&E Oversight List as of September 30, 2025

- Mine Countermeasures Unmanned Surface Vehicle and payloads
- Missile Defense System
- Mission Partner Environment (MPE)
- Mk 48 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
- Mk21A Reentry Vehicle
- Mobile Advanced Extremely High Frequency Terminal
- MQ-25 Stingray
- MQ-4C Triton
- M-SHORAD Inc 3 - Next Generation Short Range Interceptor (M-SHORAD Inc 3 MTA RP)
- National Background Investigation Services
- Navy Next Generation Air Dominance F/A-XX
- Navy Personnel and Pay System
- Next Gen Overhead Persistent Infrared - Polar
- 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 - Geosynchronous Earth Orbit
- Next Generation Squad Weapons Weapons and Ammunition Rapid Fielding (NGSW W&A RF)
- Nuclear-Armed Sea-Launched Cruise Missile
- Offensive Anti-Surface Warfare Increment 1 (Long Range Anti-Ship Missile)
- Over The Horizon Weapon System
- Patriot Advanced Capability 3
- Precision Strike Missile Increment 1 (PrSM Inc 1)
- Proliferated Warfighter Space Architecture Tranche 1 Tracking Layer
- Proliferated Warfighter Space Architecture Tranche 1 Transport Layer
- Protected Tactical Enterprise Service
- Protected Tactical SATCOM
- Public Key Infrastructure (PKI)
- Resilient Missile Warning/Missile Tracking - Medium Earth Orbit
- Sentinel A4 Mod
- Ship Self Defense System (SSDS)
- Ship to Shore Connector
- Small Diameter Bomb Increment II
- Small Unmanned Surface Vehicle
- Space Command and Control - Advanced Launch Tracking and Analysis System
- Space Command and Control - KRONOS
- Stand In Attack Weapon
- Standard Missile 2 (SM-2) including all mods
- Standard Missile-6 Including all mods and variants
- Strategic Mission Planning and Execution System
- Surface Electronic Warfare Improvement Program
- Survivable Airborne Operations Center E-4C
- 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)
- Three-Dimensional Expeditionary Long-Range Radar
- Torso & Extremity Protection (TEP)
- Trident II (D-5) Submarine-Launched Ballistic Missile (SLBM)
- USAF Collaborative Combat Aircraft
- V-22 Osprey Joint Services Advanced Vertical Lift Aircraft (V-22)
- VC-25B
- VH-92A Presidential Helicopter

DOT&E Oversight List as of September 30, 2025

- VIRGINIA Class SSN 774
- Vital Torso Protection (VTP)
- 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)
- XM30 Combat Vehicle MTA RP (XM30 MTA RP)

DOT&E Activities

This page intentionally left blank.

Table 1. FY25 DOT&E Independent System Evaluation Reports

Program	Date
Early Fielding Reports (EFRs)	
Next Generation Jammer Mid-Band (NGJ-MB) EFR	November 2024
F-22 Release 3 (R3) Report	February 2025
F/A-18E/F and EA-18G System Configuration Set H18 Release 3 EFR	March 2025
Aegis Advanced Capability Build (ACB) 16 Capability Package (CP) 22-1 EFR	March 2025
Air Operations Center - Weapon System (AOC-WS) Block 20 EFR	May 2025
MQ-4C Triton Integrated Functional Capability (IFC) 4.2.1 EFR	May 2025
Next Generation Squad Weapons (NGSW) Weapons and Ammunition (W&A) and NGSW Fire Control (NGSW-FC) EFR	June 2025
Follow-on Operational Test and Evaluation (FOT&E) Reports	
Dry Combat Submersible (DCS) FOT&E Test Report	October 2024
Stryker Infantry Carrier Double-V Hull A1 30mm Combined FOT&E and LFT&E Report	November 2024
Public Key Infrastructure (PKI) Inc. 2 FOT&E Report – Suitability and Cyber Annex Update	November 2024
MHS GENESIS Revenue Cycle Expansion (RevX) FOT&E Report	February 2025
Tomahawk Weapon System FOT&E Report	March 2025
Initial Operational Test and Evaluation (IOT&E) Reports	
F/A-18 Infrared Search and Track (IRST) Block II IOT&E Report	February 2025
Space-Based Infrared System (SBIRS) Survivable/Endurable Evolution (S2E2) IOT&E Report	March 2025
Joint Operational Medicine Information Systems (JOMIS) – Medical Common Operating Picture (MedCOP) IOT&E Report	May 2025
T-AO 205 *John Lewis*-Class Fleet Replenishment Oiler Combined IOT&E and LFT&E Report	May 2025
Next Generation Jammer Mid-Band (NGJ-MB) IOT&E Report	July 2025
Live Fire Test and Evaluation (LFT&E) Reports	
B-21 LFT&E Fuel Tank Hydrodynamic Ram Report	October 2024
Family of Medium Tactical Vehicles (FMTV) A2 Low-Velocity Airdrop (LVAD) LFT&E Report	March 2025
F-15EX Eagle II Combined IOT&E and LFT&E Report – Live Fire Annex Update	March 2025

Table 1. FY25 DOT&E Independent System Evaluation Reports, continued

Program	Date
Operational Assessment (OA) Reports	
Family of Advanced Beyond Line-of-Sight Terminals (FAB-T) Force Element Terminal (FET) Operational Assessment One (OA-1) Report	March 2025
Lower Tier Air and Missile Defense Sensor (LTAMDS) OA Report	April 2025
F-16 Integrated Viper Electronic Warfare Suite (IVEWS) Early OA Report	May 2025
Precision Strike Missile (PrSM) Increment 1 OA Report	July 2025
Operational Demonstration (Ops Demo) Reports	
Indirect Fire Protection Capability Increment 2 (IFPC Inc 2) Ops Demo Report	April 2025
Operational Test and Evaluation (OT&E) Reports	
Defense Enterprise Office Solution (DEOS) Impact Level 6 (IL6) Cyber Survivability Report	December 2024
Key Management Infrastructure (KMI) Capability Increment 3 Release 0 Operational Verification Report	June 2025
Air Operations Center - Weapon System (AOC-WS) Cooperative Vulnerability and Penetration Assessment (CVPA) Report	July 2025

Table 2. Other FY25 DOT&E Reports

Program/Topic	Date
Legislative Reports/Responses	
Observations on the Employment of the Joint Fires Network (JFN) Baseline Report	October 2024
Electromagnetic Protection (EP) Testing for Spectrum-Dependent Systems Under DOT&E Oversight: FY24 NDAA Section 1686 Interim Report	November 2024
Annual Report of Electromagnetic Testing (EP) for Spectrum-Dependent Systems (FY24 NDAA Section 1686 Report)	January 2025
Testing for Artificial Intelligence System Survivability (118-188 - SASC Report on FY25 NDAA)	March 2025
Observations on the Employment of the Joint Fires Network (JFN) Bi-Annual Report	April 2025
Missile Defense System Report	
2024 Assessment of the Missile Defense System (MDS)	February 2025
Special Reports	
U.S. Special Operations Command (USSOCOM) Cyber Assessment for FY22 and FY23	November 2024

Table 2. Other FY25 DOT&E Reports, continued

Program/Topic	Date
Observations on the Mission Effects of Common Cyber Vulnerabilities	January 2025
Demonstrated Risks to Military Platforms and Connected Command and Control via Civil Data Links and Tactical Data Links	February 2025
Certification of Appropriateness and Risk Assessment of Services' Planned Test Strategies for Approved Middle Tier of Acquisition (804) and Accelerated Acquisition Programs	February 2025
U.S. Central Command (USCENTCOM) Cyber Readiness Campaign (CRC) Report for FY24	April 2025
Recommendations for NC3 Sensing and Monitoring Strategy	May 2025
FY24 U.S. Navy Cyber Assessments	May 2025
U.S. Transportation Command (USTRANSCOM) Cyber Assessment for FY23 – 24	July 2025
DOT&E Cyber Assessment of COSMIC RAM 25	July 2025

Table 3. FY25 DOT&E-Approved TEMPs and Test Strategy Documents (Live Fire Test Strategies marked with *)

Program Document
AIAMD 2025 SAMP T&E Annex
AIM-9X Block II Operational Flight Software 9.5 TEMP and Test Plan Approval*
Air Operations Center – Weapon System TES approval
Annex E – Extended Range Guided Multiple Launch Rocket System TEMP Annex Acquisition Category IC*
Approval for TEMP TEIN 1787 Tab 5 for the F/A-18E/F and EA-18G Flight Plan FOT&E
Approval of the Joint Cyber Warfighting Architecture TES
Next Generation Overhead Persistent Infrared (NG-OPIR) TEMP, FORGE BA/TI Delivery #2 Annex
Joint TEMP for 371-04 (rev 1) Addendum MK 48 Mod 7 Advanced Processor Build upgrades
E-2D TEMP Revision G Approval
F-15EX FOT&E TEMP
F-35 Block 4 CUI and Classified TEMP Annex 3

Table 3. FY25 DOT&E-Approved TEMPs and Test Strategy Documents (Live Fire Test Strategies marked with *)

Program Document
Lower Tier Air and Missile Defense Sensor (LTAMDS) TEMP
Master Test Strategy for Airborne Network Extension (ANE) – SkyTower II (ST II) Payload
MK 58 Compact Rapid Attack Weapon (CRAW) Very Lightweight Torpedo TI-1 Master Test Strategy Approval
Mobile Advanced Extremely High Frequency Program Master Test Strategy
Navy NGAD F/A-XX TEMP Approval*
Tactical Intelligence Targeting Access Node (TITAN) TES Middle Tier of Acquisition (MTA) Rapid Prototyping
Tactical Operations Center – Light TES approval
TEMP Joint Light Tactical Vehicle (JLTV) Follow-on Contract*
TEMP for the Indirect Fire Protection Capability (IFPC) Increment 2 Milestone C*
TES for Cartridge, .338 Norma Magnum: Anti-Materiel (ACAT IV)*
TEMP for Armor Piercing Family (APF), 30X173MM: XM1170 Armor Piercing Fin Stabilized Discarding Sabot With Trace (APFSDS-T)*
TEMP For the XM30 Combat Vehicle*
TEMP for Mounted Assured Positioning, Navigation, And Timing System Generation II
TEMP for the CH-47F Block II Program Cargo Helicopters Project Management Office
TEMP for the Precision Strike Missile (PrSM) Increment 1 Acquisition Category 1 B*
TES Autonomous Transport Vehicle – System (ATV-S) Middle Tier of Acquisition-Rapid Prototype (MTA-RP)
TRIDENT II D5 Life Extension Second Variant (LE2) iTEMP

Table 4. FY25 DOT&E-Disapproved TEMPs and Test Strategy Documents

Program Document
Integrated Master Test Plan (IMTP) v26.1 * Disapproval

Table 5. FY25 DOT&E-Approved Test Plans

Program Document
603 Air Operations Center-Weapon System (AOC-WS) Cooperative Vulnerability and Penetration Assessment (CVPA)
Advanced Processor Build (APB) 6 Software on the MK 48 MOD 7 Common Broadband Advanced Sonar System Torpedo FOT&E Plan Change 1
Aegis Advanced Capability Build (ACB) 16 BL 9 Cyber Operational Test Plan
Aegis ACB 16 BL 9 Cyber Operational Test Plan - Update
AIM-9X Block II Operational Flight Software 9.5 Data Collection Plan
AIM-9X Block II Operational Flight Software 9.5 TEMP and Test Plan
Air and Missile Defense Test Directorate (AMDTD)-Requested Changes to the Sentinel A4 IOT Phase I OT Plan (OTP)
AN/APR-39E(V)2 Modernized Radar Warning Receiver FOT&E OTP
AOC-WS ARE 24-09 Risk Concurrence
AOC-WS ARE 25-05 Risk Concurrence
Amphibious Combat Vehicle 30 (ACV-30) Program OTP
Army Integrated Air and Missile Defense (AIAMD) Integrated First Test Campaign 2025 Test Plan
AIAMD Cyber Test Plan
CH-53K King Stallion FOT&E (OT-D2) Plan (TEIN 1683)
Classified Test Plan
Classified Test Plan
Classified Test and Evaluation Plan
Cloud Based Command and Control (CBC2) Operational Assessment (OA) Test Plan Update
Columbia Operational Test B3 (OT-B3) Test Plan
Conventional Prompt Strike (CPS) Arena Test 4 Test Plan
CPS Joint Flight Campaign (JFC)-4 Test Plan
CVN 78 IOT&E Test Plan Change Transmittal 2
Defense Enterprise Office Solution (DEOS) Impact Level 5 (IL5) OT Cyber Survivability Test Assessment Plan

Table 5. FY25 DOT&E-Approved Test Plans, continued

Program Document
Detailed Test Plan (DTP) for the First Article Test (FAT) of the Next Generation (NG) Integrated Head Protection System (IHPS)
DTP for the FAT of the Soldier Protection System (SPS) Torso Extremity Protection (TEP) Ballistic Combat Shirt (BCS)
DTP for the FAT of the SPS Vital Torso Protection (VTP) Lightweight Small Arms Protective Insert (LSAPI) Gen I
DTP for the FAT of the SPS Torso and Extremity Protection Modular Scalable Vest
Deviation from the Approved HH-60W Jolly Green II (Combat Rescue Helicopter) FOT&E Plan
Distributed Common Ground Station (DCGS) Radio Frequency (RF) Minimum Viable Capability Release (MVCR) IOT&E Test Plan
DCGS CVPA Plan
DCGS–Navy (DCGS-N) Quick Reaction Assessment (QRA)
Dry Combat Submersible (DCS) Platform Integrated Control System (PICS) FOT&E Test Plan
E-2D Delta System Software Configuration (DSSC) 5.1 Test Data Collection Plan
E-2D DSSC 5.1 Test Plan
E-2D Hawkeye Integrated Training System DSSC-4 Test Plan
E-7 Live Fire Ullage Ignition Test Plan
EA- 37B Compass Call Block 3 Integrated Test Plan
Enhanced Polar System – Recapitalization (EPS-R) OUE Test Plan
F-15EX FOT&E Test Plan
F-22 Release 4 OFP Force Development Evaluation Test Plan
F-35 30R08 Test Plan
F-35 ALIS CVPA and Adversarial Assessment (AA)
F-35 Annual Suitability Test Plan
F-35 United Operational Test Team (UOTT) Response to Director Approval Memo for F-35 Annual Suitability Test Plan
FA-18 E/F and EA-18G SCS CIDD 25 FOT&E Test Plan Data Collection

Table 5. FY25 DOT&E-Approved Test Plans, continued

Program Document
FA-18 E/F and EA-18G SCS CIDD 25 FOT&E Test Plan
Future Operational Resilient Ground Evolution (FORGE) BATI OD#2 CVPA Plan
FORGE Operational Utility Evaluation (OUE) and Adversarial Assessment (AA) Test Plan
Future Tactical Uncrewed Aircraft System (FTUSA) Inc 2 CPVA OTP
Gerald R. Ford (CVN 78) Class Nuclear Aircraft Carrier IOT&E Test Plan Update 1
Gerald R. Ford (CVN 78) Total Ship Survivability Test
Global Positioning System (GPS) Next Generation Operational Control System (OCX) Cybersecurity Event Plan
GPS Integrated System Test 3-3 Phase 4 Gray Eagle Lead Platform Testing of Military GPS User Equipment (MGUE) Inc 1 OTP
GPS OCX IOT&E Plan
Guided Multiple Launch Rocket System Rocket with Enhanced Alternative Warheads (GMLRS EAW) Live Fire Test Design Plan
Healthcare Delivery Cyber Test Plan
Joint Biological Tactical Detection System (JBTDS) DT/OT Live Agent Aerosol Test Production and Deployment DTP
JBTDS MOT&E OTP
Joint Cyber Command and Control OUE Plan
Joint Light Tactical Vehicle (JLTV) A2 LFT&E TDP
Joint Planning and Execution Services (JPES) CVPA Test Plan
KC-46A IOT&E Test Plan Deviation
Key Management Infrastructure (KMI) Capability Increment 3 Release 0 Operational Verification Plan
KMI Capability Increment 3 Release 0 Operational Verification Cyber Survivability Assessment Plan Annex
M10 Booker Combat Vehicle (BCV) IOT&E OTP Revision
Maritime Strike Tomahawk (MST) Quick Reaction Assessment (QRA) Test Plan
MH-139 CVPA Plan

Table 5. FY25 DOT&E-Approved Test Plans, continued

Program Document
MH-139A IOT&E Plan
MH-139A IOT&E Plan Change
Navy LRASM 1.1 IOT&E Test Plan
Navy NGAD F/A-XX Alternate LFT&E Strategy
OA-1K Armor Test Plan Addendum
OA-1K Fuselage Fuel System Test Plan
OA-1K Wing Fuel System Vulnerability Test Plan
Precision Strike Missile (PrSM) IOT&E Test Plan
PrSM Limited User Test (LUT) OTP
Sentinel A4 IOT&E Phase 1 OTP
Sky Tower II Test Plan
Space Domain Awareness Command and Control Test Campaign Plan
Space-Based Infrared System (SBIRS) Survivable Endurable Evolution (S2E2) IOT&E Test Plan
Surface Electronic Warfare Improvement Program (SEWIP) Block 2 FOT&E Plan
SEWIP Bock 2 FOT&E Plan – Update
SEWIP Block 3 IOT&E Test Plan
Survivable Airborne Operations Center (SAOC) Alternate Test Plan
Theater Blood OA Plan
Three-Dimensional Expeditionary Long-Range Radar (3DELRR) OA Test Plan
USS *Gerald R. Ford* (CVN 78) Integrated Combat System (ICS), Ship Self-Defense System (SSDS), and Cooperative Engagement Capability (CEC) IOT&E Test Plan

Service Secretary Comments

This page intentionally left blank.

SECRETARY OF THE ARMY
WASHINGTON

25 FEB 2026

MEMORANDUM FOR DIRECTOR, OPERATIONAL TEST AND EVALUATION, 1700 DEFENSE PENTAGON, WASHINGTON, DC 20301-1700

SUBJECT: Department of the Army Response to the Fiscal Year 2025 Director, Operational Test and Evaluation Annual Report

1. Thank you for the opportunity to respond to the Fiscal Year 2025 (FY25) Director, Operational Test and Evaluation Annual Report. We appreciate the effort and diligence that went into its preparation and adjudication.

2. The Army disagrees with the assessment of the Lower Tier Air and Missile Defense Sensor. The Army asserts that the current test articles are production representative and that the testing scheduled for FY26 is an Initial Operational Test and Evaluation (IOT&E) event, not an Operational Assessment. Additionally, the Army requires that a Beyond Low-Rate Initial Production Report, not an Early Fielding Report, be issued following the FY26 IOT&E to support a Full Rate Production Decision.

3. For the Next Generation Squad Weapon and Fire Control program, the Army is now pursuing the M8 Carbine version which addresses Soldier feedback and Human Systems Integration concerns. The Army is also exploring a variety of alternate sight options as a lower cost alternative to the M157.

4. The Army is committed to accelerating the delivery of effective capabilities to our Soldiers, an objective that requires the active cooperation of your office. We look forward to continued collaboration and appreciate your support of Army Programs and our Soldiers.

Dan Driscoll

This page intentionally left blank.

SECRETARY OF THE AIR FORCE
WASHINGTON

MAR 0 5 2026

MEMORANDUM FOR DIRECTOR, OPERATIONAL TEST AND EVALUATION

SUBJECT: Department of the Air Force Response to Fiscal Year (FY) 2025 Director, Operational Test and Evaluation (DOT&E) Annual Report

I appreciate the opportunity to review the FY25 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 War test enterprise.

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.

Troy E. Meink

cc:
AF/CV
SF/VCSO
AF/TE

This page intentionally left blank.

DOT&E did not receive a response from the Secretary of the Navy in time to be printed. However, if a response is received by March 16, 2026, it will be posted on DOT&E's public website with the rest of the FY25 Annual Report: https://www.dote.osd.mil/annualreport/

This page intentionally left blank.

Commonly Used Acronyms

This page intentionally left blank.

The following acronyms are used throughout this Annual Report:

- #QFY## — # Quarter Fiscal Year ##
- CONUS — Continental United States
- DoD — Department of Defense
- DOT&E — Director, Operational Test and Evaluation
- DoW — Department of War
- FAA — Federal Aviation Administration
- 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
- NASA — National Aeronautics and Space Administration
- NATO — North Atlantic Treaty Organization
- NDAA — National Defense Authorization Act
- NIPRNet — Non-classified Internet Protocol Router Network
- NSA — National Security Agency
- OCONUS — Outside the Continental United States
- OSD — Office of the Secretary of Defense
- OSW — Office of the Secretary of War
- OT&E — Operational Test and Evaluation
- OUSW — Office of the Under Secretary of War
- SecWar — Secretary of War
- SIPRNet — Secret Internet Protocol Router Network
- T&E — Test and Evaluation
- TEMP — Test and Evaluation Master Plan
- URL — Uniform Resource Locator
- USB — Universal Serial Bus
- USW(A&S) — Under Secretary of War for Acquisition and Sustainment
- USW(I&S) — Under Secretary of War for Intelligence and Security
- USW(P&R) — Under Secretary of War for Personnel and Readiness
- USW(R&E) — Under Secretary of War for Research and Engineering

This page intentionally left blank.

Index of Programs

This page intentionally left blank.

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

S

T

www.dote.osd.mil