Director, Operational Test & Evaluation

January 2023

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

Nickolas H. Guertin
Director

Director's Introduction

On December 20, 2021, I took an oath to support and defend the Constitution of the United States of America when I became the eighth Director, Operational Test and Evaluation. Since then, the security environment has changed in ways few expected. Full-scale war returned to the European continent for the first time in decades, fully exposing the consequences of Russian aggression; and the very real need for, and strength of, our alliances and partnerships in Europe and around the globe. Simultaneously, the People's Republic of China continued to expand rapidly its military capacity and capability, as well as its economic reach. As the 2022 National Defense Strategy (NDS) states, China will remain "our most consequential strategic competitor" for decades to come. In addition to China and Russia, other threats, including Iran, North Korea and non-state actors, persist and continue to expand their capabilities. The extensive proliferation of advanced threat capabilities makes for a more uncertain world and increases warfighter risk.

Our national defense depends on adept and agile Armed Forces, equipped with superior technology, training, and tactics, all of which must continue to improve over time in ever-shorter cycles. The conditions described above amplify the urgency of ensuring that our women and men in uniform have exactly what they need, when they need it. The test and evaluation community must find new ways of performing our duties to support faster fielding of combat-relevant capability.

Independent operational and live fire test and evaluation that focus on the effectiveness, suitability, survivability, and lethality of evolving and innovative capability are integral to fulfilling my obligation to the warfighter. Strategic decision makers, tactical planners, and warfighters can only execute their missions with confidence when armed with the knowledge that system performance has been tested in operationally representative scenarios. As noted in the NDS, to sustain and strengthen deterrence, DOD must "design, develop, and manage a combat-credible U.S. military fit for advancing our highest defense priorities." Determining that we have weapons that work – evaluated independently and without bias – is the heart of DOT&E.

TESTING TO DETERMINE HOW WEAPONS WORK, FASTER

Building on the assertions I made in last year's DOT&E Annual Report, we must continue to change and modernize how we perform test and evaluation. We have redoubled our efforts to transform as a central leader in the T&E ecosystem. As Secretary Austin said in the 2022 NDS, "business as usual at the Department is not acceptable." With this challenge firmly in mind, DOT&E, with our DOD and Services partners, took a hard look at development and acquisition methods, the associated technology pipelines, concepts of operation, threat intelligence, and plans for improving capabilities in ways that can keep up with warfighters' needs. Based on rigorous research and informed by our communities' experience, we sought to better understand how to be effective testers when all these things are evolving rapidly and continuously. We have resolved that, to fulfill our obligations to the warfighter and the Congress, test and evaluation must embrace innovation to address broad and deep change.

The Joint Force, with international partners, will engage increasingly adaptive and technologically sophisticated adversaries in multi-domain operations. They will rely upon systems of systems and kill webs that require reliable, resilient interoperable capabilities, informed by all-domain command and control. They will both use, and need to counter, a plethora of technologies, such as hypersonic weapons, systems based on artificial intelligence, machine learning and autonomous action, swarming un-crewed systems, offensive and defensive cyber operations, and space-based systems – with many more new capabilities and novel employment methods certain to come on ever-shorter intervals.

Timely, thorough assessment of new capabilities requires the right infrastructure, the right tools, and a workforce of the right size with the right expertise. What is "right" is not static. It changes as warfighting environments, technologies, innovative capabilities, and novel tactics (both ours and our adversaries') change. In order to be adequately prepared, the T&E community must develop test methods and a test ecosystem that can rapidly adapt to warfighter needs, new technologies, and fluid tactics – now and well into the future.

2022 DOT&E STRATEGY UPDATE

The 2022 DOT&E Strategy Update I signed in June lays the foundation for how the T&E enterprise will address the operational test and evaluation challenges we face and continue to be the key to weapons that work, delivered faster than ever before. Its objectives are a combination of commonsense changes and fresh initiatives.

Test the Way We Fight. Testing the way we fight encompasses the fundamental requirement for operationally representative T&E that determines, with confidence, whether a system will be effective, suitable, survivable, and lethal in the hands of a warfighter facing a thinking enemy. It means architecting T&E around current, validated mission threads; accurately replicating the anticipated operating environment; and employing realistic warfighting tactics, techniques, and procedures during testing. All of these elements are dynamic. T&E infrastructure, tools, and processes must be able to scale and adapt quickly to reflect changes when they arise and efficiently evaluate kill web and system-of-systems performance.

Accelerate Delivery of Weapons That Work. Operational T&E must contribute to accelerating delivery of weapons that work. In the near term, OT&E will achieve the biggest gains through automation and more widespread use of digital technologies. The 2022 DOT&E Strategy Update addresses establishing enterprise-level T&E data management. Test and evaluation activities generate enormous quantities of data. At the individual program level, sharing data among all stakeholders can be cumbersome and time-consuming, slowing analysis and, ultimately, acquisition decision making. In the aggregate, the Department risks losing knowledge that could dramatically affect research, development, testing, and acquisition. We do not have a clear view of the test related data that exists across the entire DOD, and have identified the need to improve access to that data in order to extract new insights. Automated networked computing infrastructure that collects, hosts, and conducts streaming analysis of test data across all of DOD – while adhering to DOD's data strategy – will accelerate the fielding of robust, combat-credible capabilities.

Improve Survivability in Contested Environments. While U.S. forces remain dominant, no warfighting domain is uncontested. Improving survivability in these environments is an ever-changing area of our practice that is paramount to the Nation. Cyber, electromagnetic spectrum (EMS), and space threats are examples of tremendous current challenges to warfighting forces. In the near term, the T&E ecosystem must improve and expand its means of testing cyber and EMS survivability in mission scenarios, and replicating the space environment and space threats, both kinetic and non-kinetic. The acquisition community must dedicate more programmatic time and resources to assessing performance in contested environments.

Pioneer T&E of Systems Built to Change Over Time. The practice of increasing warfighter capability by improving our existing systems is an affordable and effective way of delivering winning performance – especially for those that are software-intensive. This is an increasingly dominant aspect of DOD's inventory of weapon and combat-supporting systems. Seemingly simple changes to a system already in the field may alter operational effectiveness, suitability, survivability, and lethality. These changes may also impact how it and other systems interoperate and function within the kill web. We must therefore "look right" into the life cycle of a system as we work on new ways to pioneer T&E of systems built to change over time. To assure continued combat credibility, we will work with the T&E community to determine how and when to test systems that have evolved substantially after fielding. This is especially important for the operational and responsible performance of systems that incorporate artificial intelligence, autonomy, and machine learning.

One important step is to develop a framework to evaluate iterative software improvements and their impact to a system's role in and interoperability with the kill web. At the same time, the T&E community must broaden its development and use of new testing methods, such as digital twins. This and other best practices will help us keep pace with the rapid and frequent changes we both encourage and expect, such that we can test them safely with minimal disruption to warfighting units. With the user and acquisition communities, we will have to work together to set parameters for continuous monitoring of the operational performance of interoperable sets of fielded systems. Digital twins will aid, but not obviate, the need for live operational and live fire T&E events. In particular, any model we utilize needs to be validated, verified, and accredited (VV&A) for its intended use to reflect, as accurately as possible, the real world. When the results of testing via a digital twin diverge substantially from what we observe in the field, careful examination of the VV&A of those models will be necessary and likely require a live operational or live fire T&E event to reconnect us to an accurate reflection of the operating environment.

Foster an Agile and Enduring T&E Enterprise Workforce. Evolving the craft of operational test and evaluation to the vision articulated above is contingent upon having a creative, highly skilled, and deeply knowledgeable workforce. As the NDS attests, people are DOD's "most valuable resource" and "to recruit and retain the most talented Americans, we must change our institutional culture and reform how we do business." The final pillar of DOT&E's strategy therefore focuses on fostering an agile and enduring T&E enterprise workforce. Looking at today's environment and into the near future, our most significant human resource gaps lie in the use of automation, cyber survivability, data management, artificial intelligence, and digital engineering. There are at least three moving parts we need to keep in mind: the tools used to create new capabilities are changing rapidly; we are using those rapidly changing tools to quickly improve and deliver new capabilities for our weapon systems; and the underlying T&E technologies and practices we must employ to practice our craft are also constantly in motion. To remain effective in this environment, our personnel must broaden their knowledge and take advantage of training opportunities. DOT&E will apply available training and development resources to improve our diverse workforce. In addition, we will pursue NDS suggestions for bringing in new perspectives through fellowships, internships, and rotational assignments, including with the private sector. Creating a wide array of collaboration opportunities and expanding our range of experience will help to bring the best practices into our community.

BRINGING THE 2022 DOT&E STRATEGY UPDATE TO FRUITION

DOT&E is working to bring the 2022 Strategy Update to fruition. A prescient reorganization that occurred before I joined the team established a new deputate focused on strategic initiatives, policy, and emerging technologies (SIPET). Accompanied by the incorporation of live fire T&E into our warfighting domain deputates, DOT&E now has the right structure to achieve the NDS's call to "modernize the systems that design and build the Joint Force, with a focus on innovation and rapid adjustment to new strategic demands." The SIPET deputate, in close collaboration with the T&E community, is leading development of the 2022 DOT&E Strategy Update Implementation Plan, which we expect to publish in FY23.

To do a better job of testing as we fight, DOD will need to improve our capacity to test in a realistic, joint, multi-domain environment – to include with international partners where possible. This will entail a geographically dispersed yet integrated, cross-service, live-virtual-constructive T&E infrastructure that can scale and adapt as technologies and concepts of operations change. Devising and implementing an architecture for collaborative and synergistic testing across these facilities will require some investment.

Test realism also depends on threat accuracy which is an area that constantly needs improvement. The adversary cycle of capability change is shorter than ever, yet representation within the test environment often takes three to five years. We will need to continue to innovate on the use of simulation and/or emulation of threats in representative environments to ensure that weapon systems will be effective when called upon.

Cooperation across multiple disciplines and communities is required to remedy this threat realism gap. To ensure we can adequately test throughout a system's entire life cycle, the acquisition and sustainment communities will need to work with the intelligence community to understand the collected threat data and to identify missing pieces of the threat/capability overmatch puzzle. A threat reference framework along with threat-agnostic models would facilitate threat simulation and emulation. DOT&E will be exploring the application of artificial intelligence to create threat models over shorter timelines.

Testing of mission systems must also move away from the classic "System Under Test" construct. Warfighting is executed jointly and across multiple domains. Capability is now generated through interoperability of systems of systems, to include platforms in different domains – not individual systems operating in disconnected silos. DOT&E will be looking for ways to routinely assess interoperability as it is affected by the introduction of a new capability, or modification to an existing capability, on those kill webs.

These reforms and advances will require collaboration with other T&E stakeholders, the acquisition, intelligence, and sustainment communities, and the Congress. The amount of change necessary for OT&E to remain credible and trusted cannot happen tomorrow. But we need a concerted effort now – heavy investment in individual brainstorming; collaborative brainstorming among government entities, the private sector, and academia; and smartly timed planning and programming in the amounts required.

COVID-19

At no point since March 2020, when the full impact of the COVID-19 pandemic hit, have the dedicated women and men of DOT&E allowed our mission to falter – accepting risk to themselves to ensure support to our warfighters. For that, the Department and the Nation owe them a debt of gratitude. After another year of medical advances, the fight against COVID-19 has progressed dramatically. Though it has not been eradicated, and the possibility of infection remains, vaccines have allowed most people to resume daily life with prudence.

As a science-based organization that seeks and follows data, DOT&E used what we learned from this experience to refashion our workforce approach. We continue to pursue new ways of connecting our analysts with T&E and warfighting environments in order to provide them the maximum ability and flexibility to do their critical work. We also have revised our internal cadence, taking better advantage of the remote work tools available to DOD. Taking full advantage of these practices will aid in retention and improving our workforce's depth of experience, which is paramount to our success.

ONE ANNUAL REPORT

Many may remember that last year DOT&E issued two Annual Reports: one that contained controlled unclassified information, per statute, regulations, and program-specific classification guides; and the other one fully cleared for public release. Issuing two documents allowed DOT&E to be more transparent with congressional and DOD personnel, while maintaining the integrity of information related to programs under oversight. This year, in consultation with Congress, we produced a single, publicly releasable report. Doing so complies with both the spirit and letter of the legislation governing the Annual Report. This 2022 report reflects careful consultation with the program offices that determine the classification of information about systems under DOT&E oversight, and contains the maximum detail permitted. As always, the DOT&E team is ready and available, on request, to assist members of Congress and their staff in understanding the performance of systems in the DOD acquisition pipeline at higher levels of classification.

SUSTAINMENT OF INTEGRITY IN OPERATIONAL TEST OVERSIGHT

Prior to this report being finalized, on November 15, 2022, I was nominated by the President for the position of Assistant Secretary of the Navy (Research, Development, and Acquisition). While the confirmation process is under way, I directed the establishment of a File for the Record of all decisions related to Navy acquisition programs until my confirmation process runs its course as I continue to serve as the Director, Operational Test and Evaluation, the position for which I was appointed by the President and confirmed by the Senate.

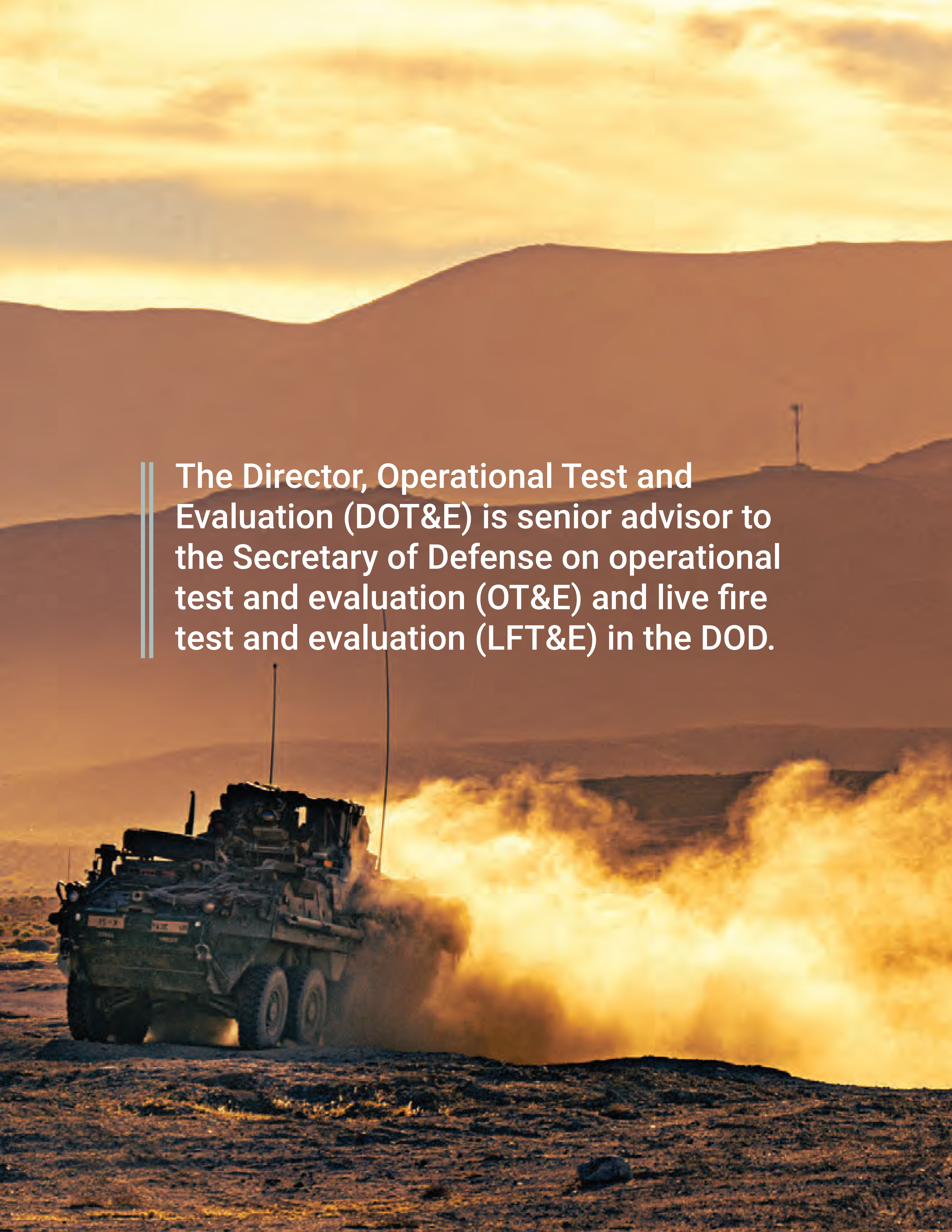
As Director, I continue to uphold the highest standards of ethical conduct and ensuring that the transparency and integrity of OT&E decisions are sustained in the Department's independent assessments. The responsibilities of my office, as the independent voice of the warfighter, to the Secretary and to the Congress continue to be held to the highest level of integrity.

Nickolas H Guertin

Nickolas H. Guertin
Director

CONTENTS

CONTENTS



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

DOT&E'S MISSION:

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

DOT&E responsibilities are detailed in the legislation codified in 1983 (Title 10, Sections 139, 4171, and 4231) and then in 1986 (Title 10, Section 4172).[1] These responsibilities were established to support the fielding of weapon systems that work in combat regardless of the competing acquisition priorities. DOT&E responsibilities have since been augmented through a range of subsequent National Defense Authorization Acts, DOD Directives, and DOD Instructions. DOD Directive 5141.02 assigns the following, critical DOD programs and activities to DOT&E:

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

1 As of January 1, 2022, there was a restructuring of Title 10, which renumbered many of the sections. Section 2399 was renumbered as 4171; 2400 as 4231; and 2366 as 4172. There were no substantive changes to DOT&E responsibilities.

EXECUTIVE SUMMARY

MAJOR PRODUCTS

In FY22, DOT&E provided operational and/or live fire test and evaluation oversight for 243 acquisition programs at various stages in their acquisition cycle.[1] Specifically, DOT&E reviewed and approved 27 Test and Evaluation strategies / Test and Evaluation Master Plans (TEMPs), 9 of which included a Live Fire Test and Evaluation (LFT&E) Strategy. DOT&E also approved 68 individual test plans and disapproved 3 test plans.

DOT&E evaluates the adequacy of the Service test strategies and plans based on the degree that they will provide: 1) data to support adequate evaluation of operational effectiveness and operational suitability; 2) coverage of the battlespace and threats; 3) credible use of modeling and simulation (M&S); 4) complete assessments of system survivability and lethality against mission-relevant threats (e.g., kinetic; cyber; electromagnetic; and Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE)); 5) production representative test articles; 6) operational realism; and 7) sufficient funding and resources required to support test execution.

In FY22, DOT&E published 48 reports, including 37 reports to Congress and the SECDEF, and a classified annual report on the Missile Defense System. In addition to the assessment of test adequacy, DOT&E reports summarize the Director's independent assessment of operational effectiveness, lethality (where relevant), suitability, and survivability of DOD weapon and business systems in realistic operational conditions. In instances where operational and/or live fire testing and evaluation have not yet been completed, DOT&E provides an interim assessment and identifies any risk to accomplishing the required operational performance in upcoming operational and/or live fire test, prior to fielding or the next acquisition decision review. DOT&E reports include practical recommendations to fix the identified deficiencies and improve the operational performance of the weapon or business system in expected operational scenarios and conditions to minimize risk to warfighters and maximize probability of mission success in conflict.

In FY22, DOT&E responded to several National Defense Authorization Act (NDAA) tasks and other Congressional taskers, the status of which is summarized in Table 1.

1 The number of programs on DOT&E oversight fluctuates throughout the year; 243 is the number of programs on DOT&E oversight as of September 30, 2022.

Table 1. Summary of DOT&E Congressional Activities

Source	Title	Status
FY20 NDAA		
Sec. 231	Digital Engineering Capability to Automate Testing and Evaluation	Ongoing; DOT&E in support of USD(R&E)
FY21 NDAA		
*Sec. 112	Report on limitations of Integrated Visual Augmentation System (IVAS)	Complete
Sec. 159	Documentation Related to F-35 Program	Ongoing
Sec. 162	Briefings on Software Regression Testing for F-35	Ongoing; USD(A&S) develop quarterly briefings in consultation with DOT&E
Sec. 222	Activities to Improve Fielding of Air Force Hypersonic Capabilities	Ongoing; USD(R&E) to deliver report in consultation with DOT&E
FY22 NDAA		
*Sec. 115	Limitation on Availability of funds pending report on the Integrated Visual Augmentation System	Complete
Sec. 223	Development and implementation of digital technologies for survivability and lethality testing	Ongoing; program selection complete
*Sec. 235	Limitation on transfer of certain operational flight test events and reductions in operational flight test capacity	Complete
*Sec. 1046	Comparative testing reports for certain aircraft	Complete
Sec. 1529	Demonstration program for automated security validation tools	Ongoing
Other FY22 Congressional Taskers		
*Appn ES pg. 5-6	Department of Defense Test Infrastructure Investments: Detailed Spend Plan	Complete
*Appn ES pg. 12	Certification of test strategies on Middle-Tier Acquisition and Rapid Prototyping programs	Complete
*Appn ES pg. 119-120	Self-defense test ship Congressional Response	Complete
*Appn ES pg. 138-139	Certification of funding for test infrastructure and test event resources	Complete
SASC Report pg. 191-192	Electronic Health Record interoperability between DOD and Veterans Affairs	Ongoing
HASC Report pg. 54	Commercial Virtualization Technology briefing	Complete
*HASC Report pg. 70	Digital twin assessment and agile verification processes report	Complete

Table 1. Summary of DOT&E Congressional Activities

Source	Title	Status
*HASC Report pg. 268	Software academic technical expertise implementation plan	Complete
Appn ES – Appropriations Act Explanatory Statement; HASC – House Armed Services Committee; NDAA – National Defense Authorization Act; SASC – Senate Armed Services Committee; USD(A&S) – Under Secretary of Defense for Acquisition and Sustainment; USD(R&E) – Under Secretary of Defense for Research and Engineering * These activities resulted in reports to Congress which are reflected in the Appendix.		

Lastly, DOT&E published the DOT&E Strategy Update 2022, outlining the intent to transform T&E and enable delivery of the world's most advanced warfighting capabilities at the speed of need. Driven by challenges caused largely by software-reliant systems, artificial intelligence (AI) and machine learning, Joint All-Domain Operations, data management, speed to field, culture, and talent management, this strategy seeks to advance the T&E infrastructure, processes, tools, and workforce needed to meet the T&E demands of the future. The Strategy intends to deliver on this intent by focusing on five pillars: 1) Test the way we fight; 2) Accelerate the delivery of weapons that work; 3) Improve the survivability of the DOD in contested environments, 4) Pioneer T&E of weapon systems built to change over time; and 5) Foster an agile and enduring T&E enterprise workforce. An accompanying Implementation Plan, treated as a living document that DOT&E will update annually in coordination with the T&E community, clarifies the desired end-state and specific actions and deliverables proposed to contribute to the accomplishment of the strategic intent.

MAJOR CONTRIBUTIONS

» ENSURING ADEQUATE TESTING IN COMBAT-REPRESENTATIVE CONDITIONS

In FY22, DOT&E continued to highlight and correct instances where proposed test plans were not adequate. Based on the test plans that DOT&E reviewed in FY22, common shortfalls were associated with deficiencies with M&S verification and validation (V&V), insufficient coverage of the operational environment and threats, including insufficient threat realism for cyber assessments, and inadequate data collection to support an evaluation of operational performance. DOT&E also noted a lack of production representative systems due to differences in software between the fielded system and the system under test. DOT&E worked with program stakeholders to improve the test adequacy of plans.

In FY22, at DOT&E's request, the National Academies of Sciences, Engineering, and Medicine completed their study on the health and readiness of the DOD test ranges and associated infrastructure for future operational and live fire testing. The National Academies' resulting classified Phase II report was published in August 2022, and expands upon previous findings summarized in the unclassified, Phase 1 report, published in September 2021. Specifically, it focuses on 1) improving threat modeling and prototyping to keep pace with the adversary; 2) addressing gaps in testing driven by new and emerging technologies; 3) testing as you fight with a focus on operational capability, not technical requirements; 4) formalizing a test range for multi-domain operational test at a system-of-systems level, based on live, virtual, and constructive technologies; and 5) testing at the speed of operational needs. DOT&E continues to evaluate the National Academies' recommendations and will include many of them, as appropriate, in the Implementation Plan for the DOT&E Strategy.

In parallel, through the DOT&E Resources and Infrastructure Working Group, and in coordination with the Test Resources Management Center in

USD(R&E), DOT&E received funding to upgrade T&E capabilities in support of next-generation weapons, including hypersonics, directed energy, and space technologies, and to improve realistic threats through verified and validated threat model surrogates. Additional details are available in the T&E Resources section of this report.

» ENSURING ADEQUATE TESTING ACROSS EVERY ACQUISITION PATHWAY

In FY22, DOT&E, in close coordination with the Director of Developmental Test, Evaluation and Assessments within USD(R&E), published a T&E Enterprise Guidebook to replace the current Defense Acquisition Guidebook, Chapter 8 and provide the DOD's acquisition and T&E communities with detailed guidance on adequate developmental, operational, and live fire T&E for each of the acquisition pathways. Across all acquisition pathways, the T&E Enterprise Guidebook emphasizes 1) the need for early and active engagement in acquisition programs to inform requirement development and acquisition contracts; 2) the use of any and all test events and data collection opportunities to support assessment of technical and operational performance; 3) the establishment of data storage and management processes to build accessible data repositories to support timely evaluations; and 4) the use of digital engineering and automation tools, supported by rigorous V&V processes, whenever possible for T&E planning, analysis, and reporting.

In FY22, DOT&E evaluated the DOD and Service test resources and funding profiles needed to support agreed-upon TEMPs for Major Defense Acquisition Programs and T&E strategies for prototyping programs.

Fifty-one of 101 programs (51 percent) were found to have adequate funding to support the remainder of the planned test execution. One program, the CH-53K King Stallion, was identified as having funding shortfalls related to survivability testing planned in the live fire plan. DOT&E also identified 34 of 101 programs (34 percent) that required updated TEMPs or T&E strategies due to program changes and thus, may have new or altered testing or resource requirements. Fifteen of 101 programs (15 percent) have fully executed all required testing; no current or Future Years Defense Program funding is required or allocated.

DOT&E also assessed the appropriateness of the test strategies for 105 programs approved by the Service Acquisition Executives to pursue accelerated acquisition authorities. DOT&E received and reviewed 53 test strategies and determined 41 of those to be appropriate. DOT&E's assessment was based on the test strategy supporting demonstration of the maturity and feasibility of the system to achieve the required capability, mission-relevant system capabilities and limitations with planned operational units, operators, missions, and environments, and system survivability against mission-relevant threats. DOT&E also assessed whether the test strategy identified the funding required to support the test execution.

» TRANSFORMING T&E

As the warfighting capability continues to evolve to support the DOD's ability to fight and dominate in a multi-domain operational environment, the T&E community will require innovative, enterprise-level approaches to enable realistic testing. Improvements in infrastructure, tools, processes and the T&E workforce are needed to ensure adequate characterization of joint warfighting concepts and support delivery of the most advanced technical capabilities at the speed of need. The initiatives required to accomplish this are summarized in five major pillars of the DOT&E Strategy Update 2022.

1. Test the way we fight

Accurate evaluation of warfighting capabilities requires an adequate, scalable, and adaptive representation of the multi-domain operational environment as well as the ability to measure the operational performance of the future Joint Force capabilities in such an environment. DOT&E seeks to enable the identification, prioritization, and tracking of key range capability and funding requirements as driven by emerging technologies and threats.

DOT&E also seeks to define the OT&E and LFT&E requirements needed to support an operational evaluation of DOD scenarios, vignettes, and mission threads, including kill webs, in addition to evaluation of individual acquisition systems within those mission threads. In FY22, DOT&E highlighted key OT&E and LFT&E gaps in test range capabilities, instrumentation, and threat representation. In addition, given the growing importance of M&S and other virtual representations, DOT&E considered the challenges preventing rigorous V&V of M&S used to supplement findings from live test events. To improve M&S V&V adequacy, DOT&E, in conjunction with USD(R&E), is developing new M&S V&V policy to enable increased use of M&S in operational evaluation. However, availability of test data needed to enable credible V&V of key M&S tools remains a challenge.

2. Accelerate the delivery of weapons that work

As the complexity of systems grow, so often does the amount of data needed to support an adequate evaluation of their operational performance. For the T&E community to optimize the use of large volume of data, it must accelerate the implementation of the DOD Data Management Strategy and the five data decrees. To increase T&E and acquisition efficiencies, including automated, near real-time, enterprise-level data management and analysis to drive new insights, T&E data must be contained in data repositories that are discoverable, accessible, and secure. Internally, in FY22, DOT&E continued working a proof of concept to improve T&E data management with goals of improved searchability and the ability to document trends in findings across reports.

DOT&E is also exploring ways to better implement digital data practices across the DOD as a way to operationalize the "Shift Left" approach. By understanding a system's performance throughout the life cycle with increased access to data, the T&E community can use tools common in digital engineering and Bayesian inference processes to more efficiently integrate testing and analyze results. DOT&E hosted a workshop with the T&E community focused on exploring methods for taking advantage of digital engineering principles in the T&E planning process. DOT&E is using feedback from across the Services to understand where model-based TEMPs and T&E strategies may be most beneficial as a tool for efficiently documenting test planning and tracking execution.

DOT&E is working with USD(R&E) on updated policy for TEMPs and T&E strategies. The updated policy places a new emphasis on the Integrated Decision Support Key as a tool that finds opportunities for shifting left through integrated test designs (i.e., T&E events designed to meet developmental, live fire and operational test objectives) that provide useable data for multiple evaluations. This policy will provide a more structured and standardized approach for program stakeholders to align decision points with the operational and technical evaluations and events necessary to inform decisions. The Integrated Decision Support Key also lays the groundwork for further research into statistical application of sequential methods, development or relational databases, and similar tools that could be used to optimize the use of available data collected under different but relevant conditions.

3. Improve the survivability of the DOD in contested environments

To improve DOD survivability, DOT&E is committed to helping minimize the number of mission critical vulnerabilities in fielded systems through continuous mission-based risk assessments and rigorous evaluations, as both U.S. systems and the threats they face evolve. DOT&E continues to find that many programs are not survivable against operationally relevant threats. As systems become more interoperable, the attack surface increases exponentially, while also complicating the assessment of synergistic effects of multiple threats across a given mission thread. In FY22, DOT&E considered the survivability of systems against the full spectrum of potential threats. In our initial response to FY22 NDAA Section 223, we chose four programs to serve as pilots for full spectrum survivability testing approaches: 1) the Army's Future Long Range Assault Aircraft, 2) the Air Force's LGM-35A Sentinel (Ground Based Strategic Deterrent), 3) the Navy's DDG 51

Flight III, and 4) the Joint F-35 program. Each of the programs uses some form of digital technologies, in addition to live testing, for their evaluations. DOT&E will continue exploring the overall utility of live, virtual, and constructive methods in standardizing the assessment of mission-based survivability in FY23 as part of a more detailed response to the Section 223 task.

DOT&E continues to emphasize cyber and electromagnetic spectrum survivability as attack surfaces multiply. DOT&E also sees space as an increasingly congested and contested environment. In FY22, DOT&E, in conjunction with USD(R&E), drafted an update to cyber T&E and electromagnetic spectrum operations T&E policies. The T&E community must consider supply chains, software factories and pipelines, and an array of cloud solutions in survivability assessments. DOT&E observed in FY22 that test teams across the Army, Navy, and Air Force demonstrated the capability to test non-IP systems during operational test. Other new tools and processes may be necessary to effectively assess countermeasures and other self-defense solutions.

4. Pioneer T&E of weapon systems built to change over time

AI-based systems require the T&E community to continuously monitor and evaluate the system' behavior, including in theater post-fielding, to ensure their ethical, effective, and safe use as they're exposed to new operating environments that they may have not been trained and tested on. Similarly, with the increased prevalence of software-reliant programs planning to deliver capabilities more frequently, DOT&E has considered how some T&E practices may need to evolve to enable continuous monitoring and evaluation of their operational performance. DOT&E is committed to enabling operationally relevant and timely evaluations for these rapidly changing systems to ensure they continue to be effective, lethal, suitable, and survivable as both they and the threat change. In particular, DOT&E plans to issue policy on T&E of software and AI-enabled systems. The policy places emphasis on early involvement in requirements development and program planning. It encourages early integration of end users to understand the complex dynamic of how warfighters use systems to accomplish their missions and how those might supplement automated test results.

The use of digital twins and commercial virtualization technology may be a means to enable continuous evaluation of operational performance. Such technologies may optimize the use of model-based system engineering supporting early, continuous, and automated T&E across the life-cycle of the system. In FY22, DOT&E responded to the House Armed Services Committee (HASC) task on digital twin practices and commercial virtualization technology, assessing that that a consensus on what constitutes a digital twin for the purposes of OT&E and LFT&E has not yet been reached. DOT&E also assessed that only a small fraction (about 7 percent) of the acquisition programs currently on DOT&E oversight have developed or are developing some version of a digital twin. While use of digital twins for OT&E and LFT&E is not yet common practice, DOT&E is researching the work on the verification, validation, and accreditation of these along with the benefits and challenges of these approaches.

5. Foster an agile and enduring T&E workforce

DOT&E requires a trained and equipped workforce, prepared to meet the toughest T&E challenges, with access to continuous learning opportunities. In June 2022, DOT&E completed a workforce assessment to identify existing strengths and weaknesses and clarify follow-on actions needed to ensure that DOT&E is optimally structured, organized, and postured to meet the demands of the future. As a result, DOT&E developed core DOT&E workforce competencies that will be used to develop and implement a continuous learning curriculum and future operating model to support DOT&E's future mission execution and keep pace with the evolving T&E environment. Time to train, speed to hire, and easy access to in-demand expertise remain a challenge.

In addition to the workforce assessment, DOT&E partnered with Cyber Test Teams across the Services to complete the Software and Cyber Network of Excellence for Testing (SCyNET) pathfinding activities.

In July 2022, DOT&E responded to the HASC task by providing an implementation plan for a Cyber and Software Test and Evaluation Center of Excellence. The plan provides a strategy for a scalable, one-stop-shop for cutting edge research and development, thought leadership, and collaboration across the T&E enterprise with three major objectives: 1) nurture a culture of information exchange across the T&E enterprise; 2) drive continuous innovation across cyber and software T&E; and 3) build a pipeline for talent acquisition, training, and retention through multiple key actions.

DOT&E also responded to an NDAA Section 235 tasker to evaluate the effect of the Navy's proposed manpower reductions on naval aviation OT. DOT&E found that OT squadrons (VX-1 and VX-9) have adequate physical and organizational infrastructure but, if the proposed manpower reductions get implemented, the squadrons' capacity utilization will exceed 100% precluding either squadron to complete the planned and required operational testing. DOT&E recommended against delegating OT to non-OT units citing several reasons that could cause a negative effect on the cost, schedule, and capacity of Naval Aviation OT. Instead, DOT&E recommended that the VX-1 OT squadron maintain its FY22 manning and that VX-9 OT squadron add 106 maintainers to its FY22 manning.

» DEMONSTRATING THE VALUE OF T&E

T&E is essential to demonstrate weapon system performance and provide DOD mission planners, commanders, and operators and maintainers with an understanding of true system capabilities to adequately plan and execute their missions. Examples of this can be found in the Joint Technical Coordinating Group for Munition Effectiveness, Joint Test and Evaluation, and Cyber Assessment Program sections of this report. Specifically, DOT&E cyber-related activities have helped the DOD characterize cyber effects on mission performance, identify network and system vulnerabilities, assess operational concepts and procedures, enhance cyber team capabilities, update guidance and methodologies, facilitate operational assessment of offensive cyber capabilities, and inform the Department on cyber considerations of initiatives and technologies such as the move to commercial cloud-based computing. DOT&E cybersecurity assessments have uncovered important vulnerabilities that, if corrected, will improve the Department's resilience against cyber-attacks. T&E, in general, identifies warfighting performance shortfalls that could and should be addressed prior to weapon system fielding or the next acquisition decision. This identification permits corrective action to be taken before large quantities of a system are procured and avoids expensive retrofit of system modifications. Examples of common problems discovered in OT&E include poor system performance, poor interoperability with Joint Partners, poor human systems integration, insufficient training, and various hardware failures. The performance trends section below provides additional detail on the value of T&E.

MAJOR FINDINGS

Figures 1 through 4 summarize the trends in DOT&E assessments of test adequacy, operational effectiveness, operational suitability, and survivability since FY16. While DOT&E published 48 reports in FY22, 28 reports focused on acquisition programs. Of those 28 reports, not all included an assessment of final determination of operational performance due to either maturity of the program, test limitations, or multi-level classifications. More specifically, all 28 reports included an assessment of test adequacy,15 included an assessment of operational effectiveness, and 13 included an assessment of operational suitability and survivability. As discussed below, operational testing continues to reveal challenges with effectiveness, suitability, and survivability that would not be observed by developmental testing alone.

» TEST ADEQUACY TRENDS

In FY22, DOT&E reported that 75 percent (21of 28) of programs conducted adequate operational and/or live fire testing, as detailed in Figure 1. This was similar to prior years where the fraction of programs conducting adequate testing ranged from 57 to 74 percent. The majority of programs (6 of 7) assessed as not adequate or partially adequate were early fielding reports for programs that did not complete operational testing prior to fielding. DOT&E assessed one program as partially adequate because the test did not include all relevant threats and operational environments.

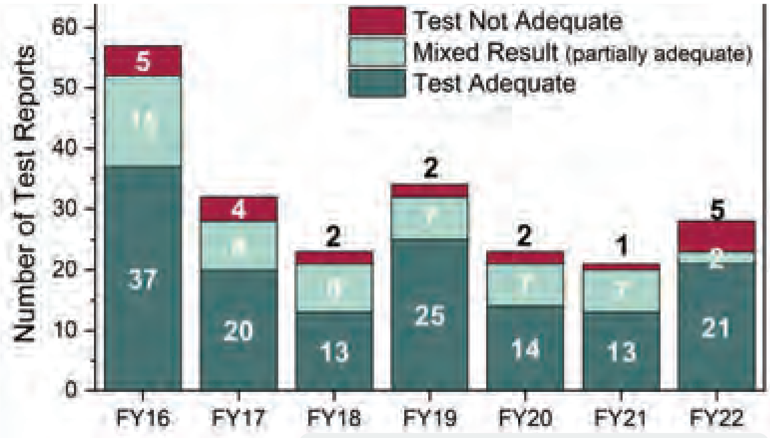


Figure 1. Test Adequacy Trends

Of the 28 reports, 27 noted at least one test limitation. Cyber survivability was the most common category of test limitation. Common cyber test limitations included testing that did not cover all cyber threat postures or attack vectors, such as supply chain compromise or outsider postures; failure to collect all data due to insufficient time or resources; lack of production-representative assets during early tests; and deferral of operational cyber testing to a later date. Other common test limitations included insufficient coverage of the threat environment or operational profiles, M&S deficiencies resulting from simplifying assumptions, inability to collect all required data due to test instrumentation limitations, and test range restrictions that prevented full employment of the system or threats.

» PERFORMANCE TRENDS

Effectiveness

In FY22, DOT&E evaluated 73 percent (11 of 15) of programs to be operationally effective. Since FY16, the fraction of programs assessed as operationally effective has ranged from 43 to 73 percent. DOT&E assessed four FY22 programs as not effective or having mixed effectiveness because of shortcomings when operating in particular environments, mission areas, or against specific threats. For example, one system was assessed as not effective because of performance deficiencies when employing the system at night. In another case, operational testing revealed that the units did not use the system as envisioned during developmental testing. Specifically, when used as a mobile command post, the system did not have enough secure beyond line of sight communication networks to support communication demands.

All 15 reports with an operational effectiveness assessment documented at least one problem with operational effectiveness. In several cases, operational testing of the full system of systems revealed important interoperability or integration deficiencies, such as a communication system that exceeded the bandwidth requirements of the tactical network it was operating on or a tracked vehicle that was not able to share target information with infantry target designators. Another common problem was human factors limitations that affected operator performance or unit effectiveness. In one example, the unit was not able to use the system effectively because of its complexity and the lack of user training prior to the test.

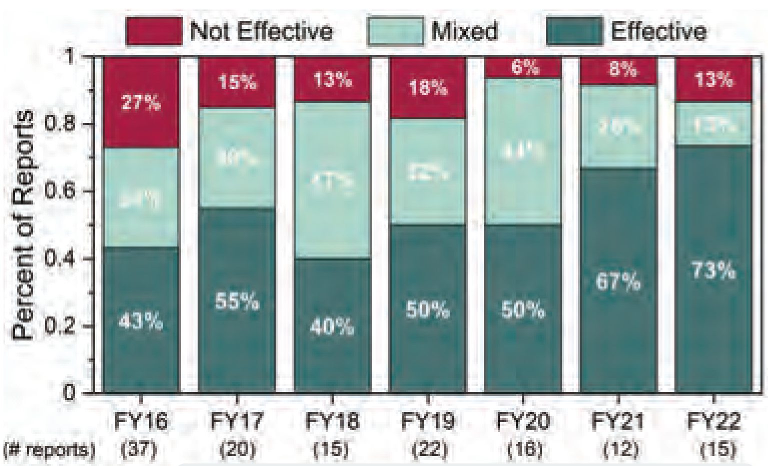


Figure 2. Operational Effectiveness Trends

Suitability

In FY22, DOT&E evaluated 38 percent (5 of 13) of the programs to be operationally suitable without any caveats. All six programs assessed as not suitable in FY22 had poor reliability resulting from a mix of software and hardware failures. In three instances, availability and maintainability shortfalls also played a role. Of the 13 programs with a suitability assessment, 10 programs had Human System Integration (HSI) challenges. Similar to FY21, lack of adequate training or training resources continues to be the primary HSI deficiency.

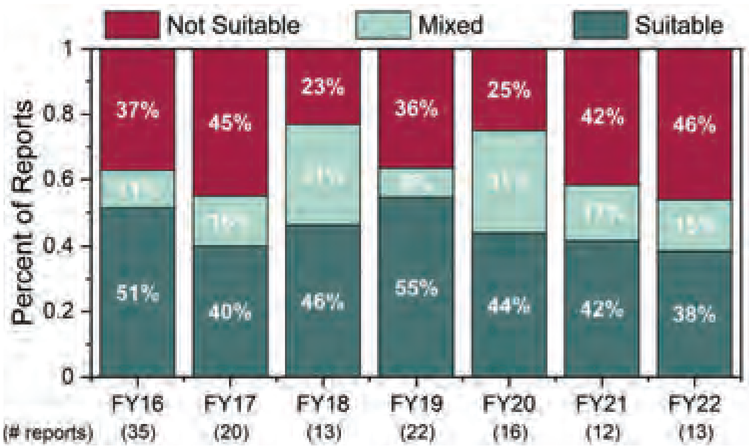


Figure 3. Operational Suitability Trends

Survivability

DOT&E evaluated 23 percent (3 of 13) of the programs to be survivable without any caveats in FY22. Similar to FY21, survivability against cyber threats was the most common problem followed by survivability against kinetic threats.

Common cyber survivability issues included unencrypted software, hardware, or network traffic; lack of safeguards to limit access to serial, USB, or Ethernet ports; and use of a 1553 data bus without encryption or authentication. In most cases, operators were the primary cyber defenders of the system and the system lacked the capability to detect, monitor, or notify the operator of a potential cyber attacks. Eight systems had vulnerabilities to specific kinetic threats unique to the system designs.

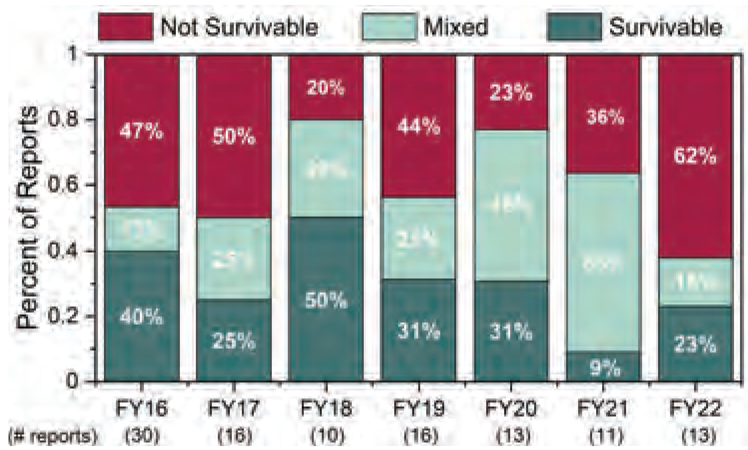


Figure 4. SurvivabilityTrends

RECOMMENDATIONS

The following recommendations are expected to better posture a program for success during operational and live fire testing:

- Integrate test planning and execution across the T&E community to increase efficiency and discover problems early by requiring demonstration of operationally relevant, mission-level goals during early testing, instead of focusing solely on specification compliance.
- Conduct operational testing that supports an assessment of the full system of systems across the relevant set of missions and operating conditions.
- Follow best practices early in the acquisition phases of a program to avoid common cyber vulnerabilities and build systems that are capable of detecting, monitoring, and notifying operators of cyber attacks.
- Establish a reliability growth process that is supported by system engineering efforts and contractual requirements.
- Refine and validate training manuals and other training resources prior to operational testing and allocate more time for operator and collective unit training.
- Develop robust and independent V&V for all M&S to be used in T&E.

TEST AND EVALUATION RESOURCES

Test and Evaluation Resources

T&E infrastructure must enable credible and comprehensive evaluation of the operational performance of DOD warfighting capabilities. To stay ahead of the adversary and keep pace with emerging and advanced technologies, the DOD must continue to advance the T&E infrastructure to accurately represent the complex and dynamic multi-domain operational environment in test and be prepared to evaluate future joint force capabilities. The DOD must also continue to recruit, train, and retain personnel with the unique skillsets needed to meet the T&E demands of the future.

As per the FY22 Consolidated Appropriations Act, Congress provided the T&E enterprise with $798,128,000 in additional appropriations:

- $422,728,000 to USD(R&E), the Space Force, the Navy, and DOT&E to upgrade lab and test range infrastructure in the areas of hypersonics, directed energy, space, targets and threats, and electromagnetic spectrum.
- $375,400,000 to USD(R&E), the Navy, and the Air Force to be put towards peer-representative threat environments for fifth-generation aircraft.

This section summarizes how these additional resources will help close some of the identified gaps in the specified areas. This section also summarizes known initiatives and the remaining T&E infrastructure and workforce shortfalls in the following areas:

- Hypersonics,
- Directed energy weapons,
- Cyber survivability,
- Chemical and biological defense,
- Nuclear modernization,
- Electromagnetic spectrum operations,
- Space,
- Autonomous and artificial intelligence (AI)-enabled systems,
- Multi-domain operations,
- Common range infrastructure,
- Threat and target surrogates,
- Knowledge management and big data analytics, and
- Range sustainability.

This section also summarizes the reports provided to DOT&E by the Service T&E Executives and Operational Test Agency (OTA) Commanders on the adequacy of their resources and the infrastructure required to accomplish the planned T&E across the Future Year Defense Program (FYDP). DOT&E did not have the detailed information to validate those reports but intends to initiate an FY23 action to support such validations in the future.

Lastly, this section summarizes other areas where the DOD needs to focus.

HYPERSONIC MISSILES AND HYPERSONIC MISSILE DEFENSE

Hypersonic missiles have unique flight characteristics designed to achieve speeds between Mach 5 and 20, ranges that can exceed 1,000 miles, and perform extensive maneuvers. These characteristics are partially distinguished from those of long-range ballistic missile weapons because hypersonic missiles fly in the Earth's atmosphere. Adequate


Figure 1: Hypersonic Sled

evaluation of the operational performance of such unique characteristics of hypersonic flight will require new or upgraded T&E range infrastructure and instrumentation.

Specifically, ground test capabilities are needed to recreate hypersonic flight. Ongoing investments are intended to:

- Improve pre-flight assessments of vehicle structural design and responses in flight (i.e., improvements to the Arnold Engineering Development Complex G-Range, Holloman High Speed Sled Track, and National Aeronautics and Space Administration Particle Impact Facility).
- Increase capacity and expand the capabilities of U.S. arcjet facilities that simulate the conditions of flight at given altitudes and velocities. All hypersonic missiles, hypersonic defense interceptors and advanced targets, and high altitude ballistic and maneuvering munitions require the use of arcjet facilities to test the thermal protection systems and vehicle aeroshells.
- Close critical T&E gaps in aerothermal structural and advanced propulsion ground testing of scramjet vehicles by providing a largescale, clean-air, variable-Mach test facility with long runtime. Most recently, the Naval Surface Warfare Center, Crane Division was awarded a contract to develop a hypersonics test bed, which will allow hypersonic technologies to mature in simulated flight and validate their performance prior to incorporation into existing weapon systems.

Additional missile test range modernization efforts are needed to support an increase in the tempo of testing and the development of new capabilities to measure hypersonic missile flight performance in increasingly complex threat environments. For example:

- Mobile instrumentation is needed to track and image atmospheric disturbances around the flight vehicle using radar and optical sensors in the visible and infrared regions of the spectrum.
- Mobile off-board sensors and additional telemetry are needed at the impact site for end-game scoring.
- The Test Resource Management Center (TRMC) is researching overland corridors that would impact at White Sands Missile Range (WSMR), referred to as the Mountain Desert Corridor (MDC). The associated Programmatic Environmental Impact Statement is expected to be complete before the end of calendar year 2022. While being pursued for long-range precision fires, the MDC may also provide an additional land-based impact site for limited hypersonic missile flight tests.
- TRMC intends to fund substantial unmanned aerial system-based range instrumentation for telemetry tracking and multispectral imaging. In FY22, two telemetry-configured Range Hawks were deployed to Marine Corps Air Station Kaneohe Bay, Hawaii to support a June 2022 flight

test. Additional data are needed to support the Missile Defense Agency (MDA) requirements.

- Flight corridors should include capacity for collection of debris dispersal, post-intercept, while also accounting for safety concerns caused by such debris.
- Development of credible models for flight and ground test venues needs to be accelerated.

OT&E of hypersonic missile defense systems continues to require threat hypersonic missile surrogates to evaluate the effectiveness of U.S. defensive capabilities against incoming hypersonic missiles. These surrogates need to be designed and built concurrently with both offensive hypersonic missiles and hypersonic defense interceptors. Multiple data collection assets are also required to capture both the dynamics of the hypersonic surrogate target as "truth" data for the test, and performance data from the hypersonic defense interceptors.

As per the FY22 Consolidated Appropriations Act, Congress provided $47.5 million to USD(R&E) and DOT&E to improve the hypersonic test infrastructure. DOT&E is focusing its investments ($7 million) on development of credible modeling and simulation (M&S) needed to support the operational effectiveness and lethality evaluations of hypersonic weapons. USD(R&E) will use its investments ($40.5 million) for: 1) the development of satellite communication relays for mobile broad ocean area scoring systems, 2) the upgrade of data collection capabilities at hypersonic flight test ranges, and 3) the development of a roll-on/roll-off range capability to support increased hypersonic flight test capacity, including telemetry, satellite communication relay, and optics capabilities.

DIRECTED ENERGY WEAPONS

Directed energy weapons are intended to disable large numbers of adversary targets at fast rates using concentrated energy in the form of high-energy lasers (HEL) or high-power microwaves (HPM).

Adequate operational testing and evaluation of HEL systems requires range instrumentation capable of characterizing laser beams as they propagate through the atmosphere and measuring their beam spot profiles on representative targets. The Mobile High Energy Laser Measurement (MHELM) project is a Joint Improvement Modernization (JIM) project supported by USD(R&E) and DOT&E. It provides advanced instrumentation needed by DOD test centers, including the High Energy Laser Systems Test Facility (HELSTF) and the Naval Air Warfare Center-Weapons Division (NAWCWD) to test and evaluate DOD HEL systems. The last MHELM project will achieve initial operational capability in FY23. The systems are being transitioned to the range partners as they are completed.

USD(R&E) manages the Directed Energy T&E Investment Roadmap for HEL. The roadmap outlines the execution of 51 HEL projects to reduce shortfalls in T&E infrastructure and instrumentation through FY30. These projects are intended to deliver representative threat lasers; infrastructure to conduct open-air tests (including range safety and predictive avoidance of satellites in orbit); ground test instrumentation for laser beam diagnostics and assessments of destructive power on real world targets; and M&S for improved prediction of atmospheric propagation characteristics. Threat representative targets (including adversarial countermeasures) are also needed to evaluate operational performance and lethality of HEL. Conversely, threat-representative HEL surrogates are needed to assess survivability of U.S. systems and performance of our countermeasures.

Adequate operational testing and evaluation of HPM systems requires range instrumentation capable of characterizing HPM envelopes and their effect on targets. USD(R&E) manages the Directed Energy T&E Investment Roadmap for HPM. The roadmap outlines 40 projects required to reduce shortfalls in HPM T&E infrastructure and instrumentation, some of which are still unfunded. Representative targets are needed for lethality assessments and accurate threat surrogates are needed to test performance and survivability. Range safety equipment is needed to protect range personnel and range equipment and to ensure stray energy does not disrupt non-range-related persons and property. M&S are needed for U.S. and adversarial weapons and for targets to execute adequate end-to-end T&E.

As per the FY22 Consolidated Appropriations Act, Congress provided $34 million to USD(R&E) and DOT&E to improve the T&E capabilities for evaluating directed energy weapons. DOT&E is focusing its investments ($12 million) on delivering ground- and air-based instrumentation and targets to support detection/tracking and lethality assessments of HELs and HPM weapons against a wide array of adversary targets. USD(R&E) will use the investments to upgrade the mobile diagnostics suite for higher fidelity characterization of HEL beam and enhance target boards to improve characterization of performance.

CYBER SURVIVABILITY

All DOD warfighting capabilities heavily rely on cyber components to fulfill their missions and must be sufficiently cyber survivable to execute assigned missions in contested cyberspace. These include, but are not limited to, communication and networking technologies, software and hardware layers, and data transfer among subsystems. All of these systems are subject to cyberattacks by threat actors. The complexity and interdependence of these systems and the rapidly evolving nature of cyber threats necessitates that T&E capabilities evolve in lockstep to enable realistic cyber T&E at scale to assess system survivability.

Needed DOD investments in hardware and software to enable adequate cyber T&E include tools and techniques to: 1) conduct attacks against Internet Protocol (IP) and non-IP systems, 2) identify unauthorized users and spoofing attempts, 3) assess radio frequency datalinks, and 4) create an adequate radio frequency test environment to support the convergence of cyber and electromagnetic spectrum operations.

The National Cyber Range Complex continues to enhance its capacities to perform more realistic system-of-systems cybersecurity test and training events through upgrades to the Joint Mission Environment Test Capability. Additional tools and techniques are required to:

Figure 2: Red Team at Cybersecurity Event

- Increase test efficiencies through rapid, accurate characterization and visualization (i.e., digital modeling) of the system or network and associated cyber vulnerabilities.
- Enable automated detection of cyber vulnerabilities in complex, interdependent systems and systems of systems, comprising various software and hardware layers.
- Manage the increasing scope of cyber assessments that 1) represent the system's functions, activities, and processes, and 2) determine mission impact from the cascading effects of cyber compromise.
- Emulate observable mission effects for systems under cyberattack.
- Enable automated adversary threat planning and emulation of routine threat capabilities.
- Provide data storage infrastructure and standards for secure handling and processing of T&E data.
- Decrease post-assessment time through integrated and standardized visualization, analysis, and reporting.
- Improve cyber countermeasure T&E frameworks, processes, and capabilities.

The scheduling and availability of operationally deployed weapon systems continues to limit the scope and breadth of cybersecurity assessments. Limited NSA-certified cyber Red Team and Blue Team availability constrains the depth of the assessments and limits operational realism.

CHEMICAL AND BIOLOGICAL DEFENSE

Advancements in the T&E infrastructure are required to adequately evaluate chemical/biological threat detection systems and the survivability of DOD weapon systems against chemical and biological agents. Specifically, software-in-the-loop testing is needed to leverage previously collected agent signature data to reduce the time and cost associated with system algorithm development and testing. M&S tools need to be adequately verified and validated to reduce the time and expense associated with repeating agent chamber testing.

In FY22, the Chemical and Biological Center's BioTesting Division awarded a contract for upgrading the Aerosol Simulant Exposure Chamber (ASEC), a bio-safety level two (BSL-2) facility. The upgrades will more accurately reproduce a wider range of threat conditions.

The West Desert Test Center at Dugway Proving Ground, Utah is experiencing a high turnover in personnel as well as difficulty in recruiting and retaining qualified personnel. The Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense is working with the Army and DOD to establish a mechanism for continuing to fund the sustainment of existing T&E infrastructure and future investments required to adequately test and evaluate new chemical and biological defense systems at Dugway Proving Ground.

NUCLEAR MODERNIZATION

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

Currently, the System Radiation Hardening of Electronic Components Forum; the Nuclear Modernization T&E Working Group; and the Chemical, Biological, Radiological, Nuclear (CBRN) Survivability Oversight Group – Nuclear (CSOG-N) T&E Subgroup have contributed to the strategic roadmap for Nuclear Modernization T&E shortfalls. While significant improvements have been accomplished in FY22, the DOD still lacks the capability to test and analyze stress, strain, rotation, translation, and failure modes on nuclear components and systems following extreme environment tests. Joint interface testing, electronics testing, performance assessment, and fault analysis when integrating system- and box-level nuclear test units are also needed.

ELECTROMAGNETIC SPECTRUM OPERATIONS


Figure 3: EMSO Discussion

The Electromagnetic Spectrum Operations (EMSO) environment is increasingly congested and contested by military and civilian systems and constrained by national and international regulatory changes. EMSO comprises the coordinated military actions to exploit, attack, protect, and manage the electromagnetic spectrum environment. Electromagnetic warfare is a vital element of EMSO and includes electromagnetic attack, electromagnetic protection, and electromagnetic support. One area of active research and development to improve system operations in this complex environment is focused on cognitive EMSO systems (incorporating AI technologies to varying degrees). Cognitive EMSO systems create complex and autonomous behaviors that will adapt to changing environments as the system learns. These unique system attributes introduce new T&E infrastructure challenges.

In FY22, the DOD invested extensively in improving the threat densities and realism for the EMSO for Live, Virtual, and Constructive (LVC) environments. Joint Electronic Warfare Test and Evaluation Strategy (JETS) Increment I is a significant capability that will replicate a dense integrated air defense system (IADS) environment and is an early implementation of a multi-range LVC environment. However, airborne threat software-defined radars (SDRs) remain a shortfall. Adversaries are developing multi-static radars that utilize the transmissions from commercial transmitters, which will further complicate EMSO. Developing simulators to mimic these emissions is critical to OT&E of future joint warfighting capabilities. Additional details can be found in the Threat and Target Systems subsection below. The Army has also reported a need for electronic intelligence simulators that are required to test emerging Army sensors and offensive devices for weapon systems intended to identify and affect near-peer threats. In addition, shortfalls exist in the capacity and certifications to conduct frequent and simultaneous GPS jamming and spoofing across multiple test ranges.

As per the FY22 Consolidated Appropriations Act, Congress provided $375,400,000 to USD(R&E), the Navy, and the Air Force to develop peer-representative threat environments for fifth-generation aircraft. USD(R&E) is focusing its investments ($263 million) on developing new radars and decoy systems. The Navy and Air Force are focusing their investments ($37.1 million and $75.3 million, respectively) on upgrades to their radars.

SPACE

Critical DOD space assets are potentially subject to a range of adversarial attacks, including directed energy weapons, kinetic threats, cyberattacks, electromagnetic spectrum fires, and nuclear weapons. To adequately evaluate the survivability of U.S. space systems against such engagements and to mitigate any identified vulnerabilities, the Department requires space-range infrastructure (physical and digital), instrumentation, and high-fidelity-threat surrogates and M&S tools.

As per the FY22 Consolidated Appropriations Act, Congress provided $57 million to DOT&E, USD(R&E), and the Space Force. DOT&E is focusing its resources ($9 million) on the development of tools for operational and live fire T&E. USD(R&E), as managed by TRMC, is focusing its investments ($33 million) on prototyping space telemetry collection and replicating space radio frequency environments. The Space Force is focusing its investments ($15 million) on accelerating the National Space Test and Training Complex, specifically on developing a foundational and scalable software baseline for an enduring on-orbit capability, acquisition of a dedicated space command and control antennas, and a prototype model-based system engineering baseline for future digital space T&E campaigns informed by LVC testing.

AUTONOMOUS SYSTEMS AND ARTIFICIAL INTELLIGENCE

Autonomous and artificial intelligence (A&AI)-based systems are software-intensive and data-driven systems that can learn over time and develop emergent behaviors. Current range control and range safety systems will need to be updated to account for with A&AI systems during live testing systems, particularly with manned/unmanned teaming. The following T&E infrastructure investment areas are projected to be required to evaluate A&AI performance as such systems evolve:

- Data – Massive amounts of data are needed to make adequate assessments of A&AI in OT. Input and output data are critical for a full understanding of system capability and its effect on the downstream systems that execute its decisions. Data management investments are key to ensuring viable data sets for training, stimulation, and validation of AI-enabled systems. Other important aspects of data management to T&E include storage, access, processing, visualization, and security.
- Software – Fully matured A&AI systems are highly reliant on stable software. While the machine learning and deep learning math libraries and algorithms are available via commercial off-the-shelf means, AI software development tools and services are required to load, build, and test the various AI models. Adequate understanding of A&AI software builds trust, determines cause and effect relationships, and most importantly, identifies vulnerabilities to adversary tactics.
- Architecture – To facilitate the use and sharing of data, high-performance computing and network investments are needed. Multi-site DOD networks, like the Defense Research and Engineering Network, that connect test venues and support test events, need modernization to access enterprise-wide services. T&E of A&AI systems will also expand OT&E's human factors assessment process. OT&E will evaluate human-machine teaming capabilities by conducting human factors analysis of warfighters using AI-enabled systems. This entails efficient data capture of message traffic across the machine-human interface, the tactical decision operating picture, and other services. Specific attributes to an efficient network architecture include high-bandwidth and low-latency data transfer.
- LVC – In order to present an AI or autonomous system with enough operationally representative scenarios, a robust LVC environment is needed. AI system performance will be validated via a combination of virtual and physical testing. Among other attributes, the LVC test environment will consists of sensors, cameras, computers, software (machine learning), and remote operators.

JOINT ALL-DOMAIN OPERATIONS (JADO)

JADO will move mission concept of operations away from single sensor-to-shooter solutions (i.e., kill chains), toward fusion of all sensor data into a single image of the battlespace utilizing Joint All-Domain Command and Control (JADC2). JADC2 will use the fused image to identify the most effective solutions to deny, disrupt, or destroy the enemy forces (i.e., kill webs). Similarly, an evaluation of a complete, integrated air, cruise missile, hypersonic, and missile defense portfolio is required to successfully assess such capabilities in the multi-domain operating environment.

T&E in the JADO environment will require the critical test and training ranges to be interconnected with high-bandwidth secure communications. During T&E, weapon systems will be evaluated on their contribution to the kill-web solution. In addition, T&E in the JADO environment will require:

- An adequate operational test venue for hardware-in-the-loop and distributed testing.
- Big Data Centers with A&AI-based tools to collect and assess the massive amount of data that will be generated during test events.
- Fusion engines to analyze and utilize the data.
- Credible models and simulations, including digital twins, to represent both the U.S. (blue) and adversary (red) systems.
- Tools and methods for assessing mission threads JADC2 decisions.

COMMON RANGE INSTRUMENTATION AND INFRASTRUCTURE

Significant changes to the T&E range instrumentation and infrastructure are needed to enable adequate evaluation of advanced weapon systems. For example, the DOD needs:

- State-of-the-art tracking radars, telemetry systems, infrared/optics, and threat emulators and targets to enable operationally representative evaluation of the future Joint Force.
- Expanded instrumented range space for advanced long-range weapons systems and modern blue and red weapon systems that operate over large distances.
- High-speed, multi-level, secure communications within and across test and training ranges to enable T&E in JADO environments.
- State-of-the-art, high speed test tracks.
- Develop a transmitting target detector for the Rolling Airframe Missile, a radio frequency interference model, an enterprise test bed Dual-Band Radar model, and an Evolved Sea Sparrow Missile Block 2 M&S tool in support of several surface warfare programs.

USD(R&E) has several ongoing efforts to modernize and equip T&E ranges to meet these needs:

- Development of MDC overland corridors impacting at WSMR, which is expected to deliver a Programmatic Environmental Impact Statement before the end of calendar year 2022.
- Development of the Next Generation Air Combat Maneuvering Instrumentation/Time Space Position Information to enable more realistic air combat exercises against networked integrated air defense systems.
- The Joint Mission Environment Test Capability Multi-Level Security project that will be evaluated from an OT&E perspective.
- Next Generation Optical Tracking Capability, which was successfully demonstrated this year and is on schedule for delivery in FY23.
- Assessment of alternatives for repair or replacement of the Holloman High Speed Test Track.

» WARRIOR INJURY ASSESSMENT MANIKIN (WIAMAN)

WIAMan is a military-specific anthropomorphic test device (ATD) the Army intends to use to evaluate injuries to ground combat vehicle occupants due to vertical accelerative loading typically observed in mine engagements. The WIAMan program consists of three main efforts:

- Development of the ATD with an integrated data acquisition system.
- Biomechanics research to accurately characterize and predict the injury.
- Development of a finite element model of the WIAMan to support future M&S assessments.

WIAMan was successfully used to assess injuries for the first time in Armored Multi-Purpose Vehicle full-up system-level testing, which was completed in FY22. In FY22, the U.S. Army Combat Capabilities Development Command Analysis Center investigated the range of applicable postures for the injury criteria.

The Army currently has 10 WIAMan ATDs and does not plan to buy any additional WIAMan ATDs. Some vehicles seat more than 10 occupants and LFT&E is ongoing for multiple programs simultaneously. DOT&E assesses that the current Army inventory of 10 WIAMan ATDs is not sufficient to support the LFT&E programs, to include, but not limited to: Mobile Protected

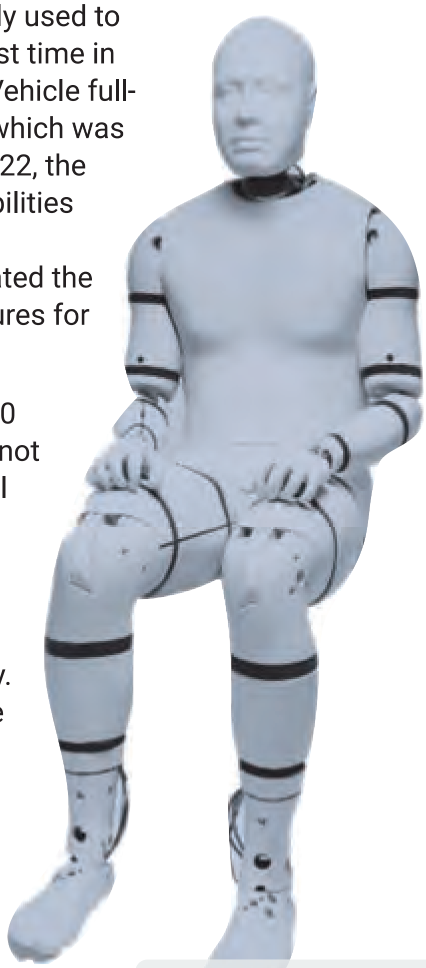


Figure 4: WIAMan ATD

Firepower, Optionally Manned Fighting Vehicle, Stryker 30mm, and M88 Recovery Vehicle. The cost of each WIAMan ATD is approximately $900,000.

DOT&E recommends that the Army investigate whether additional funding for the WIAMan program is needed to purchase additional WIAMan to support LFT&E; improve the accuracy of the injury criteria across all relevant postures; and determine if there is a joint need from other Services, such as, for example, the Marine Corps Advanced Reconnaissance Vehicle program.

THREAT AND TARGET SYSTEMS

The DOD needs additional advanced threat and target surrogates across all domains to conduct authoritative end-to-end, open-air testing, and credible virtual testing of U.S. weapons systems in an operationally representative contested environment. Specifically, the T&E enterprise needs to:

- Develop and field fifth-generation aerial targets.
- Develop and field representative surface-to-air threat system surrogates (i.e., accurate shapes and signatures).
- Develop or procure reprogrammable ground-, ship-, and air-based air defense radars and electronic attack threat surrogates capable of representing the capabilities of new and emerging near-peer threats.
- Develop or procure adversarial hypersonic missile and advanced Anti-Ship Cruise Missile (ASCM) threat surrogates.
- Develop or procure advanced ballistic missile threat surrogates with modern countermeasure suites.
- Field an unmanned test capability that provides a more realistic threat to evaluate the effectiveness of U.S. combat ships' self-defense systems and ship survivability unsupported by live tests against manned ships.
- Develop threat submarine targets with countermeasures that are representative of the current and emerging threats.
- Develop threat representative targets to evaluate the performance of hypersonic missiles and directed energy weapons (either offensive or defensive).
- Develop a set-to-hit target for the evaluation of Navy torpedo programs.

As per the FY22 Consolidated Appropriations Act, Congress provided $114 million to DOT&E, USD(R&E), and the Navy to develop peer-representative targets.

- DOT&E is focusing its investments ($19 million) for: 1) the development of validated threats surrogates (e.g., ballistic missiles, surface-to-air missiles, directed energy, air intercept radars, torpedoes, etc.) required for operationally realistic evaluations, and 2) development of weaponeering tools that will also be used for credible evaluation of the lethality of U.S. weapons against emerging targets.
- USD(R&E) is focusing its investments ($59 million) on the development of fifth-generation aerial target prototypes, an instrumented surrogate cruise missile target, and an HPM source suitable for airborne environments.
- The Navy is focusing its investments ($36 million) on recapitalizing the Sea Range Mobile Ship Target, accelerating the Atlantic Undersea Test and Evaluation Center (AUTEC) In-water Sensor Replacement Program, and developing supersonic sea-skimming target payloads.

KNOWLEDGE MANAGEMENT AND BIG DATA ANALYTICS

Data sharing obstacles among critical stakeholders continue to challenge timely and complete analysis by the assessment community. Limited investment in operationally realistic communication data architectures for distributed testing challenges interoperability testing. In accordance with the DOD Data Management Strategy, the T&E enterprise needs a multi-level secure enterprise knowledge and data management system to keep pace with the volume and complexity of T&E data needs. This includes:

- Development of data standards, data repositories, data marts, and an enterprise data architecture that make data and analysis artifacts easily ingestible, discoverable, and accessible.
- Big-data analytic capabilities that enable efficient search and analyses of large amounts of data at scale, and that include data fusion integrated across multiple test ranges and domains. This includes secure cloud-based parallel-processing capabilities.

This enterprise T&E knowledge and data management system must securely leverage both commercial and purpose-built big data analytics and cloud computing technologies to improve data discoverability and accessibility. This will drive higher evaluation quality and efficiency, leading to more comprehensive and timely information compilation for decision making.

THE T&E ENTERPRISE WORKFORCE

The T&E enterprise faces both workforce "demand" and "supply" challenges. On the demand side, T&E job complexity to support faster and more effective evaluation of complex and interconnected systems has increased dramatically over the last few years. Contributing factors include the rise of software-intensive systems and modern technologies such as autonomous/AI-enabled systems. In addition, the increasingly dynamic and joint multi-domain operations environment that includes advanced maritime, air, land, cyber, space, and electromagnetic spectrum threats must be accounted for throughout the system lifecycle. The demands of innovative, adaptive acquisition framework initiatives call for rapid delivery of new capabilities and at more iterative increments, placing added burden on the workforce to meet shift-left objectives including diminishing acquisition timelines.

On the supply side, the T&E enterprise faces strong competition for top talent. For example, it is difficult to attract and retain talent given the commercial industry's compensation advantages. Additionally, the half-life of technical T&E skills is increasingly shrinking, which further strains the T&E enterprise's learning and development capabilities.

Taken together, these challenges are overextending the T&E workforce without alleviating talent gaps and shortfalls. While each of the Services is addressing most of these shortfalls to varying degrees, we recommend taking a more holistic, T&E enterprise approach. Specifically, the T&E enterprise should get together to share their initiatives and lessons learned, as well as:

- Assess the T&E workforce architecture to identify gaps and opportunities to build future T&E skills, jobs, and workforce composition to support evolving mission requirements.
- Assess, recommend, and implement improvements to the T&E enterprise's talent acquisition processes and pipeline for recruiting high-quality talent in each project office and matrixed organization.
- Complete a Learning Needs Assessment to identify T&E training needs, curriculum gaps, duplicative courses, and opportunities to expand learning and development access across the T&E enterprise.
- Develop and sustain the execution of world-class training, internships, and job rotations in specific technical areas, with periodic refresh, to support the skills of the future.
- Continue to build partnerships with and create reach-back mechanisms to access subject matter experts within key universities, research organizations, industry, federal, and international partners, to share and apply lessons learned, and leverage T&E investments in areas of mutual interest. The Army has reported some success in this area.
- Evaluate the development of an occupational series career code for T&E.
- Evaluate the need to activate reserve officers for short tours providing unique blend of skill sets. The Missile Defense Systems (MDS) OTA has observed some success in this area.

Direct hiring authorities continue to add value to the T&E enterprise.

RANGE SUSTAINABILITY

» 5G AND RADIO FREQUENCY SPECTRUM FOR T&E

National spectrum policy supports turning over more spectrum resources to commercial users in frequency bands currently used to support testing and training. This spectrum sell-off is competing with the Department's increased need for additional spectrum as network-centric systems expand. While the Department continues to work with agency partners to develop transition plans to accommodate spectrum sales and joint use policies, there are several concerns that may limit the Department's ability to assess combat system effectiveness and survivability. These concerns are related to the ability to emulate 5G networks for: 1) accurate representation of the operational environment, 2) spectrum sharing strategies in the S-Band, and 3) impact of 5G L-Band on GPS and Iridium satellite telephone systems.

» WIND FARMS

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

SERVICE T&E ENTERPRISE INPUT

» ARMY T&E ENTERPRISE

The Army reported a balanced program across the Future Years Defense Program (FYDP, FY24-FY28). The Army increased T&E funds in FY24 and has reported significant investment across the FYDP to improve T&E capabilities ranging from investments in DT test centers and OT instrumentation, targets and threats, to include cyber improvements. The Army did indicate the need for TRMC's assistance with funding for threat systems.

» NAVY T&E ENTERPRISE

The Navy T&E enterprise reported a balanced and adequate Major Range and Test Facility Base, T&E Support, and target budget to support Navy T&E requirements. For example, the Navy added additional resources for the upcoming maintenance availabilities for the Self Defense Test Ship and Mobile At-Sea Sensor Barge to ensure the long-term viability of these test platforms. The Navy expressed concern over continued efforts to develop offshore renewable energy projects in offshore Warning Areas used to conduct test and training. The Navy also expressed a concern over the selloff of additional spectrum dedicated to exclusive federal use. Loss of maneuver space above, on, and below the surface, and access to dedicated spectrum will challenge the Navy's ability to ensure future readiness.

» MARINE CORPS OPERATIONAL TEST AND EVALUATION ACTIVITY (MCOTEA)

MCOTEA reported adequate funding to enable planning, execution, and reporting of mandated T&E responsibilities. MCOTEA also reported strong collaboration with the Navy to highlight any range limitations that would affect the evaluation of the

USMC mission. Examples include the ability to adequately represent the multi-domain operating environment, electromagnetic spectrum and infrastructure, tools, processes, and workforce needed to evaluate autonomous and AI-enabled systems.

» AIR FORCE AND SPACE FORCE T&E ENTERPRISE

The Air Force T&E enterprise reported a balanced and adequate FY24 funding program needed to meet OT&E and LFT&E requirements. The Air Force reported an increase in resources across the FYDP to support space system operational tests, the Weapon System Evaluation Program, and the Space Test Course. The Air Force also reported transferring additional resources to enable recapitalization of the space test and training range family of capabilities to conduct combat relevant space electronic warfare testing and training.

» JOINT INTEROPERABILITY TEST COMMAND (JITC)

JITC reported an adequately funded operating account while citing several critical unfunded requirements across the FYDP, to include a need to upgrade their facilities, modernize test bed operations, radio test capability engineering, tactical data link, M&S tools, and test automation. JITC also reported a continued challenge to recruit and retain specialized positions such as cyber security professionals.

» MDA AND THE MDS OTA

The MDA reported an adequate FY24 budget while acknowledging the benefits of Congressional support to meet the MDS Integrated Master Test Plan (IMTP) version 24.0 requirements. MDA assures full access to resources to enable the MDS OTA team's execution of mandated T&E responsibilities. The MDA and MDS OTA team continue refining the budget for future growth, including all-digital venue, space sensor layer, and hypersonic defense requirements as details mature. Specifically, MDS OTA:

- Partnered with the intelligence community and MDA to advance threat model development and ensure applicability to ground test venues.
- Deployed new cloud-based analytical tool suites to accommodate new mission areas, increase handling of large data sets, and use on-demand cloud computing to produce faster analysis and reporting.
- Provided M&S requirements and data needs for accreditation to support operational assessments.
- Enhanced reporting of OT accreditation and model limitations through web-based data tools.
- Strengthened reporting to Combatant Commands and Service elements.
- Collaborated with Service Reserve Components to tap unique civilian expertise and augmented cybersecurity teams with non-DOD cybersecurity experts.

MDA has identified the Pacific Collector/Pacific Tracker Ship Replacement as a critical shortfall. MDA also confirmed that the T&E infrastructure is currently limited by the availability and reliability of existing telemetry and range safety system assets in the broad ocean area, as discussed in the hypersonic section of this report. The capacity of test ranges will become stressed as the Sentinel test program ramps up while also stretching current T&E personnel.

SUMMARY

Accurate evaluation of warfighting capabilities requires an adequate representation of the theater-representative operating environment during test, which is accomplished by T&E resources. It also requires equipment that can adequately measure technical and operational performance of emerging or fielded warfighting capabilities in that environment. The DOD has an array of test and training ranges and capabilities managed, funded, and operated by different stakeholders. To enable efficient and structured modernization and sustainment of existing range capabilities while also transforming the ranges to meet the demands of the future, it is important to have an accurate and common picture of existing and required, future range capabilities. It will be equally important to ensure this common picture is accurate, digitized, and transparent to key T&E stakeholders to enable collaboration in developing joint/interoperable solutions, avoiding redundancies while increasing capability delivery and efficiencies. In FY23, DOT&E intends to establish a multi-disciplinary team to kick off the following actions:

- Develop, digitally document, prioritize, and track T&E range capability and funding requirements including threats and targets needed for adequate operational and live fire T&E of current and emerging DOD warfighting capabilities. This will include physical and virtual infrastructure with focus on adequate operational T&E of emerging technologies and kill-webs within DOD scenarios, vignettes, mission threads, and joint warfighting concepts. The desired end state is an accurate and validated data dashboard of existing and required capabilities, and their statuses, accessible to key T&E and funding stakeholders.
- Review the range enterprise funding model to identify courses of actions that might introduce efficiencies.

The successful execution of these actions will depend on the cooperation of Service T&E Executive Offices, Program Offices, and range commanders to share relevant data and inform the dashboard design solutions. Success will also depend on input and collaboration with the TRMC within USD(R&E).

DOD PROGRAMS

Aerosol and Vapor Chemical Agent Detector (AVCAD)

The Aerosol and Vapor Chemical Agent Detector (AVCAD) program completed planned Engineering and Manufacturing Development phase testing, as documented in the Test and Evaluation Master Plan, including a multi-phase operational assessment (OA) in FY22. The Program Office worked with two different vendors developing systems to investigate performance issues, institute reliability upgrades, and plan and conduct regression testing. The AVCAD program conducted extensive developmental test (DT), including ship shock and vibration testing, an OA, a DT Soldier Touch Point, and combined DT/operational test (OT) in FY22 to support the planned February 2023 Milestone C Low-Rate Initial Production (LRIP) decision. The Air Force withdrew from the OA and the program due to changes in employment concept and concerns that the detector would not meet their requirements. During the OA events, the vendors' systems experienced numerous false alarms and reliability issues. The program conducted a Soldier Touch Point which demonstrated some reliability improvement. The program allowed one vendor's contract to expire. The program should implement corrective actions to improve performance and conduct regression testing prior to Milestone C.

SYSTEM DESCRIPTION

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

MISSION

Joint warfighters equipped with the AVCAD will employ the system to detect chemical warfare agents 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 across the full range of military operations

PROGRAM

The AVCAD program is a joint Acquisition Category II program in the Engineering and Manufacturing Development phase of acquisition. DOT&E approved the Milestone B Test and Evaluation Master Plan in 2019 and subsequent changes to this plan in 2021. The Program Office conducted an in-depth review of the technical, cost, and schedule risks to achieve the required performance for the two Milestone B contractors in 2022. The Government chose to continue the contract with Smiths Detection Incorporated. The Milestone C LRIP decision is planned in February 2023.

» MAJOR CONTRACTOR

- Smiths Detection Incorporated – Edgewood, Maryland

TEST ADEQUACY

The AVCAD program conducted extensive developmental test (DT), an OA, a DT Soldier Touch Point, and combined DT/operational test (OT) in FY22 to support the planned Milestone C LRIP decision. DT included multiple phases of false alarm testing in various operational environments, military standard durability testing, and electromagnetic interference testing to assess suitability in operationally realistic environments. DT/OT included chemical agent testing and chemical, biological, radiological, and nuclear survivability testing. The Army, Navy, and Marine Corps conducted the OA that included two phases of land-based testing, shipboard testing, a cybersecurity cooperative vulnerability penetration assessment, and a cyber-adversarial assessment. DOT&E observed the OA events, the DT Soldier Touch Point, and some of the False Alarm DT. The OA events were conducted in accordance with DOT&E-approved test plans. Agent chamber testing identified system performance degradation over time. The program manager decision to not conduct additional AVCAD DT/OT agent chamber test on systems used during field testing leaves uncertainty about the impact of prolonged operational use on AVCAD performance. Multiple software algorithm changes during DT/OT chemical chamber testing, without regression testing leave unanswered questions regarding overall system performance. Otherwise, the testing conducted was adequate to identify performance issues and assess progress toward operational effectiveness, suitability, and survivability. The use of pre-scheduled cyberattacks and the time required to establish connectivity of the AVCAD sensor network resulted in missed opportunities to assess the operational impacts of cyberattacks. The AVCAD program should plan and conduct regression testing to verify corrective actions and performance improvements prior to the Milestone C LRIP decision in February 2023.

PERFORMANCE

» EFFECTIVENESS

The Smiths Detection AVCAD has demonstrated the capability to detect the required liquid and solid aerosol threats, but not at the required sensitivity. The vender is continuing to refine the hardware and software. The AVCAD detection performance degrades in high humidity environments. The system's false alarm rate exceeds the required level in some key operational environments. Testing identified significant system-to-system performance variability.

» SUITABILITY

The AVCAD system suitability has improved over time. Despite this upward trend, the system reliability at the May 2022 Soldier Touch Point was less than 13 percent of the required 850 hours mean time between operational mission failures, which was driven by Air Force requirements. The Joint Staff is working with the Army, Navy, and Marine Corps to reassess the operation requirements based on the Air Force's withdraw from the program. Testing identified continuing reliability issues related to battery power, failures related to the sensor air flow path, and wireless radio network connectivity. This resulted in burdensome operator field maintenance and higher level maintenance actions that created gaps in sensor coverage and delays recognizing that a simulated chemical attack had occurred. Military operators continue to express concern with the physical burdens associated with carrying the AVCAD over distances because of its size and weight. Operators noted that the brightness of the current night vision display mode makes it difficult to read when wearing night vision goggles.

» SURVIVABILITY

Test units were not able to distinguish cyberattacks from stimulated chemical attacks during the operational assessment. The cyberattacks had limited impact to operations. Ship shock, vibration, and electromagnetic interference testing resulted in AVCAD failures, which need to be resolved prior to continued operation.

RECOMMENDATIONS

The Program Office should:

1. Work with the Joint Requirements Office and the Services to reassess the operational performance and reliability requirements due to the Air Force departure from the program.
2. Work with Smiths Detection to determine required changes to the system to address identified deficiencies.
3. Work with the Service Operational Test Agencies and DOT&E to identify and execute adequate regression testing to evaluate changes to the AVCAD in support of a Milestone C LRIP decision planned in February 2023.
4. Address cybersecurity deficiencies prior to the next phase of cybersecurity testing.
5. Address deficiencies identified during ship shock, vibration, and electromagnetic interference testing.

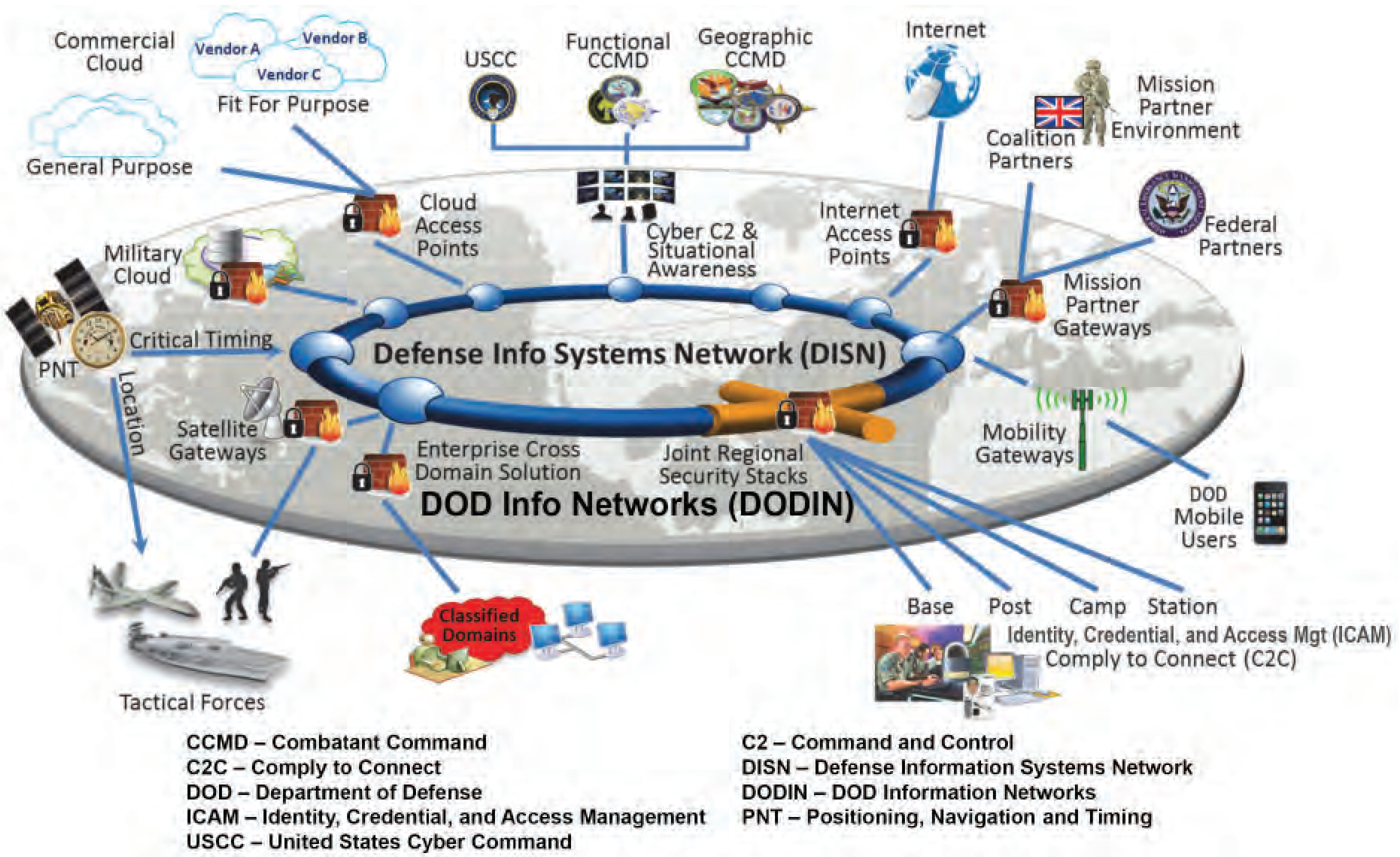
Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives

The former Deputy SECDEF approved the DOD Digital Moderation Strategy (DMS) in 2019. The DOD Chief Information Officer (CIO), Defense Information Systems Agency (DISA), and Services have been implementing programs, projects, and initiatives intended to achieve DOD DMS objectives. Many DMS initiatives lack an overarching systems integration process, test strategy, and program executive organization to manage cost, drive schedules, and monitor performance. Deploying untested DMS programs, projects, and initiatives poses an operational risk to the DOD enterprise, particularly in a cyber-contested environment. Future deployment decisions need to be informed by adequate OT&E.

SYSTEM DESCRIPTION

The DOD DMS summarizes the Department's approach to information technology (IT) modernization, focused on the Joint Information Environment Framework intended to improve networking capabilities for fixed and mobile users. The DOD DMS aims to institute new enterprise IT services, modernize technology through coordinated refresh efforts, implement a new joint cybersecurity capability, and improve access to data. DOT&E is monitoring the DMS programs, projects, and initiatives that could provide significant benefits to the DOD, but also could pose a significant operational risk to the DOD in a cyber-contested environment. These FY22 efforts align with the DOD DMS to:

- Deliver a DOD enterprise cloud environment that leverages commercial technology and innovations
- Optimize DOD office productivity and collaboration capabilities, e.g., Enterprise Collaboration and Productivity Services (ECAPS) Capability Set 1 - Defense Enterprise Office Solution (DEOS), Microsoft Office 365 (O365), and ECAPS Capability Sets 2 and 3
- Deploy an end-to-end Identity, Credential, and Access Management (ICAM) infrastructure to support DOD systems
- Transform the DOD cybersecurity architecture to implement Zero Trust throughout the DOD Enterprise, including initiatives to provide endpoint security for devices (both desktop and mobile devices)
- Implement cybersecurity capabilities to protect the DOD Information Network and support defensive cyber operations and network operations for bases, posts, camps, and stations (known as Joint Regional Security Stack (JRSS))
- Strengthen collaboration, international partnerships, and allied interoperability through a Mission Partner Environment (MPE).



PROGRAMS, PROJECTS, AND INITIATIVES

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

- **Enterprise Collaboration and Productivity Services (ECAPS)** – In FY22, the DEOS Program Office began efforts to provide commercial cloud-hosted SIPRNET office productivity and collaboration capabilities (known as DOD365-SEC) with testing support provided by the Joint Interoperability Test Command (JITC). JITC is developing a Test and Evaluation Strategy (TES) for DOD365-SEC and intends to perform early operational testing in FY23. In FY22, the DOD CIO and DISA reviewed technologies and are finalizing a strategy for DOD users to be provided ECAPS Capability Set 2 (Business Voice and Video) by FY24 and Capability Set 3 (Precedence-based Command and Control Voice) by FY25.
- **Identity, Credential, and Access Management (ICAM)**, based on the draft DOD Enterprise ICAM Implementation Plan, comprises 30+ enterprise capabilities managed by DOD Components intended to create a secure, trusted environment where authorized users can access IT resources. The DOD CIO is the lead for ICAM governance and intends to establish an ICAM Executive Board to manage Enterprise ICAM efforts. The DOD CIO is clarifying the roles, responsibilities, and lines of authority for DOD enterprise ICAM capabilities. In FY22, DISA developed an enterprise Global Directory Service to provide cryptographic authentication for SIPRNET. In FY22, DISA began integrating several financial application pilots with the DISA ICAM capabilities; this effort will continue and expand to other financial applications in 2023. In FY23, JITC is funded as the operational test agency (OTA) to support DISA ICAM capability testing. A major ICAM acquisition effort is the Public Key Infrastructure, detailed in this Annual Report.
- **Zero Trust** is a data-centric security model that eliminates the idea of trusted networks, devices, personas or processes and enables authentication and authorization policies under the concept of least privileged access. Zero Trust implementations can repurpose network security to augment data-centric security. The DOD CIO is developing and intends to publish a Zero Trust Strategy in 2023 as well as a companion Endpoint Security Strategy. In FY21, DISA began planning a Zero Trust effort (known as Thunderdome) focused on the network infrastructure. DISA awarded the Thunderdome prototype contract in January 2022. The Services can use Thunderdome or implement their own Zero Trust solutions. JITC is planning to conduct operational testing of the NIPRNET Thunderdome pilot in FY23. DISA intends to begin user migrations to initial Thunderdome capabilities in late FY23. DISA is also working on a new initiative to integrate Thunderdome pilot capabilities with SIPRNET modernization efforts.
- **Joint Regional Security Stack (JRSS)** – Previous testing demonstrated that JRSS could not help cyber defenders withstand threat-representative attacks. In FY21, the DOD CIO began efforts to phase out JRSS and to transition to a new Zero Trust security and

network architecture. JITC did not conduct JRSS operational testing in FY22. In FY23, JITC intends to complete the cyber survivability assessment and an operational assessment of the final JRSS capability upgrades. JRSS is scheduled to be decommissioned by the end of FY27.

- **Mission Partner Environment (MPE)** – In support of DOD Directive 5101.22E, the Air Force is acquiring strategic, operational, and tactical MPE services tailored to meet mission partner information sharing needs, while consolidating existing MPE capabilities, such as Combined Enterprise Regional Information Exchange Systems (CENTRIXS), across the DOD. In FY22-23, the Air Force is integrating commercial collaboration capabilities with a National Security Agency-developed Zero Trust architecture to create a DOD-owned and operated cloud environment that will enable secure mission partner information sharing. The Air Force is developing a test strategy and intends to conduct future MPE testing in the JITC-sponsored Coalition Test and Evaluation Laboratory with mission partners.
- **Enterprise Cloud Efforts** are initiatives intended to leverage commercial cloud innovation for the DOD enterprise to deliver infrastructure and services. DISA disestablished military cloud (milCloud) 2.0 in FY22 and then established a new government-owned cloud (known as Stratus). Stratus is an on-premise cloud built to meet unique DOD mission requirements. Stratus provides multi-tenant, self-service management capabilities for cloud computing, storage, and network infrastructure. DISA is developing the Joint Warfighter Cloud Capability (JWCC) multi-vendor commercial cloud contract with a projected award date in early FY23.

TEST ADEQUACY

- **ECAPS:** JITC did not conduct any OT&E of the DOD365-SEC capabilities, or the ECAPS Capability Sets 2 and 3 in FY22. JITC and the DEOS PMO intend to conduct an early operational assessment of the DOD365-SEC capabilities in FY23, and they plan to operationally test the ECAPS Capability Set 2 finalized solution prior to fielding in FY24.
- **ICAM:** JITC conducted limited user acceptance testing of the initial DISA ICAM capabilities associated with several financial application pilots in FY22. There was no formal test planning for DISA ICAM capabilities.
- **Zero Trust:** JITC conducted an early operational assessment of Thunderdome pilot capabilities from August to mid-October 2022 to inform a network architecture decision.
- **JRSS:** JITC did not conduct OT&E of JRSS in FY22.
- **MPE:** The Air Force has yet to coordinate with an OTA to perform independent T&E for the MPE capabilities.
- **Enterprise Cloud Efforts:** The DOD has yet to conduct comprehensive, independent, threat-representative cyber survivability testing of any commercial or government-owned cloud and its hosting infrastructure (to include DOD O365, DOD365-SEC, Stratus, and the planned JWCC effort), which will require appropriate agreements between the DOD and the commercial cloud service providers.

PERFORMANCE

There has been little operationally realistic testing performed on DMS programs, projects, and initiatives, precluding an evaluation of their operational effectiveness, suitability, or cyber survivability. Many DMS efforts lack an overarching systems integration process, test strategy, and program executive organization to manage cost, drive schedules, and monitor performance factors. Many DMS initiatives also use commercial cloud environments, but threat-representative cyber survivability testing on the commercial side of cloud environments is not currently being conducted by the DOD per the DOT&E memorandum, Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, dated April 3, 2018.

RECOMMENDATIONS

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

1. Manage the key ICAM capabilities, and all other DMS initiatives, with trained program managers and supporting offices.
2. Designate an OTA for ICAM capabilities and develop an overarching ICAM TES that encompasses the key issues and concepts to be tested.
3. Designate an OTA for MPE and develop an MPE TES.
4. Fund JITC to fully support DMS enterprise IT initiatives, testing, and test-related forums.
5. Develop a TES for DOD365-SEC, and more generally a TEMP or TES for each funded DMS enterprise IT initiative.
6. Conduct adequate cyber survivability testing of all DMS enterprise IT programs, projects, and initiatives in accordance with current DOD and DOT&E cyber survivability T&E guidance and policy.
7. Perform threat-representative cyber survivability testing of military and DOD commercial cloud environments, to include the commercial infrastructure operated by cloud service providers.
8. Conduct comprehensive cyber survivability testing of Zero Trust implementations to inform fielding decisions.
9. Use operational test data, analyses, and reporting to inform DMI EXCOM decisions.

F-35 Joint Strike Fighter (JSF)

Twenty F-35B aircraft aboard USS Tripoli *(LHA 7) during FY22 demonstration of Lightning Carrier Concept*

The F-35 program made steady progress in FY22 to prepare the Joint Simulation Environment (JSE) for the 64 JSE test trials required to complete IOT&E. The current estimated completion of IOT&E trials in the JSE is the end of August 2023, a date that DOT&E considers at risk, due to the possibility of further discoveries of deficiencies and potential delays in the verification, validation, and accreditation (VV&A) process.

The F-35 program continues to field immature, deficient, and insufficiently tested Block 4 mission systems software to fielded units. The operational test (OT) teams continue to identify deficiencies that require software corrections and, with them, additional time and resources.

The F-35 Joint Program Office (JPO) has not adequately planned for operational testing of the upgraded hardware configuration, referred to as Technology Refresh 3 (TR-3), that is currently scheduled to be delivered in production Lot 15 aircraft, beginning in 4QFY23. Additionally, the necessary flight test instrumentation (including both aircraft and Open Air Battle Shaping (OABS) instrumentation) for both the remaining Technology Refresh 2 (TR-2) and upgraded TR-3 OT aircraft is not all on contract and will not be available, so OT squadrons may not have sufficient test aircraft with adequate capability or sufficient time to test new capabilities before operational employment.

SYSTEM DESCRIPTION

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

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

The F-35 Block 4 Modernization Capability Development Document specifies required capabilities and associated capability gaps that drive incremental improvements.

MISSION

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

PROGRAM

The F-35 JSF is an Acquisition Category ID program. DOT&E approved the fourth revision of the System Development and Demonstration (SDD) Test and Evaluation Master Plan (TEMP), which governs the conduct of IOT&E, in March 2013. DOT&E approved the F-35 Overarching Block 4 TEMP and Increment 1 Annex on May 18, 2020. The Increment 1 Annex covers the Block 4 developmental and operational flight testing of software versions 30R03 though 30R06, which were completed in 3QFY21. The Increment 2 Annex, which covers Block 4 software versions 30R07, 30R08, and 40R01, and their associated hardware enablers, to include the transition from TR-2 to TR-3 equipped aircraft in the production line, is in final staffing within OSD at the time of this report. Increment 3 Annexes, which cover Block 4 software versions 40R02 through 42R01, and their associated hardware enablers are in coordination with the F-35 JPO. The Block 4 TEMP and associated Annexes govern the conduct of FOT&E.

» MAJOR CONTRACTORS

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

F-35B aircraft aboard USS Tripoli *(LHA 7) , August 2022*

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

F-35 Development Phase	Major Avionics Hardware	Capabilities	Mission Systems Software	Operational Testing*
SSD	TR-1	Block 2B	Block 2B Software	• Marine Corps Fielding Reports and F-35B IOC • Service and JOTT test events • Formal OUE canceled
	TR-2	Block 3i	Block 3i Software	• Air Force Fielding Reports and F-35A IOC • Service and JOTT test events
		Block 3F	Block 3F/ 3FR6**	**Pre-IOT&E Increment 1 (Jan – Feb 2018) Cold Weather Deployment** For-score testing to evaluate the suitability of the F-35 air system and alert launch timelines in an extreme cold weather environment
			Block 3F/30R00***	• Navy Service Fielding Reports • **Pre-IOT&E Increment 2 (Starting Mar 2018)** For-score testing of limited two-ship mission scenarios, F-35A deployment, F-35C deployment to a carrier, and weapons delivery events
C2D2		Block 4, 30 Series	30R02.04	**Portion of Formal IOT&E (Dec 2018 – Sep 2019)** For-score testing of more complex open-air missions
			30R04.52	**Portion of Formal IOT&E (Jul 2020)** For-score testing of more complex open-air missions
			30R06.041 & .042	UOTT evaluated these versions in FY21 IAW a DOT&E-approved FOT&E Test Plan
			30R06.042	Software fix needed for weapon event in **Jun 2021 that completed events approved in Pre-IOT&E Increment 2**
			30R07	UOTT evaluated this series of software versions in FY22 IAW a DOT&E-approved FOT&E Test Plan
			30R08	UOTT began flying with early versions of this software in August, 2022. DOT&E approval of a FOT&E Test Plan for 30R08 is TBD
	TR-3	Block 4, 40 Series	40R0X	Dedicated operational tests planned for each release of capability in the series

Notes:

* For-score IOT&E events are highlighted in bold.
** The final planned version of Block 3F software was 3FR6.
*** The program changed software nomenclature for the initial increments of Block 4 from "3F" used during SDD to "30RXX" for development and "30PXX" for fielding software. The 30 Series software is compatible with the Block 3F aircraft hardware configuration and is being used to address deficiencies and add Service-prioritized capabilities.

Acronyms: C2D2 – Continuous Capability Development and Delivery; EA – Electronic Attack; IAW – In accordance with; IOC – Initial Operational Capability; JOTT – JSF Operational Test Team; OUE – Operational Utility Evaluation; SDD – System Development and Demonstration; TBD – To be determined; TR-X – Technology Refresh [version #], referring to the suite of various avionics and supporting subsystems; UOTT – U.S. Operational Test Team

» IOT&E

Open-Air Testing

The F-35 program is nearing completion of a multi-year IOT&E. The JSF Operational Test Team (JOTT) completed and DOT&E observed a series of weapons trials (both bombs and missiles); mission trials; and testing that compared F-35 performance to that of fourth-generation fighters against traditional and more modern surface-to-air threats currently fielded by potential adversaries. Open-air test missions evaluated the F-35 in multiple roles: offensive counter-air (OCA), defensive counter-air (DCA), cruise missile defense, suppression/destruction of enemy air defenses (S/DEAD), reconnaissance, electronic attack (EA), close air support, forward air control (airborne), strike coordination and armed reconnaissance, combat search and rescue, anti-surface warfare, and air interdiction. The JOTT conducted test trials in varying threat environments using two-, four-, and eight-F-35 aircraft mission scenarios. During the S/DEAD and EA trials, the F-35 faced operationally representative surface-to-air threat environments represented by Radar Signal Emulators installed on the open-air ranges. Open-air test trials were completed with the execution of the final AIM-120 missile trial, which was accomplished using an F-35C aircraft. Deficiencies in earlier versions of the aircraft software prevented this event from being accomplished until June 2021, when the program delivered software version 30R06.042 with the fixes needed to complete the trial.

Modeling and Simulation Development

The required events in the IOT&E test plan that remain to be accomplished are 64 trials, which is 42 percent of the overall mission trial requirement, in the JSE at Naval Air Station Patuxent River, Maryland. These trials include 11 DCA, 22 cruise missile defense, and 31 combined OCA/air interdiction/DEAD trials in operationally representative, dense, defense-in-depth scenarios with the latest threat systems that are not available on open-air ranges. All three F-35 variants will be involved in the execution of the trials.

A robust process has been established to identify, prioritize, track, and fix the remaining JSE deficiencies. The JSE team has focused on addressing open deficiencies that would affect trial validity in the simulator, reducing the list of “must-fix” deficiencies requiring resolution to two as of 26 October 2022. The VV&A effort is ongoing and as of 19 October 2022, 74 percent of the component V&V packages were rated as likely to accredit by the accreditation authority, with the remaining component packages still in work. The team is currently focusing effort on the systems level V&V, which ensures multiple models interact correctly. Current program estimates show IOT&E test missions occurring in August 2023. However, the ongoing VV&A process, as well as test readiness preparations, will likely lead to the discovery of new deficiencies that will need to be corrected prior to the for-score test missions. The time required to fix these deficiencies and update the analysis in the final system-level VV&A documentation will be key indicators of additional schedule pressures. Assuming any remaining key deficiencies are addressed and no significant uncorrectable discoveries occur, the JSE will be on track to provide a well-documented, accredited test venue with sufficient threat and system-under-test fidelity to determine F-35 effectiveness against a near-peer adversary in an operationally representative environment.

Suitability Testing

The JOTT completed and DOT&E observed cold-weather testing; deployments to ships and austere environments; observation of day-to-day maintenance and sustainment activities; interviews with maintenance and sustainment personnel; joint technical data verification; and reliability, maintainability, and availability data analysis and adjudication. The JOTT completed all required suitability-related test plan activities by the end of 1QFY21.

Survivability Testing

The JOTT completed and DOT&E observed cybersecurity testing of the air vehicle (AV), training systems, mission data reprogramming laboratory, and the Autonomic Logistics Information System (ALIS) to include an enterprise adversarial assessment. The JOTT completed all required survivability-related test plan activities by the end of 1QFY21.

» FOT&E

Open-Air Testing

The U.S. Operational Test Team (UOTT) conducted operational testing of 30R07 in FY22 in accordance with the DOT&E-approved test plan. DOT&E observed the test mission trials and weapons events, which included: four Close Air Support test missions flown with F-35B aircraft; three DCA test missions flown with F-35A and F-35C aircraft; four OCA test missions flown with F-35A and F-35C aircraft; four S/DEAD test missions flown with F-35A and F-35C aircraft; and two missiles-test events, one AIM-120 and one AIM-9X. Test efficiency was hindered by poor preparation and readiness of the F-35 test enterprise and the performance of the OABS system, which resulted in invalid trials and the need to reschedule test events..

Per the Block 4 TEMP and associated Annexes, OT aircraft are required to support both developmental and operational testing. Modifications to these aircraft must be funded, scheduled, and completed just after developmental test (DT) aircraft modifications to enable integrated DT/OT, DT assist, and mission-level testing of future capabilities. Although the JPO has funded and contracted for some of the OT aircraft modifications, it currently does not have a scheduled and coordinated plan to ensure that all of the required hardware, flight test instrumentation, and OABS modifications are completed for test aircraft that will remain in the TR-2 configuration or are slated to be modified to TR-3. Because of these issues, adequate OT of the 30R08 capability is not forecast to be completed prior to fielding in the fall of 2023, nor will OT of the first TR-3 production configuration in 40R01 be done prior to the Services accepting the first aircraft in 4QFY23. The TR-3 configuration contains upgraded integrated core processors and other critical hardware updates.

Modeling and Simulation Development

The extended delay in completing the necessary VV&A of the F-35 JSE for conducting the IOT&E test missions has also delayed preparations for operational testing of current F-35 upgrades. Licensing issues associated with the F-35-In-A-Box (FIAB) have also contributed to the delayed JSE modernization efforts. While completing the current VV&A effort, the program should simultaneously make every effort to align JSE delivery to required Block 4 FOT&E periods now, so that the UOTT can use the JSE to accomplish critical testing of future capabilities. These plans must include capability upgrades to the FIAB, blue and red weapons models, and red ground threat models required for FOT&E.

Suitability Testing

The UOTT conducted suitability testing per the annual DOT&E-approved suitability test plan in FY22. The test team conducted interviews with maintenance personnel and pilots on training, technical orders, the use of ALIS, software updates, maintenance of the low observable characteristics of the aircraft, support equipment and tools, and safety issues.

Operational test teams from the Navy and the Marine Corps, supported by the UOTT, participated in testing on the USS *Tripoli* (LHA 7) (pictured at the beginning of this article) to explore the F-35B Heavy Air Combat Element (ACE) concept of operations (CONOPS). This was conducted as FOT&E for the LHA 6 program, per the DOT&E-approved test plan. DOT&E observed the concept exploration exercise and recommends that the Services continue to refine and test the F-35B Heavy ACE CONOPS based on feedback from this event. This should include considerations of ship manning, ACE composition, increased dedicated classified workspace, provisioning of additional Ship's Inertial Navigation Systems cables and refueling stations, and optimizing ALIS to support increased numbers of F-35s over a ship's SATCOM connection to the ALIS Central Point of Entry, accounting for potential reduced emissions control scenarios.

The UOTT continued developing plans to conduct a 30-day demonstration of the capability to conduct F-35 flight operations without ALIS connectivity. The UOTT has not been able to identify a unit to perform this test event, which remains unscheduled. DOT&E considers this testing to be a high priority.

Cybersecurity Testing

The UOTT cybersecurity test teams conducted an on-aircraft cybersecurity assessment of Identification Friend or Foe (IFF) Mode 5 in an anechoic chamber at the Patuxent River Naval Air Station in FY22, in accordance with the DOT&E-approved test plan. More in depth testing is needed to assess the cybersecurity of the AV. To date, on the AV, the UOTT has tested IFF Mode 5, IFF Mode S, GPS, Variable Message Format, Link 16, and weapons interface testing for air-to-ground and air-to-air weapons on the AV. Key systems such as the Multifunction Advanced Data Link, Small Diameter Bomb II, and RADAR are planned for FY23 and later. AV test assets are made available to support AV testing, which is limited in scope based on the potentially disruptive nature of cyber. The Services and JPO should invest in requisite hardware- and software-in-the-loop capabilities to support more robust and representative AV cyber testing.

PERFORMANCE

» IOT&E

Effectiveness

The results of effectiveness testing during IOT&E will be reported within 90 days of completion of testing in the F-35 JSE.

Suitability

Suitability testing is complete. The results of suitability testing during IOT&E will be reported within 90 days of completion of testing in the F-35 JSE.

Survivability

Survivabiliy testing is complete. The results of survivability testing (to include cybersecurity testing) during IOT&E will be reported within 90 days of completion of testing in the F-35 JSE.

» FOT&E

Effectiveness

The JPO designed the current development process, referred to as Continuous Capability Development and Delivery (C2D2), to provide new capabilities and updates in time-phased increments. The program continues to field immature, deficient, and insufficiently tested mission systems software to fielded units without adequate operational testing. Although the program designed C2D2 around commercial "agile software" development concepts, it does not adhere to the industry best practices that include clear articulation of the capabilities required in the Minimum Viable Product, focused testing, comprehensive characterization of the product, and full delivery of the specified operational capabilities. The program has consistently failed to deliver the full set of capabilities contained in their master schedule as defined by the Air System Playbook, which was updated again in FY22 to realign capability delivery to another delayed schedule. Although the program has begun addressing some of the key findings from the 2021 software independent review team, more needs to be done to reduce the discovery of deficiencies in the field, including expansion of and updates to hardware- and software-in-the-loop labs.

The program plans to begin developmental flight testing of the TR-3 configuration in December 2023, with software version 40R01. To begin the transition to TR-3 from TR-2, this version of software was developed using the baseline capabilities provided in the 30R07 Series, which completed development in 1QFY22.

The JSF program continues to carry a large number of deficiencies, and conducts recurring reviews with Service requirements representatives to prioritize resources to address them. Although initial development in Block 4 was intended to both introduce new capabilities and address deficiencies identified during SDD, the overall number of open deficiencies has not significantly decreased since the completion of SDD due to the continued discovery of problems. The new deficiencies include those associated with new capabilities as well as some associated with previously functioning capabilities that no longer work. The operational test teams identified deficiencies associated with communication systems, weapons, fusion, pilot-vehicle-interfaces, and the radar during testing of the 30R06 and 30R07 software versions.

Suitability

The operational suitability of the F-35 fleet remains below Service expectations. In FY22, the trend in aircraft availability was flat, after declining for most of FY21 after a historic program high in January 2021.

At the close of FY22, 540 aircraft have been produced for the U.S. Services. These aircraft do not include any aircraft assigned to dedicated developmental testing and provide the basis of analyses contained in this section of the report.

Aircraft availability is determined by measuring the percentage of time individual aircraft are in an "available" status, aggregated monthly over a reporting period. The historic program-set availability goal is 65 percent; the following fleet-wide availability discussion uses data from the 12-month period ending September 2022. The average fleet-wide monthly availability rate for only the U.S. aircraft (includes all aircraft categories – those designated for combat, training, advanced training and tactics development, and operational test) is below the target value of 65 percent. The DOT&E assessment shows a relatively flat trend in FY22.

The program and Services track aircraft by unit and mission assignment. The combat coded fleet of aircraft are assigned to units that can deploy for combat operations; the training fleet is for new F-35 pilot accessions; the advanced training and tactics development fleet is used for fighter weapons school; and the test fleet for operational testing. The proportion of the fleet that is combat coded has risen steadily over time and represents approximately half of the U.S. fleet over the 12 months ending in September 2022. Consistent with prior Annual Reports, the combat coded fleet, which has the newest aircraft on average and often receives elevated supply priority, demonstrated the highest availability and achieved the 65 percent target for monthly average availability for the overall, combined 12 months ending in September 2022.

Aircraft that are not available are designated in one of three status categories: Not Mission Capable for Maintenance (NMC-M), Depot (i.e., in the depot for modifications or repairs beyond the capability of unit level squadrons), and Not Mission Capable for Supply (NMC-S). The monthly NMC-S rate began climbing (worsening) in July 2021, compared to earlier trends, and stayed relatively flat for most of FY22 with a worsening trend in the last quarter. To improve aircraft availability, the program should continue to pursue maintenance system improvements, especially for common processes distributed among many different NMC-M drivers, such as low-observable repairs, and spares posture for those critical items most in demand.

A significant shortage of fully functional F135 engines has also contributed to reduced aircraft availability. The F-35A variant is most affected by the engine shortage, which has been exacerbated by a lack of depot repair capacity. Recent efforts to lay in additional depot resources, improve depot efficiencies, and ruggedize key engine components have reduced the number of aircraft without an engine. Nonetheless, the program projects that without further action, a lack of propulsion spares will result in some aircraft not having a functional engine through at least 2028.

The F-35 fleet remains below JSF Operational Requirements Document (ORD) thresholds in some areas for overall reliability and maintainability. Maintenance data gathered through April 2022 from the U.S. fleet of all three variants show that the F-35A and F-35B are not meeting the full set of ORD reliability and maintainability requirements for mature aircraft. The F-35C, which reached the 50,000-hour milestone designated for maturity in 2QFY22, is meeting the ORD reliability requirements. No variant is meeting the maintainability requirements.

The tables below show reliability and maintainability performance compared to ORD requirements. For the reliability metrics, higher numbers reflect better performance (i.e., a more reliable system) and for maintainability metrics, lower numbers reflect better performance (i.e., less maintenance burden). Tables 2 and 3 show trends in the reliability and maintainability metrics, respectively, based on data aggregated in 3-month rolling windows, where monthly reports are generated based on the last 3 months of data. This process enables trends to be observed more clearly than reports generated by only a single month of data.

Table 2. F-35 Reliability Metrics Assessment as of April 30, 2022

Variant	Flight Hours for ORD or JCS Threshold	Cumulative Flight Hours	MFHBCF (hours)			MFHBR (hours)			MFHBME (hours)			MFHBF-DC (hours)		
			ORD Threshold	Change: Apr 2021 to Apr 2022	Meeting ORD Threshold	ORD Threshold	Change: Apr 2021 to Apr 2022	Meeting ORD Threshold	ORD Threshold	Change: Apr 2021 to Apr 2022	Meeting ORD Threshold	JCS Requirement	Change: Apr 2021 to Apr 2022	Meeting JCS Threshold
F-35A	75,000	246,843	20	↑	No	6.5	↑	Yes	2.0	↑	Yes	6.0	↑	Yes
F-35B	75,000	90,895	12	↓	No	6.0	↑	No	1.5	↑	Yes	4.0	↑	Yes
F-35C	50,000	54,920	14	↑	Yes	6.0	↑	Yes	1.5	↑	Yes	4.0	↓	Yes

Note:
Up arrow (↑) represents improving trend

Acronyms: JCS – Joint Capability Specification; MFHBCF – Mean Flight Hours Between Critical Failures; MFHBF-DC – Mean Flight Hours Between Failures-Design Controllable; MFHBME – Mean Flight Hours Between Maintenance Event; MFHBR – Mean Flight Hours Between Removal; ORD – Operational Requirements Document

Table 3. F-35 Maintainability Metrics Assessment as of April 30, 2022

Variant	Flight Hours for ORD Threshold	Cumulative Flight Hours	MCMTCF (hours)			MTTR (hours)		
			ORD Threshold	Change: Apr 2021 to Apr 2022	Meeting ORD Threshold	ORD Threshold	Change: Apr 2021 to Apr 2022	Meeting ORD Threshold
F-35A	75,000	246,843	4.0	↓	No	2.5	↓	No
F-35B	75,000	90,895	4.5	↓	No	3.0	↓	No
F-35C	50,000	54,920	4.0	↑	No	2.5	↑	No

Note:
Down arrow (↓) represents improving trend

Acronyms: MCMTCF – Mean Corrective Maintenance Time for Critical Failures; MTTR – Mean Time To Repair; ORD – Operational Requirements Document

ALIS and Operational Data Integrated Network (ODIN)

ALIS is a large, distributed information system that supports F-35 operations and maintenance, supply, and training. ALIS is composed of hardware and software components located at both the squadron level and enterprise level, and includes both government- and contractor-owned assets. In FY22, the program continued planned development efforts while transitioning from ALIS to ODIN, adding hardware to the field while migrating software. The first transition of hardware, from the ALIS Standard Operating Unit (SOU) to the ODIN Base Kit (OBK), reached selected field units during FY22, and the program has contracted for OBK delivery to all units by September 2023. To support eventual shipboard operations, the program recently completed shock and vibration testing of the OBK. The testing identified minor changes needed to meet U.S. Navy and Marine Corps requirements for shipboard installation. The transition for ALIS software to be hosted on ODIN hardware has been divided in to three pathways: architecture and environment, data, and ALIS applications.

The path to containerized ALIS, which will be the software bundle ported from the legacy ALIS hardware systems into the OBKs to formalize an ODIN software and hardware system, follows three steps. Step one, called 35P21.Q4, is the current release of ALIS software in testing. Testing of this version discovered a number of Category One (i.e., safety critical) deficiencies, resulting in significant changes to the software code and subsequent delays. Currently, 35P21.Q4 is preparing for flight test and is projected to be released to the fleet in November 2022. Step two, called 35P22.Q4, which is planned as the last software version to be used on ALIS hardware, was also delayed as resources were shifted to correct issues with the preceding release, and is now projected to be released in 4QFY23. A number of code infrastructure and cybersecurity updates are planned for this release to cover anticipated software obsolescence during the required software freeze period to perform containerization. Noteworthy in the 35P22.Q4 release, are planned improvements to transport layer protocols to better support maritime and forward deployed operations. The final step, containerization of ALIS, which was originally planned to enter flight test in July 2023, is now projected to enter flight test in June 2024. Between the release of 35P22.Q4 and the release of containerized ALIS, there are no plans to make any performance or capability improvements to ALIS, as changes mid-containerization would produce significant delays in the transformation process and potential errors in the software.

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. ALIS does not currently have the capability to automatically log these events in the Computerized Maintenance Management System (CMMS). While pilots can manually document instability events, this occurs infrequently as the process is cumbersome, and Service policy is to rely on an ALIS automated process. The data in CMMS are used to report reliability and maintainability metrics. However, because software instability issues are underreported, they are not reflected in the metrics. Currently, only proprietary tools used by contractor field service engineers can identify pilot-initiated reset events. DOT&E recommends, in order to improve F-35 aircraft mission systems stability, that ODIN include the capability to automatically document pilot-initiated resets of mission systems.

In April-May 2022, the U.S. Air Force conducted agile combat employment operations with the F-35A in Exercise Valiant Shield. This exercise highlighted the need for ALIS and ODIN to operate with limited data, or entirely disconnected at forward operating locations. While the Services are experimenting with distributed operations and limited data transfer in contested environments, DOT&E maintains the need to formally test and document F-35 aircraft operations and maintenance – for up to 30 days – with ALIS or ODIN disconnected from their supporting network infrastructure.

Survivability

No cybersecurity discrepancies were resolved during FY22 testing and a large number of cybersecurity deficiencies remain across the F-35 program. To address the discrepancies, the JPO invested in cyber mitigations associated with recent JOTT testing, and key test findings are being tracked to closure by the newly delegated Authorizing Official for ALIS and ODIN. Access to proprietary information for contractor cybersecurity testers impeded execution of several planned tests in FY22, requiring their rescheduling for FY23. The UOTT worked with the F-35 JPO and stakeholders across the DOD to identify relevant scenarios, qualified test personnel, and adequate resources for conducting cybersecurity testing on AV components and support systems.

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

In light of current cybersecurity threats and vulnerabilities, along with peer and near-peer threats to bases and communications, DOT&E continues to require the F-35 program and Services to conduct testing of aircraft operations without access to the ALIS SOU for extended periods of time, with an objective of demonstrating the SOU-specified 30 days of operations, which is also a suitability testing requirement. The program has yet to meet this requirement, and is currently in the planning stages for a test of the ALIS Contingency Operations Plan, which will test standardized procedures for lack-of-connectivity scenarios.

Emerging candidates for cybersecurity testing are the F-35 JSE and the activation of data ports on operational aircraft for use in downloading aircraft performance data. Further insights into priority testing will be forthcoming from a Mission-Based Cyber Risk Assessment commencing in 1QFY23.

RECOMMENDATIONS

The F-35 JPO and Services as appropriate should:

1. Complete the remaining VV&A of the JSE to enable timely completion of the required IOT&E trials.
2. Develop and begin executing plans for upgrading the JSE to support Block 4 OT requirements. These plans must include capability upgrades to the FIAB, blue and red weapons models, red ground threat models and improved environment characteristics.
3. In accordance with the DOT&E-approved Block 4 TEMP, Increment 1 approval memo:
   - Fully fund, develop, and update the detailed plan to modify all OT aircraft with the appropriate capabilities, life limit, and instrumentation, including OABS requirements;
   - Complete a 30-day demonstration of flight operations without ALIS connectivity; and
   - Align the components of the F-35 air system delivery framework for each increment of capability to allow enough time for adequate testing of the fully representative system that is planned to be fielded.
4. Reduce discovery of deficiencies in the field by continuing to address more findings from the 2021 software independent review team, and upgrading and increasing the capacity of hardware- and software-in-the-loop labs.
5. Continue to pursue maintenance system improvements, especially for common processes distributed among Non-Mission Capable Maintenance drivers, such as low observable repairs and adhesive cure times.
6. Improve spares posture, especially for F135 engines, to reduce down-time for aircraft waiting spare parts by developing alternate sources of repair, including organic repair.
7. Accomplish rigorous testing of data integrity while the transition from ALIS to ODIN continues, as this will be critical to the success of ALIS to ODIN while also supporting operational unit day-to-day activities.
8. Ensure both developmental and operational testing for ALIS and ODIN are adequately resourced to reduce the high risk associated with fielding an immature and inadequately tested replacement.
9. Conduct more in-depth cyber testing of the AV, ALIS/ODIN, US Reprogramming Lab, training systems, and eventually JSE; provide dedicated hardware- and software-in-the-loop cyber-test assets that can be used for the full extent of cyber testing.
10. Correct program-wide deficiencies identified during cybersecurity testing in a timely manner and verify corrections within ALIS prior to rehosting ALIS software on ODIN.
11. Develop and routinely report software sustainment and stability metrics that show how well the program's overall software development capability for the AV and logistics sustainment system is progressing.
12. Apply lessons learned from observations of the USS *Tripoli* deployment to refine F-35B Heavy ACE CONOPS. These include:
    - The Marine Corps should continue to refine the F-35B Heavy ACE CONOPS and determine the size and composition of an F-35B Heavy ACE for a LHA 6-class vessel based on its unique flight deck, hangar bay, and aviation support services configuration.
    - The UOTT should incorporate information learned from this detachment in future test planning processes to assess the effects of long-term ALIS-denied or -degraded conditions of up to 30 days, on the ability of a unit to generate sorties.

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

The Global Command and Control System - Joint (GCCS-J) family of systems includes Joint Operation Planning and Execution System (JOPES) and Joint Planning and Execution Services (JPES), among other command and control systems. While GCCS-J was reported as not operationally effective in the FY19 DOT&E Annual Report, GCCS-J has demonstrated some progress towards effectiveness in FY22 testing. In FY23, operational effectiveness and operational suitability will be evaluated during the GCCS-J v6.1 FOT&E. GCCS-J and JPES have adopted agile software development methods using development, security, and operations (DevSecOps) processes.

SYSTEM DESCRIPTION

GCCS-J is a software-based system with commercial off-the-shelf and government off-the-shelf software and hardware and is highly modular allowing the deployed configuration to be customized to fit each deployed sites' requirements. The GCCS-J system uses procedures, standards, and interfaces that provide an integrated, near real-time picture of the battlespace that is necessary to conduct joint and multi-national operations. The JPES Program Management Office (PMO) is continuing sustainment of the JOPES v4.5.0.0 until JPES can be deployed to all JOPES users.

MISSION

The GCCS-J family of systems enables Joint Commanders to accomplish command and control by:

- Linking the National Command Authority to the Joint Task Force, component commanders, and service-unique systems at lower levels of command;
- Displaying geographic track information integrated with available intelligence and environmental information to provide the user a fused battlespace picture;
- Providing integrated imagery and intelligence capabilities (e.g., battlespace views and other relevant intelligence) into the common operational picture;
- Providing a missile warning and tracking capability;
- Translating policy decisions into operations plans that meet U.S. requirements to employ military forces;
- Supporting force deployment; and
- Conducting contingency and crisis action planning.

PROGRAM

The GCCS-J PMO intends to field version v6.1.0.0 as an upgrade to the fielded version of v6.0.1 in FY23. The JPES PMO intends to continue development and conduct user assessments to ensure all necessary functionality meets or exceeds that of JOPES, which JPES is replacing. GCCS-J and JPES are implementing the DevSecOps process as part of their agile software development framework.

» MAJOR CONTRACTORS

GCCS-J:

- Northrop Grumman Systems Corporation – San Diego, California
- NextGen Federal Systems – Annapolis Junction, Maryland

JPES/JOPES:

- InterImage Inc. – Arlington, Virginia
- ERP International, LLC – Laurel, MD
- NextGen Federal Systems – Morgantown, WV
- CompQSoft – Leesburg, VA

TEST ADEQUACY

In FY22, the Joint Interoperability Test Command (JITC) conducted two user assessments (UAs) for GCCS-J, two UAs for JPES, and one operational assessment for JOPES, in accordance with DOT&E policy. The GCCS-J and JPES integrated test environments do not currently capture the mission configurations associated with each Combatant Command and other critical sites. GCCS-J and JPES test strategies need to be developed to encompass the agile nature and varying operational site requirements to inform the Test and Evaluation Master Plans (TEMPs) and the Agile Operational Master Test Plans. Additionally, TEMP updates for the GCCS-J and JPES programs should detail operational cyber survivability tests that include cooperative vulnerability and penetration assessments followed by adversarial assessments.

PERFORMANCE

» EFFECTIVENESS

In FY19, DOT&E reported that the GCCS-J v6.0.1.0 FOT&E demonstrated that the system was not operationally effective. Based upon the PMO-conducted integration testing and JITC-conducted UAs in FY22, GCCS-J has demonstrated some progress towards effectiveness. In FY23, operational effectiveness will be evaluated during the GCCS-J v6.1 FOT&E.

JOPES v4.5.0.0 remains operationally effective. JOPES v4.5.0.0 resolved potential end-of-life concerns due to delays in the deployment of JPES.

» SUITABILITY

In FY19, DOT&E reported that the GCCS-J v6.0.1.0 FOT&E demonstrated that the system was not operationally suitable. During UAs of GCCS-J v6.0.1.x releases, users have reported some improvement in operational suitability. Due to the lack of operational representativeness in the DT environment, suitability will be evaluated during the FY23 GCCS-J v6.1 FOT&E. JOPES v4.5.0.0 remains operationally suitable.

» SURVIVABILITY

In FY19, DOT&E recommended that cyber survivability testing of GCCS-J v6.0.1.0 should be conducted in accordance with DOT&E cyber survivability policy. Due to delays in the delivery of GCCS-J v6.0.1, operational cyber survivability testing has yet to be conducted. JITC conducted developmental cyber testing of JOPES v4.5.0.0in FY22.

RECOMMENDATIONS

DISA should:

1. Improve the operational realism, and verify and validate the operational representativeness of the GCCS-J and JPES integrated test environments to ensure testing more closely reflects the diversity of deployment configurations in the operational environment.
2. Revise Agile Operational Master Test Plans and TEMPs for GCCS-J and JPES to reflect agile software development methods, the varied operational site requirements, and operational cyber survivability testing.

Joint Biological Tactical Detection System (JBTDS)

The Joint Biological Tactical Detection System (JBTDS) Engineering Manufacturing and Development phase testing in the DOT&E-approved Milestone B Test and Evaluation Master Plan (TEMP) is complete. Test results identified system-to-system variability in detection sensitivity attributed to degraded internal pump performance. The JBTDS collector functioned as intended and testing of the identifier demonstrated acceptable performance for most of the targets. The Program Office is working with the vendor to improve performance of the identifier assay for the remaining targets. Vendor-conducted testing of the new assays appear promising. The Program Office is working with the test community to identify and plan regression testing to verify performance improvements. The planned 4QFY22 Milestone C decision has been delayed.

SYSTEM DESCRIPTION

The JBTDS consists of an integrated man-portable biological warfare (BW) agent detector and sample collector, a base station, a meteorological station, a GPS receiver, a sample extraction kit, and a handheld BW agent 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

In a biological threat environment, the Army, Navy, and Marine Corps units equipped with the JBTDS will conduct biological surveillance missions to detect the presence of, warn against, collect samples of, and provide identification of biological agents to support force protection decisions, enable medical planning, and manage consequences.

PROGRAM

The JBTDS is a joint Service Acquisition Category II program. DOT&E approved a revision to the Milestone B TEMP in November 2020. The Test and Evaluation Integrated Product Team is updating the TEMP to address regression testing. Planned Milestone C and IOT&E are expected to slip.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

The JBTDS program conducted a shipboard operational assessment in December 2021 and completed the planned Engineering Manufacturing and Development phase integrated developmental/operational live agent chamber testing in March 2022, in accordance with the DOT&E-approved test plan. DOT&E did not observe live agent testing due to safety restrictions. Performance data from agent chamber testing was used as input for operational scenario modeling and simulation to assess the operational contribution of the JBTDS to reducing casualties resulting from a BW agent attack. The Program Office conducted false detection and identification testing in industrial, agricultural, urban, and maritime environments. Detectors were operated for 6,739 hours and 638 samples were analyzed by the JBTDS identifier. Testing was adequate to support an assessment of the current operational performance, suitability, and survivability of the JBTDS.

PERFORMANCE

» EFFECTIVENESS

During BW integrated chamber testing, the JBTDS was able to detect 60 percent of agent preparations tested at required levels. The identifier met the operational requirements for 70 percent of biological agents. The presence of battlefield interferents significantly impacted detector performance. Over the course of chamber testing, JBTDS performance degraded and system-to-system performance varied significantly. Demonstrated sample extraction efficiency was less than 25 percent for the agents tested. The Program Office is working with the vendor to identify and implement corrective actions.

Initial modeling and simulation using Service concepts of operation and test data indicates that JBTDS contributes to mitigating the effects of a BW attack. The time between an attack, detection of the attack, operational decisions to increase the force protective posture, the collection of a sample and identification of a BW agent and the use of prophylaxis to reduce casualties impacts the ability to reduce casualties.

» SUITABILITY

JBTDS demonstrated variable system-to-system detection sensitivity during BW testing caused by performance degradation of the system’s internal pump. The system’s built-in test capability did not alert the operator to the degraded pump performance. The vendor’s investigation revealed that the JBTDS application for the pump requires operation outside its manufacturer’s specifications. Navy operators expressed safety concerns regarding plans to store and charge JBTDS batteries aboard ships. The JBTDS tripod legs experienced failures after repeated set-up, stowage, and after ship shock testing. JBTDS consumables packaging resulted in the generation of burdensome waste that must be collected, stored, and disposed of in an operational environment. To date, JBTDS has not demonstrated operational suitability.

» SURVIVABILITY

The cooperative vulnerability and penetration assessment and adversarial assessment identified several vulnerabilities in a cyber-contested environment.

Test units were not able to distinguish cyberattacks from simulated biological attacks during the operational assessment. Electromagnetic interference, ship shock and vibration developmental testing resulted in JBTDS failures that need to be resolved. An electronic warfare developmental test revealed vulnerabilities in the JBTDS mesh sensor network to various threats that disrupt the ability to remotely monitor the sensor network.

RECOMMENDATIONS

The Program Office should:

1. Add built-in-test capability to alert the system operator to component failures that would negatively impact detection and sample collection performance.
2. Replace the detector collector pump to improve system performance and reliability.
3. Improve the identifier assays to meet performance requirements.
4. Address cybersecurity deficiencies to protect against cyberattacks.
5. Redesign the JBTDS legs to improve suitability and survivability aboard Navy ships.
6. Develop training to troubleshoot network issues and identify potential cyber and electronic warfare attacks to improve cyber survivability.

Joint Cyber Warfighting Architecture (JCWA)

The Joint Cyber Warfighting Architecture (JCWA) concept continues to mature; however, no dedicated JCWA-level operational test and evaluation (OT&E) is currently planned or resourced, despite aggressive efforts to field critical components of the architecture. This will limit the Department's ability to understand the impact of current and future capability integration on JCWA's operational effectiveness, suitability, or survivability.

SYSTEM DESCRIPTION

JCWA is designed to collect, fuse, and process data and intelligence in order to provide situational awareness and battle management at the strategic, operational, and tactical levels while also enabling access to a suite of cyber capabilities needed to rehearse and then act in cyberspace.

MISSION

U.S. Cyber Command (USCYBERCOM) intends to use JCWA to support all cyberspace operations, training, tool development, data analytics, and coordinated intelligence functions.

PROGRAM

JCWA is not a program of record itself but currently encompasses the following four acquisition programs:

- Unified Platform will act as a data hub for JCWA, unifying disparate cyber capabilities in order to enable full-spectrum cyberspace operations.

- Joint Cyber Command and Control will provide situational awareness, battle management, and cyber forces' management for full-spectrum cyber operations.
- Persistent Cyber Training Environment will provide individual and collective training as well as mission rehearsal for cyber operations.
- An access component will provide additional capability for cyber operations.

USCYBERCOM relies heavily on the Services for acquisition of the programs that comprise JCWA. To guide these individual acquisition programs, USCYBERCOM initially established the JCWA Integration Office and the JCWA Capabilities Management Office, but in FY22 merged the two offices under one principal staff advisor for efficiencies. The resulting entity from the merge continues to lack the authority and resources to effectively manage critical JCWA-level activities. Each program has its own release and deployment schedules, and there are no validated JCWA level mission thread requirements or plans for an integrated JCWA-level operational test. Three out of the four current JCWA programs leverage the software acquisition pathway and require annual value assessments that determine if capabilities delivered have been worth the investment. USCYBERCOM has yet to leverage OT&E as a data source for these annual value assessments.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

JCWA programs continue to develop T&E strategies independent of the JCWA construct. In FY22, the Service-led programs continued to conduct program-level T&E, including early cybersecurity assessments. DOT&E has informed and monitored testing conducted to date and will use the data in operational assessments where appropriate.

As the JCWA concept continues to mature, the scope of OT&E required to support cyber warfighting efforts will need to continuously evolve so that it addresses the entire architecture and the dynamic, operational environment within which it operates.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Not enough data have yet been collected to enable a preliminary assessment of the JCWA-level operational effectiveness and suitability, or the performance of its individual components.

» SURVIVABILITY

Not enough data have yet been collected to enable an evaluation of JCWA mission resilience in a cyber-contested environment.

RECOMMENDATIONS

USCYBERCOM should:

1. Immediately resource and empower the Joint Interoperability Test Command to plan, conduct, and assess integrated, JCWA-level OT&E.
2. Require OT&E to inform the JCWA value assessments.
3. Establish a cadence of test for dedicated OT&E, beginning in FY23, to understand how the capability afforded by JCWA is evolving over time and to ensure it is an effective, suitable, and survivable enabler of cyber operations.
4. Define and resource the test infrastructure required to successfully support JCWA integration, as well as T&E to support key decision points, user acceptance, and value assessments.

Key Management Infrastructure (KMI)

The Key Management Infrastructure (KMI) Program Management Office (PMO) began Increment 3 capability development in July 2021. The KMI PMO announced a 6-month schedule delay for Increment 3 in April 2022, due to hardware technical refresh supply chain and configuration problems.

SYSTEM DESCRIPTION

KMI replaces the legacy Electronic Key Management System (EKMS) to provide a means for securely ordering, generating, producing, distributing, managing, and auditing cryptographic products, to include encryption keys, cryptographic applications, and account management tools. KMI consists of core nodes that provide web operations at sites operated by the National Security Agency (NSA), as well as individual client nodes distributed globally, to enable secure key and software provisioning services for the DOD, the Intelligence Community, and other Federal agencies. The KMI Increment 3 delivery will enhance the deployed KMI Increment 2 capabilities with substantial custom software development and commercial off the-shelf computer components, which include a client host computer with monitor and peripherals, printer, and barcode scanner.

MISSION

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

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

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

PROGRAM

The NSA is delivering KMI Increment 3 in eight planned Agile releases that will enhance existing capabilities and subsume EKMS Tier 0 and Tier 1 cryptographic product delivery into the infrastructure. The KMI PMO began Increment 3 capability development in July 2021. The KMI PMO announced a 6-month schedule delay for Increment 3 in April 2022, due to hardware technical refresh supply chain delivery delays and system configuration problems.

» MAJOR CONTRACTORS

- Leidos – Columbia, Maryland (Prime)
- SafeNet – Belcamp, Maryland

TEST ADEQUACY

DOT&E approved the KMI Increment 3 Test and Evaluation Master Plan in August 2020 that defines an adequate operational test strategy for the KMI program release testing through IOT&E scheduled for late FY25. The Joint Interoperability Test Command (JITC) KMI test team will employ a multi-release test plan that can cover up to four releases over two years; however, the KMI PMO and JITC have yet to conduct any Increment 3 operational testing due to schedule delays. JITC is developing an operational test plan in early FY23 to support early KMI Increment 3 release testing that will commence in FY23.

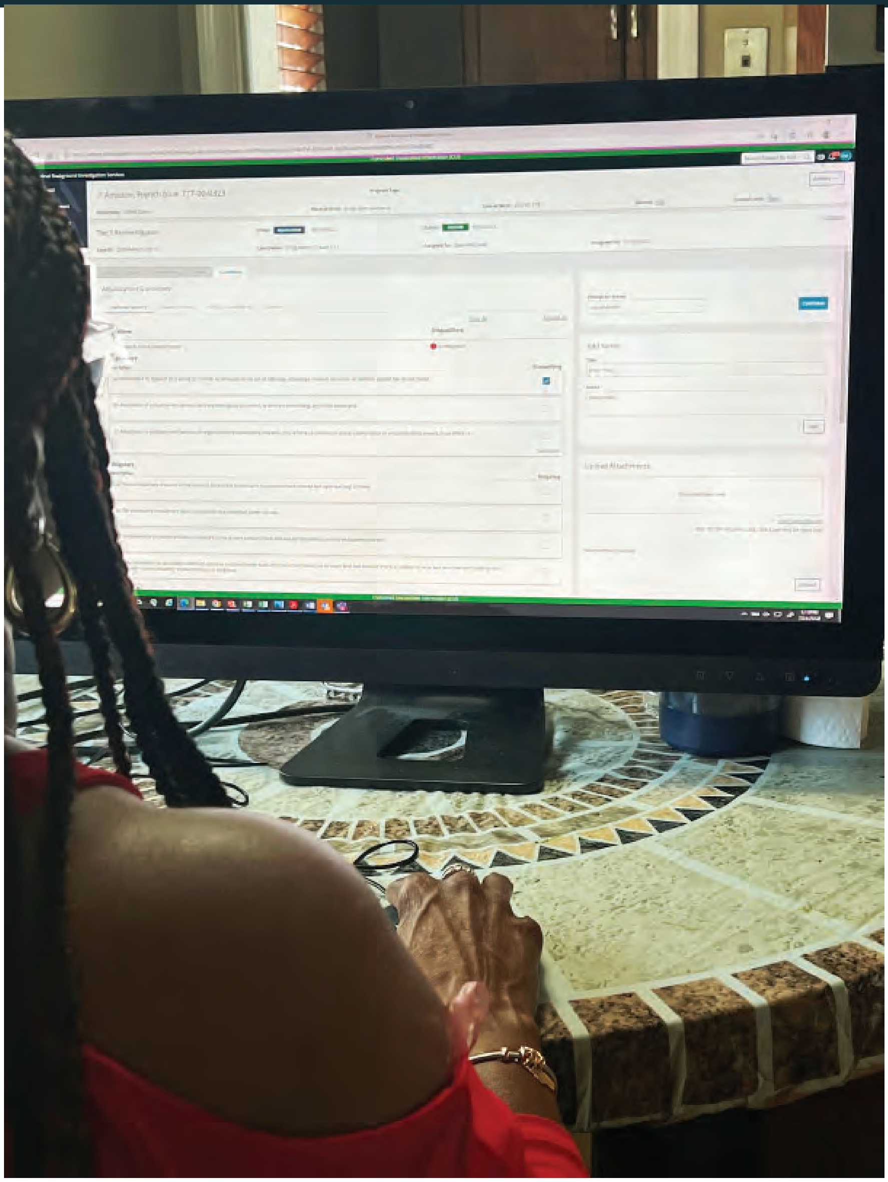
PERFORMANCE

A preliminary performance assessment will be available after the completion of the early KMI Increment 3 release testing in May 2023. The current KMI Increment 3 schedule includes concurrent test planning, execution, and reporting, which adds risk to the program. In addition, while the KMI Test Infrastructure provides a safe laboratory for evaluating KMI software builds, it is currently not maintained in the same configuration as the operational KMI. This may limit the KMI Test Infrastructure users' ability to identify problems prior to deploying a new KMI release to the operational system; however, the PMO intends to refresh the KMI Test Infrastructure and the production system to be the same in Increment 3.

RECOMMENDATIONS

1. The KMI PMO should reassess the release cadence to reduce delivery and test concurrency to make the schedule more achievable.
2. The NSA should maintain the KMI Test Infrastructure configuration to be the same as the operational environment.

National Background Investigation Services (NBIS)



The National Background Investigation Services (NBIS) integrates Agile development methodologies with flexible testing and validation processes to provide near continuous evaluation of an emerging system. The NBIS program places a strong emphasis on data security design and testing.

SYSTEM DESCRIPTION

NBIS is a cloud-based system-of-systems that will function as a single-source information technology solution for all tasks associated with end-to-end personnel security vetting and continuous reviews. NBIS includes legacy and newly developed applications in a common architecture to support data gathering, storage, and management of data associated with personnel background investigations in a secure and protected environment. NBIS will replace previously compromised legacy systems.

MISSION

The Defense Counterintelligence and Security Agency (DCSA), other Federal agencies, and industry partners will use NBIS to authorize and support conduct of background investigations for new applicants as well as incumbent government, military, and contract personnel. NBIS provides automation and support to allow agencies to initiate clearance requests, to enable candidates to complete background investigation forms, to gather public data concerning personnel applying, and to manage the findings of an investigation. The system also supports adjudication of clearances as well as continued vetting of cleared personnel.

PROGRAM

NBIS transitioned to the Software Acquisition Pathway in 2021 and uses Scaled Agile Framework (SAFe) and Development Security Operations methodologies. The DCSA assumed operational control for NBIS from Defense Information Systems Agency (DISA) in October 2020, and is deploying NBIS in multiple releases of increasing capability while building upon and replacing legacy systems, which will be decommissioned through 2023. The program has employed SAFe methodologies to rapidly develop and field capabilities in collaboration with the testers and intended customer/user base. Early releases to a limited and restricted user base supported continuous developmental testing and a cumulative validation of system and data security. In March 2022, DOT&E placed NBIS on oversight due to program size, complexity, and importance to DOD operations.

» MAJOR CONTRACTORS

- Peraton – Herndon, Virginia and Basking Ridge, New Jersey (major software developer)
- Salient Systems – Austin, Texas (security support)
- Soleil LLC – Vienna, Virginia (sustainment support)
- Accenture Federal Services – Arlington, Virginia (system onboarding to Federal agencies)
- Alion Science and Technology Corp – McLean, Virginia (user training)
- Lockheed Martin Corp, Deloitte, Kapili Services, and Perspecta Enterprise Solutions LLC (contractor support)

TEST ADEQUACY

The Joint Interoperability Test Center (JITC) is conducting both developmental and operational testing of this program. An updated Test and Evaluation Strategy (TES) for NBIS is currently in review and staffing with DOT&E. Current NBIS testing is adequate to resolve the critical operational issues, and includes several innovations in both automated and continuous testing of systems using Agile and other rapid development approaches. JITC has conducted or overseen multiple rounds of government acceptance, user acceptance, and limited user tests in 2022 using a previously prepared TES. DOT&E will capture lessons learned from the development of these testing capabilities, which may be of use in other Agile program tests.

PERFORMANCE

The program is incrementally building functionality and testing at each iteration and release. All tests to date have resulted in rapid correction of findings either during the test event or immediately thereafter.

» EFFECTIVENESS

Evaluation of the five specific mission areas include Initiation/Review/Authorize, Investigation, Adjudication/Appeals, Continuous Vetting, and Subject Management. Each are in a different stage and an effectiveness determination is in progress. No major findings from prior tests remain open.

» SUITABILITY

Determination of suitability is in progress with an expanding user base via operational tests and table top reviews to include help desk and user training. The program continues to meet or exceed system latency, loading, and simultaneous use goals.

» SURVIVABILITY

The system has no major unresolved cyber survivability findings. JITC has conducted four rounds of operational cyber testing. Findings are rapidly corrected and the emerging system continues to implement new security capabilities.

RECOMMENDATIONS

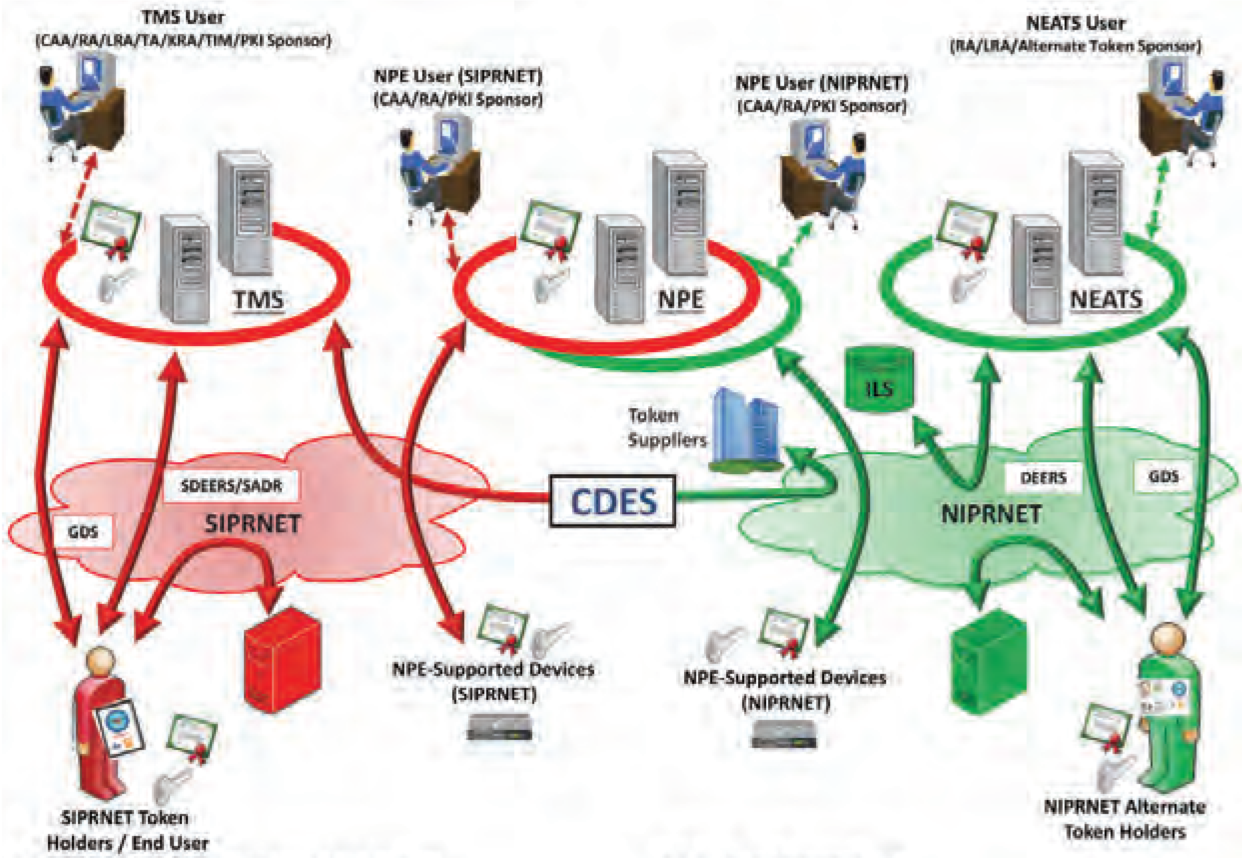
None.

Public Key Infrastructure (PKI) Increment 2

The DOD Public Key Infrastructure (PKI) Increment 2 is operationally effective, demonstrating the capability to facilitate secure electronic information exchanges between DOD users and network devices. PKI's Token Management System (TMS) is not operationally suitable due to significant problems with SIPRNET token-ordering processes and accountability based on DOT&E's PKI Increment 2 FOT&E Report published in November 2021. The NIPRNET Enterprise Alternate Token System (NEATS) and the Non-Person Entity (NPE) system are not survivable against moderate cyber threats.

SYSTEM DESCRIPTION

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



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

MISSION

DOD users at all levels use DOD PKI to provide authenticated identity management via personal identification number-protected Common Access Cards, SIPRNET or NEATS tokens to enable DOD members, coalition partners, and other authorized users to access restricted websites, enroll in online services, and encrypt/decrypt and digitally sign email. Military Service and DOD Agency operators, communities of interest, and other authorized users use DOD PKI to securely access, process, store, transport, and use information, applications, and networks. Network operators use NPE certificates for workstations, web servers, and devices to create secure network domains, which facilitate intrusion protection and detection.

PROGRAM

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

Annex in November 2020. DOT&E published the PKI Increment 2 FOT&E Report in November 2021 and a classified NPE finding memo in February 2022.

» MAJOR CONTRACTORS

- General Dynamics Mission Systems – Dedham, Massachusetts (Prime for TMS and NPE)
- Peraton – Herndon, Virginia (Prime for NEATS)
- SafeNet Assured Technologies – Abingdon, Maryland
- Giesecke and Devrient America – Twinsburg, Ohio

TEST ADEQUACY

The Joint Interoperability Test Command (JITC) conducted the PKI Increment 2 FOT&E from late November 2020 through March 2021, in accordance with a DOT&E-approved test plan. Testing was adequate to verify system fixes and assess operational effectiveness and suitability of PKI capabilities for long-term sustainment and transition. JITC conducted FOT&E follow-up re-testing and verifications of fixes in late FY22, which were observed by DOT&E. JITC intends to continue cyber survivability testing and verifications of the DOD PKI Increment 2 NEATS and NPE in FY23 in support of a yet-to-be-determined date for a full deployment decision.

PERFORMANCE

» EFFECTIVENESS

NEATS, NPE, and TMS are operationally effective, with minor problems that the PKI Program Management Office (PMO) is working to remedy. JITC conducted verification of fixes for some PKI capabilities in late FY22 and will continue verifications as needed in FY23. The NPE auto-rekey functionality on devices using the Enrollment over Secure Transport (EST) protocol remained not operationally effective and has not been widely adopted as an enterprise capability. JITC has no plans to re-test the EST protocol at this time.

» SUITABILITY

NEATS and NPE are operationally suitable, though the DMDC NEATS help desk responsiveness is not satisfactory. TMS is not operationally suitable because the Central Management of Tokens system and processes resulted in a lack of token accountability. In June 2022, the PKI PMO introduced a PKI DISA Integration Lab (DIL) designed to test new token variants and device certificates with remote access to better support user needs. JITC reassessed TMS operational suitability, observed token ordering processes, and monitored NEATS help desk metrics from late FY22 into early FY23. The PKI PMO updated the lifecycle sustainment plan and transition plan in FY22. TMS capabilities were not ready for long-term sustainment and transition in FY22.

» SURVIVABILITY

TMS is survivable, while NPE and NEATS are not survivable against moderate capability nearsider and advanced capability outsider threats. In July 2021, JITC conducted TMS and NPE cyber survivability testing and then conducted focused NPE cyber survivability testing in October 2021 that identified problems. The PKI PMO partially mitigated the NPE problems in FY22, and JITC re-tested NPE in late FY22 into FY23. The PKI PMO and DMDC are working to mitigate NEATS and other architectural problems found in earlier cyber survivability testing, after which JITC will test NEATS in FY23. The PKI PMO and DMDC token supply chain risk management processes lack transparency and need improved monitoring of token manufacturer processes.

RECOMMENDATIONS

1. The PKI PMO and DMDC should establish a reproducible and accurate token ordering and accountability process for PKI tokens.
2. The PKI PMO, NSA Acquisition Security Office, and DMDC should improve their token supply chain risk management processes to inform Service and DOD Agency token purchasing and operational use decisions.

3. The PKI PMO and DISA should remediate and test the identified NPE vulnerabilities found during cyber survivability assessments in 2021 and 2022 to secure this system.
4. The PKI PMO and DMDC should remediate and test the identified NEATS vulnerabilities found during cyber survivability assessments over the past four years to secure this system and supporting environment.
5. The PKI PMO and JITC should conduct operational cyber survivability assessments of NPE and NEATS prior to full deployment.
6. The PKI PMO, DMDC, and DISA should correct long-term sustainment problems prior to full deployment.
7. The PKI PMO and DMDC should improve NEATS help desk support.
8. The NSA should determine the path forward for the EST capability.

DEPARTMENT OF THE ARMY PROGRAMS

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

The Army completed Live Fire testing. The low-rate initial production round did not fully pass the First Article Acceptance Test. The Army is conducting an investigation to determine the cause of the failure. The Full-Rate Production decision has been delayed.

SYSTEM DESCRIPTION

The M1147 120mm Advanced Multi-Purpose (AMP) cartridge is a line of sight, full-bore multipurpose munition employed by Abrams tanks. The AMP cartridge consolidates the capabilities of four cartridges: the M830 High Explosive Anti-Tank cartridge, M830A1 Multi-Purpose AntiTank cartridge, M1028 Canister cartridge, and M908 Obstacle Reduction cartridge, into one cartridge. The AMP cartridge is intended to add new capabilities for breaching walls and against dismounted Anti-Tank Guided Missile (ATGM) teams at extended ranges.

MISSION

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

PROGRAM

The 120mm AMP cartridge is an Acquisition Category III program. The program entered Milestone C in December 2020. DOT&E approved the M1147 120mm AMP Test and Evaluation Master Plan, to include the LFT&E Strategy, in December 2020, and the IOT&E plan in August 2021. The Joint Program Executive Office Armaments and Ammunition expects to make a Full-Rate Production decision after completing the First Article Acceptance Test.

» MAJOR CONTRACTOR

- Northrop Grumman Defense Systems – Plymouth, Minnesota

TEST ADEQUACY

The Army completed explosive reactive armor demonstration shots at Aberdeen Proving Grounds, Maryland, in accordance with DOT&E-approved test plans. DOT&E did not observe the demonstration shots. DOT&E had access to all data and video from the shots.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E will provide its assessment of M1147 120mm AMP operational effectiveness, suitability, and survivability in a combined classified report for IOT&E and LFT&E after the program demonstrates airburst reliability requirement has been met.

Test of AMP cartridge at Yuma Proving Grounds, Arizona, September 2021

RECOMMENDATIONS

Recommendations for the M1147 120mm AMP cartridge will be detailed in a combined classified report for IOT&E and LFT&E in 1QFY23.

Abrams M1A2 System Enhancement Package version 4 (SEPv4) Tank

The Abrams M1A2 System Enhancement Package version 4 (SEPv4) is an incremental upgrade to the Abrams M1A2 SEPv3. The Army intends for the Abrams SEPv4 to improve lethality and survivability, primarily by integrating technologies to the platform's optics and fire control system to maximize the effectiveness of the M1147 Advanced Multi-Purpose Round. The Army is writing the Abrams SEPv4 Test and Evaluation Master Plan which they intend to submit to DOT&E for approval in 2QFY23. A materiel release decision is planned for 1QFY26.

SYSTEM DESCRIPTION

The Abrams M1A2 SEPv4 is an upgrade to the Abrams M1A2 SEPv3 to improve lethality. The Army intends to begin fielding the Abrams M1A2 SEPv4 in 3QFY28. The upgrades include:

- An improved gunner's primary sight (GPS) with 3rd Generation Forward Looking Infrared (3GEN FLIR), an improved laser range finder (LRF), and color day camera
- An improved Commander's Primary Sight with 3GEN FLIR, a LRF with laser pointer, and color day camera
- Improved lethality by providing the ability for the fire control system to digitally communicate with the new M1147 Advanced Multi-Purpose round
- Improved firing accuracy through the installation of a meteorological sensor
- Improved onboard diagnostics
- Improved thermal management system
- Improved laser warning receiver system

MISSION

Commanders employ the Abrams M1A2 SEPv4 tank to close with the enemy by means of fire and maneuver to defeat enemy forces.

PROGRAM

The Abrams M1A2 is an Acquisition Category IC program. The Army is incrementally upgrading the tank design through engineering change proposals. The current SEPv4 is known as the lethality upgrade. The Program Executive Office for Ground Combat Systems is the Decision Authority for the Abrams SEPv4 program. A materiel release is scheduled for 1QFY26. DOT&E will publish a FOT&E report upon conclusion of operational and live fire testing.

» MAJOR CONTRACTOR

- General Dynamics Land Systems – Sterling Heights, Michigan

TEST ADEQUACY

The Army is writing the Abrams SEPv4 Test and Evaluation Master Plan which they intend to submit to DOT&E for approval in 2QFY23. Operational testing will assess the operational effectiveness, suitability, and survivability of the Abrams SEPv4 equipped unit. The LFT&E program includes Full-Up System-Level testing, exploitation testing, Controlled Damage Experiments, and Modeling and Simulation (M&S). The Army is planning to begin integrated testing on the 3GEN FLIR in 1QFY23, with the remainder of DT beginning in 3QFY23.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Operational testing will assess the operational effectiveness, suitability, and survivability of the Abrams SEPv4 equipped unit in 2QFY25.

RECOMMENDATIONS

The Army should:

1. Adequately scope live fire and operational testing to be able to assess effectiveness, suitability and survivability.

Active Protection System (APS) for Abrams and Bradley

The Army tested the TROPHY Active Protection System (APS) installed on Abrams M1A2 System Enhancement Package version 3 (SEPv3) tanks in FY22 to inform an urgent materiel release (UMR). The TROPHY APS intercepted most of the incoming threats and the Abrams tank base armor provided adequate force protection.

The Army tested the Elbit Iron Fist – Light Decoupled (IFLD) APS installed on Bradley A4 from 2QFY22 to 4QFY22 to inform the UMR planned for FY26, pending funding. Performance has improved since Phase I in 2018. IFLD continues to face effectiveness deficiencies. The Army is working to address these deficiencies and intends to repeat some of the testing to verify the fixes.

SYSTEM DESCRIPTION

The TROPHY and IFLD APS include hard-kill systems designed to detect, identify, track, and destroy incoming enemy threats causing its early detonation, or divert the enemy threat. The TROPHY APS adds approximately 5,000 pounds to the Abrams SEPv3. The IFLD APS adds approximately 1,780 pounds to the Bradley. The Army has prepositioned TROPHY APS kits for installation on Abrams SEPv2 and SEPv3 tanks. The Army intends to have prepositioned IFLD kits for installation on Bradley A4.

MISSION

Army units use TROPHY APS-equipped Abrams main battle tanks to disrupt/destroy certain classes of enemy fire while safely maneuvering across a full range of military operations.

Army units use Bradley vehicles equipped with the Iron Fist APS to provide protected transport of soldiers and provide over-watching fires to support dismounted infantry in order to disrupt/destroy enemy military forces and control land areas.

PROGRAM

The Army has procured TROPHY and fulfilled two directed requirements signed in October 2016 and March 2018.

The Army is procuring IFLD APS under the directed requirement signed in October 2016. The Army intends to field one Armored Brigade Combat Team with 138 Bradley A4 Fighting Vehicles (125 M2A4s and 13 M7A4s) equipped with IFLD. The UMR decision is planned for FY26, pending funding.

» MAJOR CONTRACTORS

TROPHY APS

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

Iron Fist – Light Decoupled APS

- BAE – San Jose, California
- GD-OTS – Williston, Vermont
- Elbit Land Systems – Ramat Hasharon, Israel

TEST ADEQUACY

TROPHY APS

The Army conducted TROPHY APS Phase III testing with Abrams SEPv3 tanks in FY22 at Army Test Centers in accordance with DOT&E-approved test plans, and observed by DOT&E. Testing was adequate to assess operational effectiveness and survivability. The test scope focused on verifying performance envelope and capability demonstrated with Abrams SEPv3 tanks equipped with APS. Testing included 39 live fire tests with inert and live threats fired against a fully functional Abrams SEPv3 tank. Some of the scenarios included operationally stressing conditions (i.e., background clutter, concrete walls, vehicle elevation, gunfire, nearby vehicles, and turning turrets). Test results will inform an update to the DOT&E classified report initially published in June 2020.

Iron Fist – Light Decoupled APS

The Army completed Phase I Iron Fist APS testing on Bradley A4s in FY18. Poor performance led to a significant redesign of the system prior to entering Phase II.

The Army conducted Phase II effectiveness and survivability testing from February through September 2022 in accordance with the DOT&E-approved test plan, and observed by DOT&E. Testing involved firing operationally realistic live and inert threats at Bradley A4s equipped with IFLD. The focus of effectiveness testing was on evaluating performance of the optics and radar systems to detect, track, and intercept incoming threats in realistic operational conditions to include rain, mud, and urban clutter. Survivability testing focused on identifying vulnerabilities to the Bradley A4 vehicles after countermeasure intercept with live threats. The Army conducted a Soldier Touch Point (STP) in September 2022 at Aberdeen Test Center to gain critical insights. DOT&E was part of the team that developed the objectives. DOT&E did not approve the STP developmental test plan, as DOT&E was not assessing the IFLD in the STP. DOT&E did observe the STP. Numerous programming and calibration changes made to IFLD during testing prohibit DOT&E from making an effectiveness, suitability, and survivability assessment on production representative systems. The Army intends to repeat Phase II effectiveness and survivability testing with production representative systems prior to the Limited User Test in FY25. This testing will leverage Phase II effectiveness and survivability testing where appropriate.

PERFORMANCE

» EFFECTIVENESS

TROPHY APS

TROPHY APS effectively detects, identifies, tracks, and intercepts most of the incoming threats in basic range conditions and engagements. The system, as installed on SEPv3, demonstrated similar capabilities and deficiencies as the system installed on SEPv2. Final assessment of the performance of the TROPHY APS-equipped Abrams SEPv3 tank will be detailed in a 2QFY23 classified report.

Iron Fist – Light Decoupled APS

IFLD APS has demonstrated improved performance to detect, identify, track, and intercept incoming threats in basic range conditions and engagements over Phase I results. IFLD continues to face effectiveness deficiencies. The IFLD system tested in Phase II was not production representative due to numerous software and calibration changes made by the contractor during effectiveness testing. Details on the effectiveness deficiencies identified in Phase II will be in DOT&E's classified report planned for FY25 after completion of Phase III testing.

» SUITABILITY

Iron Fist – Light Decoupled APS

Senior non-commissioned officers participating in the STP provided suggestions to improve effectiveness and the human-machine interface to the evaluators and program. The Bradley Commander should have the means to select and place protection zones in a standby mode as they load and unload dismount soldiers. The IFLD APS should provide alerts to the crew on near misses to allow the crew to target the threat.

» SURVIVABILITY

TROPHY APS

The survivability of the TROPHY APS-equipped Abrams SEPv3 tank is proportional to the operational effectiveness of the TROPHY APS to search, detect, identify, track, and intercept the incoming threats. Survivability is dependent on the capability of the Abrams base armor to absorb the threat by-products' impacts generated after a successful intercept. The Abrams SEPv2 and v3 base armor configurations provide adequate force protection against the threat and countermeasure debris generated by a successful intercept.

Iron Fist – Light Decoupled APS

The Army completed Phase II survivability tests of live threats against Bradley equipped with Iron Fist in August 2022. Bradley's lighter main armor (compared to Abrams) will require a more efficient APS intercept capability than TROPHY in order to prevent residual threat penetration of the Bradley hull. The survivability analysis to include results of modeling and simulation is ongoing. DOT&E plans to write a survivability report in FY25, after completion of Phase III testing.

RECOMMENDATIONS

The Army should:

1. Repeat the Phase II IFLD APS effectiveness, and survivability tests after finalizing software changes to improve system effectiveness and survivability. This testing should leverage Phase II testing where appropriate.
2. Consider incorporating the senior non-commissioned officers' recommendations from the STP into the production representative Iron Fist – Light Decoupled.
3. Consider prior recommendations from the Abrams SEPv2 equipped with TROPHY APS DOT&E classified report published in June 2020.

Armored Multi-Purpose Vehicle (AMPV)

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

The Army completed Full-up System-Level (FUSL) live fire testing in May 2022 and conducted an IOT&E in July 2022. IOT&E and LFT&E data analyses are ongoing, precluding an evaluation in this article of the Armored Multi-Purpose Vehicle (AMPV) to meet operational effectiveness, suitability, and survivability requirements. The Army will use the IOT&E report and LFT&E classified survivability annex to support a Full-Rate Production decision by the Army Acquisition Executive in 2QFY23.

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, Mission Command, Medical Treatment, Medical Evacuation, and Mortar Carrier. The Army intends for the AMPV to replace the M113 Family of Vehicles and address shortcomings in survivability and force protection; size, weight, power, and cooling; and the ability to incorporate future technologies, such as the Army Network.

MISSION

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

PROGRAM

The AMPV is an Acquisition Category IC program. The Army conducted a Limited User Test in September 2018 to support a Low-Rate Production decision in January 2019. In January 2021, the Program Office rebaselined the program schedule due to production start-up issues at BAE and the impact of COVID-19 delaying the Full-Rate Production decision from 3QFY22 to 2QFY23. The Army conducted the IOT&E in July 2022. FUSL testing was completed in May 2022.

» MAJOR CONTRACTOR

- BAE Systems – York, Pennsylvania

TEST ADEQUACY

The Army conducted an IOT&E in July 2022 using units from an ABCT, which conducted tactical missions against a near-peer opposing force operating in an electronic warfare and cyber-contested environment. FUSL testing was conducted from May 2021 to May 2022. The Army executed 35 FUSL events using production-representative vehicles to evaluate system and crew vulnerability to kinetic threat engagements. The Army also tested the Automated Fire Extinguishing System in all variants. Operational and live fire testing was conducted in accordance with DOT&E-approved test plans, and was observed by DOT&E. The Army will use the IOT&E and LFT&E data to support a Full-Rate Production decision in 2QFY23. DOT&E will publish an IOT&E report with a classified survivability annex in support of the Full-Rate Production decision.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

The IOT&E and LFT&E data analyses are ongoing, precluding an evaluation of the AMPV's operational effectiveness, suitability, and survivability. Details will be provided in the IOT&E report and classified survivability annex to be published in support of a Full-Rate Production decision in 2QFY23.

RECOMMENDATION

The Army should:

1. Address the recommendations provided in the IOT&E report and classified survivability annex.

AMPV Test at Fort Greely, Alaska, December 2021

AMPV Test at U.S. Army Tropic Regions Test Center, Panama, April 2022

Army Integrated Air and Missile Defense (AIAMD)

In FY22, the Army split the Army Integrated Air and Missile Defense (AIAMD) program IOT&E into two phases. The Army Test and Evaluation Command (ATEC) conducted IOT&E Phase 1 from January through March 2022. ATEC started IOT&E Phase 2 in August 2022 and expects to complete testing in October 2022. DOT&E will publish a final assessment of AIAMD operational effectiveness, suitability, and survivability in a classified report to inform the Full-Rate Production decision in 2QFY23.

SYSTEM DESCRIPTION

AIAMD is a command and control system that integrates Engagement Operations Centers (EOC), Sentinel air-surveillance radars, and Patriot missile-system radars and launchers across an integrated fire control network (IFCN). EOCs provide the operating environment for soldiers to monitor and direct sensor employment and the engagement of air threats. Hardware interface kits connect adapted Patriot and Sentinel components to the IFCN, either through an EOC or through an IFCN Relay. IFCN Relays also provide mobile communications nodes to extend fire control connectivity and distributed operations.

MISSION

Air Defense Artillery forces will use the AIAMD system to provide the timely detection, identification, monitoring, and (if required) engagement of air threats in support of active defense of the homeland, critical assets and locations, and forces.

PROGRAM

AIAMD is an Acquisition Category ID program, developing hardware using the Major Capability Acquisition Pathway and conducting agile software development using the Software Acquisition Pathway. DOT&E approved the Milestone C Test and Evaluation Master Plan in April 2019 and the IOT&E test plan in October 2021. The Army intends to enter full-rate production in 2QFY23. The program will integrate new and existing sensors and weapons in a series of future increments.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

ATEC conducted a cybersecurity adversarial assessment (AA) from October through November 2021 at White Sands Missile Range, New Mexico, in accordance with the DOT&E-approved IOT&E test plan, and observed by DOT&E. The AA included both sustained live air and software/hardware-in-the-loop configurations, with electronic attack.

In January 2022, the Army split IOT&E into two phases due to known software deficiencies. ATEC completed IOT&E Phase 1 from January through March 2022 at White Sands Missile Range, New Mexico; including sustained live air; sustained software/hardware-in-the-loop with accredited modeling and simulation (M&S) tools; and two missile flight tests in accordance with the DOT&E-approved IOT&E test plan, and observed by DOT&E.

ATEC started IOT&E Phase 2 in August 2022 with an updated and re-accredited M&S environment, after the program used the agile software development process to make incremental improvements to mitigate known software deficiencies. ATEC expects to complete the Phase 2 in October 2022, including sustained live air, sustained software/hardware-in-the-loop, and a third missile flight test. Only data collected during IOT&E Phase 2 will be used to evaluate integrated defense effectiveness.

PERFORMANCE

» EFFECTIVENESS

The Army conducted IOT&E Phase 1 with system limitations caused by known software deficiencies and additional deficiencies were discovered during testing. The program used agile software development to modify the software to mitigate some of these limitations prior to the start of IOT&E Phase 2. DOT&E will provide a final assessment of system operational effectiveness, predominately using data collected during IOT&E Phase 2, in a classified report to inform the Full-Rate Production decision scheduled for 2QFY23.

» SUITABILITY

DOT&E will provide a final assessment of system operational suitability, using data from IOT&E

Phase 1 and 2, in a classified report to inform the Full-Rate Production decision scheduled for 2QFY23.

» SURVIVABILITY

DOT&E will provide a final assessment of system survivability, using cybersecurity data collected from the AA and the FY21 cooperative vulnerability and penetration assessment, in a classified report to inform the Full-Rate Production decision scheduled for 2QFY23.

RECOMMENDATION

The Army should:

1. Develop an integrated suite of M&S tools to support follow-on testing of AIAMD with existing and future launchers, sensors, and other systems to provide operationally representative assessments of increasingly complex system-of-systems.

CH-47F Block II Chinook

The CH-47F Block II Chinook accomplishes critical tasks across the operational environment including air assault, air movement, causality evacuation, aerial recovery, and area resupply. Dialogue continues between Army leadership and members of Congress that will shape an updated acquisition strategy. The current Test and Evaluation Master Plan (TEMP) was approved 4QFY16 and will require an update when the Army's revised acquisition strategy is finalized.

SYSTEM DESCRIPTION

The CH-47 is the Army's tandem rotor cargo helicopter with a capacity to transport 31 combat-loaded troops. The CH-47F Block II retains the Chinook's legacy fiberglass rotor blades but includes a number of system improvements including an improved power train and rotor system, software and avionics upgrades, and a redesigned lightweight fuel system. The Army is in the process of changing the system described in the CH-47F TEMP that was approved in 4QFY16 as the CH-47F Block II. The program is moving away from the development of the Advanced Chinook Rotor Blades due to unresolvable vibration issues. The CH-47F Block II should be able to improve performance at lower altitudes and cooler temperatures using the fiberglass rotor blades. Current analysis shows that the CH-47F Block II will not be able to meet its performance requirements at high altitudes and in hot conditions in this configuration.

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 is an Acquisition Category IC program led by the Army's Program Executive Office Aviation at Redstone Arsenal, Alabama. The Milestone Decision Authority is the Army Acquisition Executive. The Army has not updated the program's TEMP since 4QFY16, and it is no longer valid due to numerous programmatic changes. The Army cancelled a Limited User Test scheduled for 2QFY21 that would have informed a subsequently cancelled Milestone C decision in 4QFY21.

DOT&E is awaiting an updated acquisition strategy and program content update (i.e., rotor blades, fuel cell, drive train, flight control system, avionics) in order to begin work on a revised test strategy and TEMP.

» MAJOR CONTRACTOR

- The Boeing Co. – Ridley Park, Pennsylvania

TEST ADEQUACY

The Army completed a CH-47F Chinook Block II cooperative vulnerability and penetration assessment (CVPA) at Redstone Arsenal, Alabama in 3QFY21. The CVPA was completed in accordance with a DOT&E-approved test plan, and observed by DOT&E. The CVPA was well executed using an accredited system integration lab and a hangered aircraft. The CVPA was intended to support the cancelled 4QFY21 Milestone C decision.

The program executed post-ballistic testing of the CH-47F Block I and Block II synchronization shafts at Boeing, Ridley Park, Pennsylvania, in 1QFY22 to evaluate the survivability of these components following ballistic damage. Testing was completed in accordance with the DOT&E-approved test plan and under DOT&E observation. Testing was informed by prior static testing of the articles at Aberdeen Proving Ground, Maryland.

Following cessation of development of the Advanced Chinook Rotor Blades, DOT&E recommended dynamic ballistic testing of the legacy fiberglass rotor blades to assess survivability in accordance with program requirements. This testing was originally planned for 2003 but not executed when the CH-47 Ground Test Vehicle was destroyed in a maintenance event. The Program Office elected not to perform this testing in accordance with the DOT&E-approved TEMP and chose to concede aircraft vulnerability to the threat.

Despite the future of the CH-47F Block II program being uncertain, the program continues to conduct regular test strategy working groups to coordinate development and integration testing. The utility of these working groups is limited due to the lack of a well-defined aircraft configuration, acquisition approach, and updated TEMP.

PERFORMANCE

» EFFECTIVENESS

The CH-47F Block II developmental testing using fiberglass rotor blades has seen some performance improvements attributed to the aircraft's improved power train and rotor system. The CH-47F Block II includes other system modernizations including software and avionics upgrades.

CH-47F Block II effectiveness will be assessed during future operational testing. Operational testing is not scheduled and should be included in the TEMP update.

» SUITABILITY

CH-47F Block II suitability will be assessed during future operational testing. Operational testing is not scheduled and should be included in the TEMP update.

» SURVIVABILITY

The CH-47F Block II should complete live-fire testing to assess aircraft survivability. The program has begun but not completed ballistic self-sealing tests on the new lightweight fuel system. The fuel cell failed qualification testing and experienced other issues during testing in FY21. The Program Office must decide on a path forward to address these issues and complete qualification and live fire testing.

The Army elected not to complete live-fire testing against the fiberglass rotor blades on the basis that regardless of the result, the Army would not change CH-47 tactics, techniques, or procedures. Due to the Program Office choosing not perform rotor blade testing in accordance with the DOT&E-approved TEMP and conceding a CH-47 required threat, DOT&E must use preliminary data and assume the aircraft is vulnerable to the threat in the vulnerability analysis. This analysis will apply to both the CH-47F Block I and Block II as well as all other H-47 aircraft equipped with this blade.

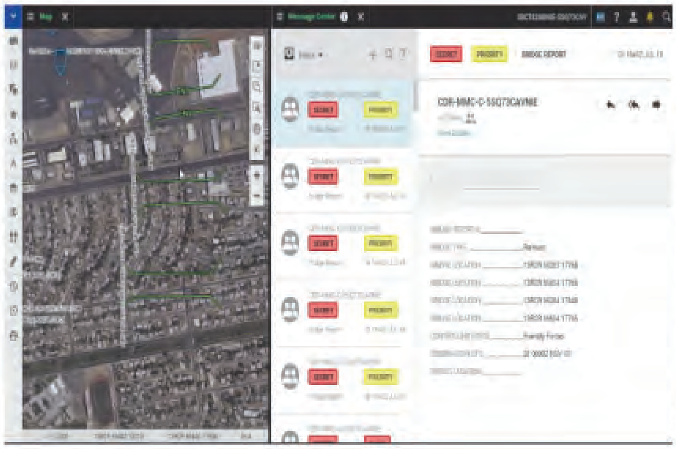
DOT&E will work with the Army to schedule operational testing once a revised acquisition strategy emerges from the Army. DOT&E will publish a complete assessment of the CH-47F Block II's operational effectiveness, suitability, and survivability at the completion of operational testing.

RECOMMENDATIONS

The Army should:

1. Complete a TEMP update to allow an assessment of test strategy adequacy.
2. Determine a path forward to address fuel cell survivability issues and execute testing in accordance with DOT&E-approved test plans.
3. Execute dynamic testing of the fiberglass rotor blade against the CH-47F required threat.

Command Post Computing Environment (CPCE)



Command Post Computing Environment (CPCE) Increment 1 is operationally effective in supporting commanders and staff with improved situational awareness and mission command. CPCE Increment 1 is not operationally suitable due to problems with reliability, training, and usability. CPCE Increment 1 is survivable and demonstrated an enhanced defensive posture within a cyber-contested environment. The Army conducted a CPCE Increment 1 full deployment decision (FDD) in December 2021 and approved the fielding of CPCE Increment 1 in a January 2022 acquisition decision memorandum (ADM).

SYSTEM DESCRIPTION

CPCE Increment 1 is a server-based software system that provides server hardware and mission command software to support commanders and staff using general-purpose client computers, located within battalion through corps Tactical Operations Centers. CPCE Increment 1 is the Army's planned evolution of the fielded CPCE Increment 0. The Army intends CPCE Increment 1 to improve the soldier's user experience, interface with more data sources, and correct deficiencies noted with CPCE Increment 0.

The server hardware to support CPCE Increment 1 includes two variants: a Tactical Server Infrastructure Large, a full server stack designed to support headquarters at brigade level and above, and a Tactical Server Infrastructure Small, a laptop-based server designed to support battalion headquarters and provide back-up capabilities for higher echelons. The CPCE Increment 1 software provides a common operational picture, a suite of web-based collaboration tools, and messaging capabilities to support the commander and staff's execution of the Army operations process.

The Army designed CPCE Increment 1 to share information with joint and coalition partners utilizing the Multilateral Interoperability Programme standard. CPCE Increment 2 provides convergence of additional Army mission command systems, and additional joint and coalition interoperability through an expanded set of message standards.

MISSION

The Army intends for commanders and staff at battalion through corps level 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

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

DOT&E approved the CPCE Increment 1 Test and Evaluation Master Plan in November 2019. The Army completed a June 2021 CPCE Increment 1 FOT&E in accordance with a DOT&E-approved test plan. DOT&E published a CPCE Increment 1 FOT&E report on December 10, 2021. The Army conducted a CPCE Increment 1 FDD in December 2021, and approved the fielding of CPCE Increment 1 in a January 2022 ADM. The program initiated an improvement plan to correct the deficiencies noted during the CPCE Increment 1 FOT&E and demonstrate these corrections during a fielding, Warfighter Exercise or CPCE Soldier Touch Point event. The program has completed a CPCE Increment 2 Test and Evaluation Master Plan which is in Army staffing for delivery to DOT&E for approval.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

The Army conducted a CPCE Increment 1 FOT&E and an adversarial assessment at Fort Carson, Colorado from June 7-24, 2021, and a cooperative vulnerability and penetration assessment, at Fort Bragg, North Carolina from April 5-9, 2021. Operational testing, executed by elements of the 4th Infantry Division and allied partners operating within a command post exercise environment, was adequate to evaluate the CPCE Increment 1 operational effectiveness, suitability, and survivability. The Army conducted the operational test in accordance with a DOT&E-approved test plan, and observed by DOT&E.

The Army completed a partial verification and validation of data instrumentation prior to the CPCE Increment 1 FOT&E due to problems with their data collection, reduction, and assessment process. DOT&E approved the operational test plan with the condition that the Army would complete the verification and validation effort following testing. The Army completed the verification and validation of CPCE Increment 1 data instrumentation, and initiated an effort to improve future CPCE data instrumentation by adopting more current, commercial standards-based applications following the CPCE Increment 1 FOT&E.

PERFORMANCE

» EFFECTIVENESS

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

» SUITABILITY

CPCE Increment 1 is not operationally suitable, experiencing problems with reliability, training, and usability:

- CPCE Increment 1 did not meet its derived reliability requirement. CPCE Increment 1's poor reliability reduces its support for commanders and staff and increases the unit's requirements for maintenance support and field service representatives.
- Training provided to soldiers did not prepare them to make full use of advanced features, troubleshooting, and employment of CPCE Increment 1 in a collaborative manner. Soldiers viewed CPCE Increment 1 as easy to use for basic features, but regarded CPCE Increment 1 as difficult to use for advanced functions, such as troubleshooting software problems and sharing operations orders.
- Soldier system administrators experienced difficulty using CPCE Increment 1 tools intended to configure and maintain CPCE software and hardware. These maintainers found CPCE Increment 1 difficult to troubleshoot and more manpower intensive than CPCE Increment 0.

» SURVIVABILITY

CPCE Increment 1 demonstrated enhanced survivability in a cyber-contested environment compared to CPCE Increment 0. CPCE Increment 1 maintained a strong cybersecurity defense posture when employed with trained Army cyber defense soldiers using integrated cyber defense tools. The full description of CPCE Increment 1 cybersecurity survivability against an operationally realistic cyber threat is included in a classified annex to the December 2021 CPCE Increment 1 FOT&E report.

RECOMMENDATIONS

The Army should:

1. Complete the improvement plan to correct deficiencies noted during the CPCE Increment 1 FOT&E, and demonstrate fixes in future CPCE test events.
2. Demonstrate training improvements to correct deficiencies noted during the CPCE Increment 1 FOT&E in a future fielding, Warfighter Exercise or CPCE Soldier Touch Point event.
3. Complete the improvement of CPCE data instrumentation to support test adequacy and confidence in data collection during future developmental and operational tests, and demonstrate its effectiveness in a CPCE test event.

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

Left: GEN 1.0 | Center: GEN 1.2 | Right: GEN II

The Dismounted Assured, Positioning, Navigation, and Timing System (DAPS) program conducted an operational assessment (OA) to support an early fielding of the Generation (GEN) 1.0 and GEN 1.2 DAPS to an Army Infantry Brigade Combat Team in FY22. The Army selected the TRX Systems Inc. DAPS GEN II for the program of record and began a series of field and lab testing in June 2022 with a Limited User Test (LUT) scheduled in early FY23.

SYSTEM DESCRIPTION

DAPS provides Army forces with unhindered access to trusted Positioning, Navigation, and Timing (PNT) information under conditions where space-based GPS signals may be limited or denied. DAPS replaces the Army's legacy Defense Advanced GPS Receiver (DAGR) used by dismounted soldiers. Unlike the DAGR, DAPS incorporates a Military Code receiver as well as non-GPS capabilities providing the user with PNT information from multiple sources.

DAPS GEN 1.0 includes a "boot module" to assist soldiers in maintaining position and navigation capability based on soldier movements. Soldiers interface with the DAPS GEN 1.0 using the Nett Warrior End User Device (EUD). DAPS GEN 1.2 has an internal rechargeable battery as well as internal inertial measurement unit and alternative satellite reception capabilities. DAPS GEN II is an improved version of DAPS GEN 1.2 with an external, detachable rechargeable battery, redesigned screen and soldier interface, and improved PNT data fusion capability. Both DAPS GEN 1.2 and GEN II can be used in a stand-alone mode or with the Nett Warrior EUD interface.

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 jamming and spoofing of the GPS.

PNT information derived from 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

In 2019, the Commanding General, Army Futures Command issued two directed requirements for the DAPS effort directing the rapid prototyping, OA, and limited fielding of advanced PNT technologies to inform an enduring requirement and follow-on program of record. The PNT Program Manager is utilizing several Other Transaction Authority contracts and a phased prototyping approach to satisfy the Army Futures Command directed requirements.

DAPS GEN 1.0 and DAPS GEN 1.2 followed the Urgent Capability Acquisition pathway culminating in an OA in 4QFY21 and a limited equipping of an Infantry Brigade Combat Team in FY22. In early FY22, the Army selected TRX Systems Inc. as the vendor for the DAPS GEN II program of record. The Army intends DAPS to transition to a major capability acquisition program at Milestone C in FY23. A DAPS Test and Evaluation Master Plan (TEMP) is currently in draft and expected to be approved by DOT&E prior to the planned Milestone C decision.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

In August and October 2021, the Army Test and Evaluation Command conducted an OA at Ft. Huachuca, Arizona, and White Sands Missile Range, New Mexico in accordance with the DOT&E-approved test plan, and observed by DOT&E. The OA was adequate to determine operational effectiveness and suitability of the GEN 1.0 and GEN 1.2 systems. The results of the OA informed the Army's decision to equip an Infantry Brigade Combat Team and the selection of TRX as the vendor for the DAPS GEN II.

The Army has addressed a DOT&E recommendation from the 2021 Annual Report and found a suitable location to conduct the LUT in 1QFY23 in accordance with the DOT&E-approved test plan.

PERFORMANCE

» EFFECTIVENESS

Both the DAPS GEN 1.0 and 1.2 systems performed better than the legacy DAGR system in GPS-degraded environments. Dismounted infantry squads equipped with either GEN 1.0 or GEN 1.2 DAPS are operationally effective at accomplishing reconnaissance missions in contested GPS environments. Performance issues are detailed in the classified DAPS early fielding report (EFR) published January 2022.

» SUITABILITY

DAPS GEN 1.0 and 1.2 systems are operationally suitable. Neither system experienced a reliability failure during the OA. The training provided by the Army was not sufficient and soldiers require more hands-on training. GEN 1.0 users preferred a stand-alone capability and user interface separate from the Nett Warrior EUD. GEN 1.2 users indicated the need for longer internal battery life when disconnected from the conformal battery. The classified DAPS EFR provides details on operational suitability.

» SURVIVABILITY

A cooperative vulnerability and penetration assessment was conducted on both DAPS prototypes and the results are detailed in the classified DAPS EFR. The Army plans to conduct an adversarial assessment in conjunction with the DAPS GEN II LUT in FY23.

RECOMMENDATION

The Army should:

1. Verify correction of DAPS performance deficiencies identified in the classified EFR prior to conducting the LUT.

Distributed Common Ground System – Army (DCGS-A) Capability Drop 2 (CD2)

The Army conducted a series of developmental tests and an Operational Utility Assessment of Distributed Common Ground System – Army (DCGS-A) Capability Drop 2 (CD2) by providing access to operationally representative intelligence units throughout the Army in September through October 2022. This assessment demonstrated both capabilities and limitations of the current version of CD2. The Army should work with DOT&E to design and execute a strategy to continue to demonstrate the operational effectiveness, suitability and survivability of the CD2.

SYSTEM DESCRIPTION

The DCGS-A CD2 replaces the current DCGS-A Brain data warehouse capability and is intended to be interoperable with legacy DCGS-A systems and CD1s. The CD2 is designed to provide a cloud-based Army intelligence data architecture that will bring in intelligence data from hundreds of Service and Intelligence Community data sources. The CD2 will organize and process the data to allow users to search and find relevant information and provide advanced intelligence analysis tools.

CD2 operates on SECRET and TOP SECRET/Sensitive Compartmented Information enclaves. Users will access CD2 data either directly from the cloud or by connecting to a Deployed Edge Node (DEN).

MISSION

Army intelligence analysts in Military Intelligence Brigades – Theater, tactical units from Corps down to battalions, and Special Operational Forces will use DCGS-A CD2 to access intelligence data. DCGS-A CD2 provides users at corps and above a set of additional advanced analytical tools. They will use DCGS-A to store, process, exploit, and disseminate intelligence data, including threat, weather, and terrain.

PROGRAM

The Project Manager (PM) Intelligence Systems and Analytics is managing DCGS-A as an inactive Major Defense Acquisition program, and intends to transition capabilities currently covered by DCGS-A to future programs.

There is no plan for further capability drops for DCGS-A.

The PM conducted a market survey and selected two vendors for CD2. After a series of developmental tests and a field test, the Army selected Palantir Technologies as the contractor for CD2. After the contract award, the program office conducted more developmental tests, but did not satisfactorily demonstrate CD2's ability to ingest, normalize and correlate intelligence data. In FY22, the Army decided to host the CD2 capability on the Army Commercial Cloud Service Platform (AC2SP). The CD2 on the Army Commercial Cloud Service Platform did not complete an operational test in FY22.

DOT&E did not approve the DCGS-A CD2 Operational Utility Assessment (OUA) Plan, because it did not describe an adequate plan for operational testing. While the operational test plan included plans for collecting test officer observations, surveys, interviews, and user's computer screenshots, these data are not adequate to determine the accuracy or completeness of CD's battlefield picture.

The Army will work with DOT&E to develop a path forward to conduct continual assessments of user and system performance with unit engagements and observations to achieve operational outcomes. The updated T&E strategy will be documented in the Test and Evaluation Master Plan.

» MAJOR CONTRACTOR

- Palantir Technologies, Inc. – Denver, Colorado

TEST ADEQUACY

The Army's initial test concept called for a series of developmental tests to test system capability as the system matures, and to develop and enhance test tools and methodology. To test a complex system such as DCGS-A CD2, the program office tried to develop a "Test Harness" that is a combination of modeling and simulation tools as well as data collection and processing tools.

The Test Harness did not work as designed, however, and the Army fell back on manual and semi-automated methods to generate intelligence data, and to process the resulting test data.

The series of developmental test events was supposed to culminate in a field test in June 2021. As initially planned, the field test would have used operationally representative data on an operationally representative network. The field test was expected to be the source of quantitative performance data. However, because of the immaturity of the system and the lack of test readiness, the Army modified the field test into a lab test, using small sample data set, conducted by the program office.

ATEC conducted a customer test of DCGS-A CD2 for the PM Intelligence Systems and Analytics in March 2022. This test was initially intended to be the first phase of an operational test, but DOT&E did not approve the operational test plan due to an inadequate plan for collecting and processing test data. Subsequently the Army modified the event to a customer test.

ATEC conducted a cooperative vulnerability and penetration assessment (CVPA) of DCGS-A CD2 on the Cloud node in July 2022. ATEC conducted a second CVPA on the DEN, also in July 2022. ATEC conducted an adversarial assessment (AA) of DCGS-A CD2 Cloud node in August through September 2022. DOT&E approved the CVPA plans and the AA plan for the cloud node. The DEN is not ready for an AA yet.

ATEC conducted an Operational User Assessment (OUA) event September 29 through October 13, 2022. The test used a subset of operationally representative real world intelligence data feeds needed for users to complete their missions. The OUA provided the Army with useful data to improve CD2 performance. However, the OUA could not determine whether DCGS-A CD2 provided accurate and complete intelligence products to system users.

PERFORMANCE

» EFFECTIVENESS

The limited testing up through the CT event has indicated that users could not bring in sufficient intelligence data from the required sources to perform intelligence missions; however, the Army continues to increase the scope of data feeds. Observations indicate that Army organization, doctrine, and training to manage intelligence data need improvement. The DEN and DCGS-A CD2 Cross-Domain Solution were not available for test. During the OUA, analysts used an external cross-domain solution.

» SUITABILITY

Limited testing to date indicates that the Army does not have sufficient capability to manage CD2 data. Management or "curation" of data is critical for a complex, data-centric system such as DCGS-A CD2 that relies on machine learning technology. The limited testing to date indicates the Army needs to improve the organization, doctrine and training for managing the intelligence data.

» SURVIVABILITY

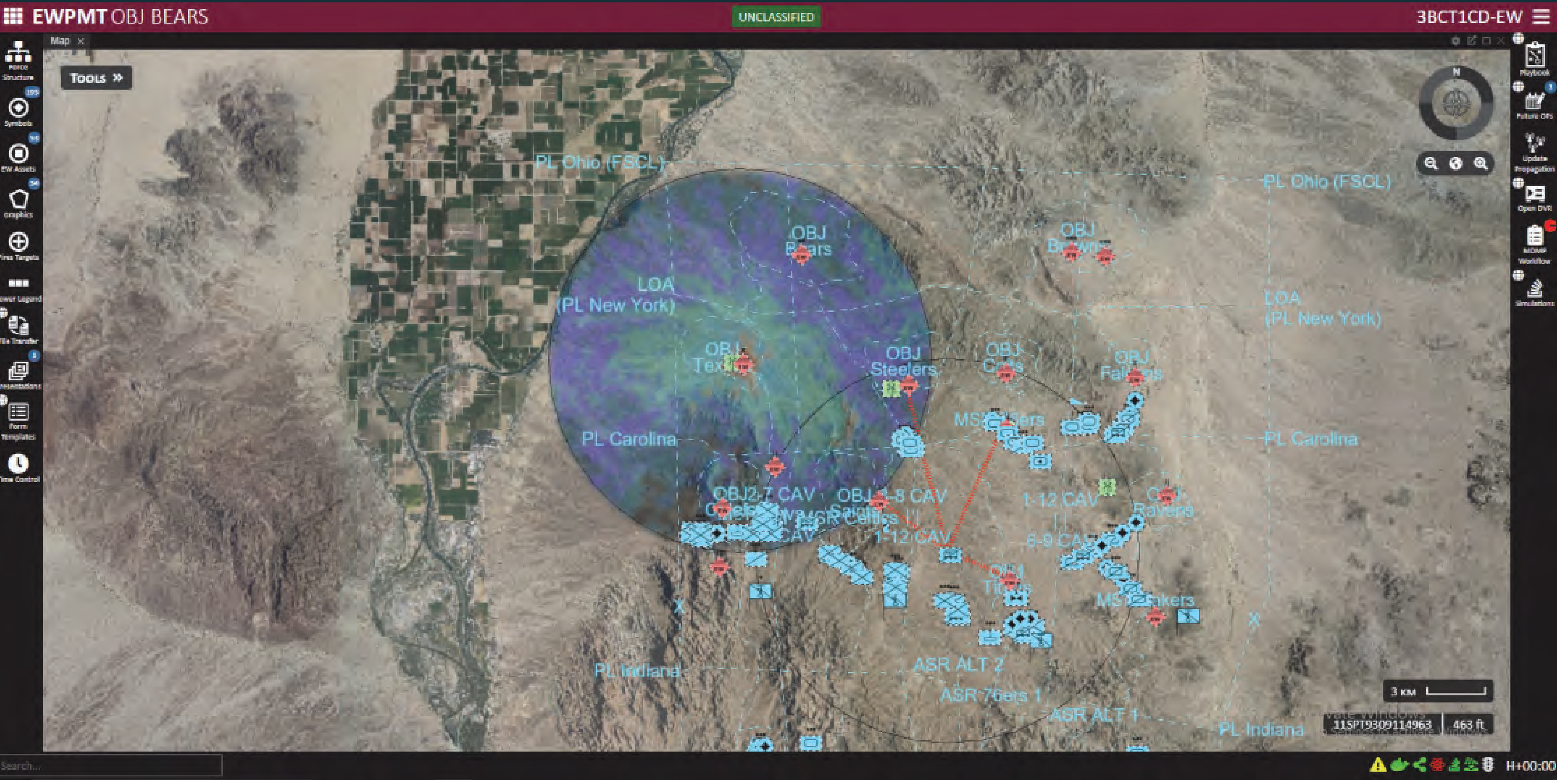
The CVPAs and AA for the cloud node showed positive developments in the Army Intelligence community's ability to defend cloud-based applications from cyber-attacks. The Army fixed most of the vulnerabilities from the CVPA, but uncovered two vulnerabilities during the AA. The Army proposed a mitigation plan for the vulnerabilities discovered during the AA, but has not conducted a validation of fixes event yet.

RECOMMENDATIONS

The Army should

1. Work with DOT&E to design and execute a strategy to demonstrate the operational effectiveness, suitability and survivability of the CD2.
2. Develop tools, technology, and training for personnel to support testing of advanced, data-centric systems such as DCGS-A CD2, and to prepare for the advanced data analytics and Artificial Intelligence systems of the future.

Electronic Warfare Planning and Management Tool (EWPMT)



The Army conducted the Electronic Warfare Planning and Management Tool (EWPMT) IOT&E in 4QFY21. DOT&E assessed EWPMT as operationally effective at supporting electromagnetic spectrum planning and management operations, demonstrating the capability to support the commander's Military Decision-Making Process subject to performance issues detailed in the classified IOT&E report published in May 2022. EWPMT is operationally suitable, demonstrating high operational availability. The Army intends to assess the remote management of electronic warfare assets in FOT&E events scheduled in FY25.

SYSTEM DESCRIPTION

EWPMT Increment 1 (INC1) is part of the Army's efforts to rebuild electronic warfare (EW) capabilities lost after the Cold War ended. It is a software application that resides on a laptop or server, enabling a unit to conduct EW mission planning, EW targeting, spectrum management, EW asset management and control, and to create an electromagnetic operating environment common operational picture. The Army intends for EWPMT to provide local and remote operational control and management of organic and assigned electronic warfare assets and integrate with the Terrestrial Layer System (TLS) and the Multi-Function Electronic Warfare – Air Large (MFEW-AL) system to execute electronic support and electronic attack.

MISSION

EWPMT INC1 is expected to provide Army corps, divisions, and brigade combat teams with software toolsets to integrate EW and spectrum management operations in support of multi-domain operations. EWPMT is used by the Commander, Electronic Warfare Officers, and Electromagnetic Spectrum Managers to plan, coordinate, integrate, and synchronize cyber electromagnetic activities.

PROGRAM

EWPMT is an Acquisition Category II Automated Information System program. The Army developed and deployed an early version of EWPMT INC1 to a limited number of brigade combat teams in response to an Operational Needs Statement. The EWPMT full deployment decision is expected in 3QFY23. The development and testing of EWPMT is guided by a Simplified Acquisition Management Plan (SAMP) rather than a traditional Test and Evaluation Master Plan (TEMP). The EWPMT SAMP integrates the TEMP, System Engineering Plan, and the Acquisition Strategy. DOT&E approved the SAMP in August 2021. EWPMT will conduct FOT&E events in FY25 in conjunction with TLS IOT&E and MFEW-AL IOT&E to evaluate EWPMT's ability to manage and control EW systems. The EWPMT FOT&E is delayed two years due to a slip in the MFEW-AL and TLS programs.

» MAJOR CONTRACTOR

- Raytheon Company – Fort Wayne, Indiana

TEST ADEQUACY

The Army's 2nd Stryker Brigade Combat Team, 4th Infantry Division conducted IOT&E in conjunction with a command post exercise in August 2021 at Fort Carson, Colorado, in accordance with the DOT&E-approved test plan, and was observed by DOT&E. IOT&E was adequate to support an assessment of operational effectiveness, suitability, and survivability. The IOT&E included an adversarial assessment to evaluate the EWPMT's cyber survivability.

The Army conducted a cooperative vulnerability and penetration assessment in May 2021 assessing EWPMT INC1 from an insider and nearsider posture. Maintenance and configuration problems of associated systems precluded an assessment from an outsider posture.

PERFORMANCE

» EFFECTIVENESS

A unit equipped with EWPMT INC1 is effective in conducting EW and electromagnetic spectrum planning and management. EWPMT INC1 supported the brigade's Military Decision-Making Process, contributed to successful engagement of high-payoff targets, provided effective tools for spectrum management, and improved the brigade commander's and staff's situational awareness of the electromagnetic operating environment. Performance issues are detailed in the EWPMT IOT&E report published May 2022.

» SUITABILITY

EWPMT INC1 is operationally suitable, demonstrating high operational availability. Soldiers were able to remedy software faults quickly. Soldiers indicated the system is easy to learn and use. Training was sufficient, but soldiers provided suggestions to increase its effectiveness.

» SURVIVABILITY

The survivability of the EWPMT INC1 in a cyber-contested environment is detailed in the classified annex to the EWPMT IOT&E Report.

RECOMMENDATIONS

The Army should:

1. Verify correction of system performance, suitability, and survivability deficiencies identified in IOT&E prior to FOT&E.
2. Complete a cybersecurity assessment from an outsider threat posture.

3. Refine training to emphasize troubleshooting and help leaders and staff understand EWPMT INC1 capabilities and operational employment.
4. Continue coordination with the MFEW-AL and TLS programs to demonstrate control and management of these systems during EWPMT's FOT&E.

Future Long Range Assault Aircraft (FLRAA)

Left: Sikorsky-Boeing prototype design | Right: Bell Textron Incorporated prototype design

The Army is completing technology development efforts for the Future Long Range Assault Aircraft (FLRAA) program. The Army is using the Middle Tier of Acquisition (MTA) rapid prototyping approach to produce a virtual prototype prior to transitioning to a Major Capability Acquisition pathway in late FY23. The Army has been transparent and collaborative while developing the FLRAA acquisition strategy and supporting T&E strategy.

SYSTEM DESCRIPTION

The Army intends FLRAA to be the next generation of vertical-lift, assault, and intra-theater aeromedical evacuation aircraft. It is a medium-lift helicopter that will augment or replace a portion of the Army's UH-60 Black Hawk utility helicopter fleet. The Army intends FLRAA to provide Combat Aviation Brigades with long-range, high-speed utility aircraft that are survivable in contested environments.

The FLRAA will serve a role in what the Army is terming the Future Vertical Lift (FVL) ecosystem, in which the different programs within the FVL ecosystem (e.g., Future Attack Reconnaissance Aircraft, Air Launched Effects, and Future Tactical Unmanned Aerial System) contribute to the effectiveness and holistic survivability of all FVL programs in a multi-domain environment.

MISSION

Units will utilize FLRAA's increased speed, range, and maneuverability to assault enemy forces from areas of relative safety outside the range of enemy long-range fires. The FLRAA will be effective, decisive, and survivable in the lower tier of the air domain. It will integrate other programs within the FVL ecosystem to ensure mission success.

PROGRAM

The Army was granted entry into the MTA pathway as a rapid prototyping effort in May 2021. Their MTA efforts will culminate in a virtual prototype of the FLRAA to reduce risk prior to prototype aircraft production. The Army plans to transition to a post-Milestone B Major Capability Acquisition program in late FY23 as an Acquisition Category IB program. The Army's Milestone B Test and Evaluation Master Plan (TEMP) is in development with excellent collaboration with the T&E community.

The program underwent a Competitive Demonstration and Risk Reduction (CD&RR) phase between two vendors: Bell Textron Incorporated and a Sikorsky-Boeing partnership. The Sikorsky-Boeing partnership proposal is based on the SB>1 Defiant technology demonstrator (left), and the Bell Textron Incorporated proposal is based on the tilt-rotor V-280 Valor technology demonstrator (right).

» MAJOR CONTRACTORS

- Bell Textron Incorporated – Fort Worth, Texas
- Sikorsky Aircraft Corporation, a Lockheed Martin Company – Stratford, Connecticut

TEST ADEQUACY

The FLRAA program is developing a TEMP to support a Milestone B decision. The top-level plan is to develop flight-worthy aircraft prototypes in FY25, followed by a Limited User Test (LUT) in FY27, a Milestone C decision in FY28, and a Full-Rate Production decision in FY30. The FLRAA T&E Working-level Integrated Product Team hosts meetings on a regular basis to support test planning and TEMP updates.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

No operational testing has been conducted to assess its effectiveness, suitability, and survivability. Transparency and collaboration has been a highlight of the FLRAA program. The Program Office engages stakeholders across the test community in order to minimize misunderstandings and strengthen lines of communication. They frequently coordinate with the joint community to leverage best practices and lessons learned from other Services. The program is developing their post-Milestone B TEMP to incorporate candid feedback from the test community. The Program Office should increase coordination across the FVL ecosystem to ensure complementary test strategies across FVL efforts. The FLRAA program has set a solid foundation for a successful program if current practices are retained.

RECOMMENDATION

The Program Office should:

1. Increase coordination across the FVL ecosystem to ensure complementary test strategies across FVL efforts.

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

In April 2022, the Army conducted a soldier touch point (STP) of the Leader Radio and Manpack demonstrating improvements in performance. Light infantry platoons equipped with the Leader Radio and Manpack are operationally effective when operating the voice and data network in the dense vegetation where they expect to operate. The Army has not demonstrated operational effectiveness or operational suitability of a company-level system-of-systems network. The system of systems that comprise the tactical network have not demonstrated operationally suitability due to incomplete testing of the logistics burden on the unit.

SYSTEM DESCRIPTION

The Handheld, Manpack, and Small Form Fit (HMS) program consists of the Leader and Manpack radios. The Leader Radio is a two-channel, handheld, software-defined radio. The Manpack radio is a two-channel, software-defined radio employed by general purpose radio users capable of operating two simultaneous waveforms. Both the Manpack and Leader Radio provide SECRET and CUI tactical voice and data communications. The Atom network management software configures the networks formed by the waveforms running on the Leader Radio and Manpack.

MISSION

Commanders employ the battalion and below networks to support mission execution through the exchange of information. The tactical networks created by Leader Radio and Manpack provide the transport layer for battalion and below network. These networks should be capable of sending and receiving the voice and data messages necessary to execute command and control and commander's intent.

PROGRAM

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

» MAJOR CONTRACTORS

- L3Harris Technologies Inc. – Melbourne, Florida
- Collins Aerospace – Cedar Rapids, Iowa
- Thales Defense and Security Inc. – Clarksburg, Maryland

TEST ADEQUACY

The Army conducted a STP customer test of the HMS Leader Radio and Manpack at Fort Bragg, North Carolina in April 2022. The Army Acquisition Executive required the program to verify corrections of deficiencies discovered during the IOT&E. The STP did not have a DOT&E-approved test plan, but was observed by DOT&E. The HMS STP was adequate to evaluate the operational effectiveness of dismounted infantry platoon missions and the suitability of training and human system interface with the radios. The STP consisted of eight force-on-force missions conducted over eight days with each mission lasting around four hours. The STP was not designed to evaluate operational effectiveness or survivability at the company echelon, as the IOT&E was. The Army did not scope the STP to assess reliability, availability, or maintainability. In accordance with the Test and Evaluation Master Plans, these will be evaluated by combining data as appropriate from annual production verification testing and STPs.

PERFORMANCE

» EFFECTIVENESS

Infantry platoons equipped with the Leader Radio and Manpack are operationally effective when operating the Tactical Scalable Mobile ad-hoc network (TSM) voice and data network provided by the HMS equipment. When connected, the TSM network provided enhanced situational awareness by providing soldier position location information and clear voice communication. The TSM network demonstrated sufficient connectivity and range in dense vegetation for platoon operations.

The Leader Radio provided TSM at ranges meeting platoon distance requirements and the Manpack TSM range supported the operationally realistic STP missions. The Army has not demonstrated TSM effectiveness at the company-echelon.

Single Channel Ground and Airborne Radio System, Mobile User Objective System, and Integrated Waveform satellite communications worked well. The Atom software was operationally effective for network management planning and loading.

» SUITABILITY

The HMS STP demonstrated improvements to Leader Radio and Manpack battery life and soldier integration. Leader Radio demonstrated a battery life that supported the limited mission lengths conducted during the STP. Extrapolation of measurements collected during the STP indicate that the Leader Radio and conformal wearable battery life support extended operations. The Manpack demonstrated improved battery life. Dismounted infantry companies demonstrated the ability to keep the Leader Radios, Manpacks, and conformal wearable batteries charged with their organic equipment, but not in an operational or field environment.

The Leader Radio demonstrated improvements integrating into soldier combat equipment. The Manpack continues to demonstrate high external temperatures and soldiers were dissatisfied with the weight. Changes in carrying packs were well received by the soldiers. Product Manager HMS is continuing to develop the packs. Signal soldiers observed improvements in Atom software's usability. Training was sufficient for the Leader Radio, Manpack, and Atom software.

The HMS IOT&E did not provide adequate data to evaluate the reliability, availability, and maintainability of the Leader Radio and Manpack. The reliability data collected during the STP will be combined with future events to provide a cumulative evaluation. HMS radios will participate in the Integrated Tactical Network Operational Demonstration in 2QFY23, providing an opportunity for assessment.

» SURVIVABILITY

The survivability of the Leader Radio and Manpack in cyber-contested and electromagnetic spectrum operational environments is detailed in the classified annex of the HMS IOT&E report published in July 2021. The Army has not corrected the cyber deficiencies.

RECOMMENDATIONS

The Army should:

1. Design a tactical network that prioritizes range for voice and position location information.
2. Test tactical power management for light infantry units in an operational environment.
3. Continue to improve integration with the rucksack for the Manpack.
4. Conduct follow-on operational testing to evaluate the remaining operational effectiveness, operational suitability, and survivability deficiencies with a company equipped with the Leader Radio and Manpack.

Infantry Squad Vehicle (ISV)

The Army fielded the Infantry Squad Vehicle (ISV) to two Infantry Brigade Combat Teams in FY22 using low-rate initial production (LRIP) quantities. They are making modifications to the LRIP configuration to address reliability, and maintainability deficiencies identified in previous testing. Reliability compliance testing to validate corrective actions on the ISV vehicle began in June 2022 and is scheduled for completion in February 2023. The Army conducted Simulated Airdrop Impact Tests (SAITs) of the ISV in July 2022. Unit airdrop operations scheduled for September 2022 were delayed due to the unavailability of production-representative vehicles. The Full-Rate Production decision is scheduled for March 2023.

SYSTEM DESCRIPTION

The ISV is a light, off-road, unarmed and unarmored vehicle designed to carry a nine-soldier infantry squad and their equipment. It provides new capabilities to infantry units conducting rapid deployment into contested areas and extended movement over difficult terrain. The ISV is based on the commercial Chevrolet Colorado ZR2 Bison platform with a 2.8-liter Duramax engine, a six-speed transmission, and an electronically actuated four-wheel drive transfer case. The vehicle has roll-over protection and is reconfigurable to transport a casualty using an integrated, stowable litter system. It is required to be externally and internally transportable by CH-47 helicopters, externally transportable by UH-60s, and able to be airdropped by C-17 and C-130 aircraft.

MISSION

Infantry Brigade Combat Teams will employ the ISV to increase the ground tactical mobility and operational tempo of light infantry units conducting decisive action operations. During forced-entry operations, units equipped with the ISV can insert at extended distances from objectives to counter threat anti-access/area denial strategies by using multiple points of entry to place the enemy at an operational disadvantage.

PROGRAM

The ISV is an Acquisition Category III program. DOT&E published an IOT&E report in December 2021 assessing operational effectiveness, suitability, and survivability. The Full-Rate Production decision is scheduled for March 2023.

» MAJOR CONTRACTOR

- General Motors Defense – Detroit, Michigan

TEST ADEQUACY

The ISV did not meet its 1,200 mean miles between operational mission failure requirement in previous testing. Reliability compliance testing of the ISV began in June 2022 to validate corrective actions implemented by the vehicle manufacturer to address deficiencies identified during developmental and operational testing. The test is planned for 5,000 miles over varying terrain and speeds consistent with the mission profile. DOT&E and Army Test and Evaluation Command will use the test data to assess if the modified ISV meets reliability requirements.

In July 2022, the Army conducted two SAITs using vehicles with corrective modifications to assess the vehicle's ability to endure the forces experienced during low velocity airdrop operations and dual rail airdrop operations, and to re-validate vehicle rigging procedures. Upon completion of the SAITs, the vehicles were driven approximately 30 miles over terrain consisting of roads and improved trails. Data from the tests are being analyzed.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Data from the simulated airdrop impact testing is under review, and data from the 5,000-mile reliability compliance testing is expected in 2QFY23. DOT&E will use the data to assess whether the vehicle meets the reliability requirement and is suitable to support airdrop operations.

Follow-on testing to assess changes in effectiveness and survivability were not conducted.

RECOMMENDATIONS

The Army should:

1. Airdrop the ISV as part of a tactical airborne operation to assess the suitability of the vehicle to support airborne operations.
2. Complete reliability compliance testing using production-representative vehicles to demonstrate compliance to the reliability requirement prior to the Full-Rate Production decision.
3. Complete, validate, and verify the technical manuals.

Integrated Personnel and Pay System – Army (IPPS-A) Increment 2

Integrated Personnel and Pay System – Army (IPPS-A) is a Business System Category 1 program with four releases. The Program Office completed development and testing of IPPS-A Release 3 in FY22. A Limited User Test (LUT) demonstrated that IPPS-A Release 3 software does not provide all of the required capabilities to meet the existing functionality of the legacy Human Resources (HR) systems that it is intended to replace. The IPPS-A Release 3 LUT Phase 1 was conducted to support a Limited Deployment (LD) Authority to Proceed (ATP) decision.

SYSTEM DESCRIPTION

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

The capabilities available in IPPS-A 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 should continue to develop IPPS-A in order to deliver a full set of necessary capabilities to support pay functionality as well.

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

IPPS-A is a single, integrated personnel and pay system that soldiers can use to conduct self-service personnel transactions and reduce the need for face-to-face interaction with HR professionals.

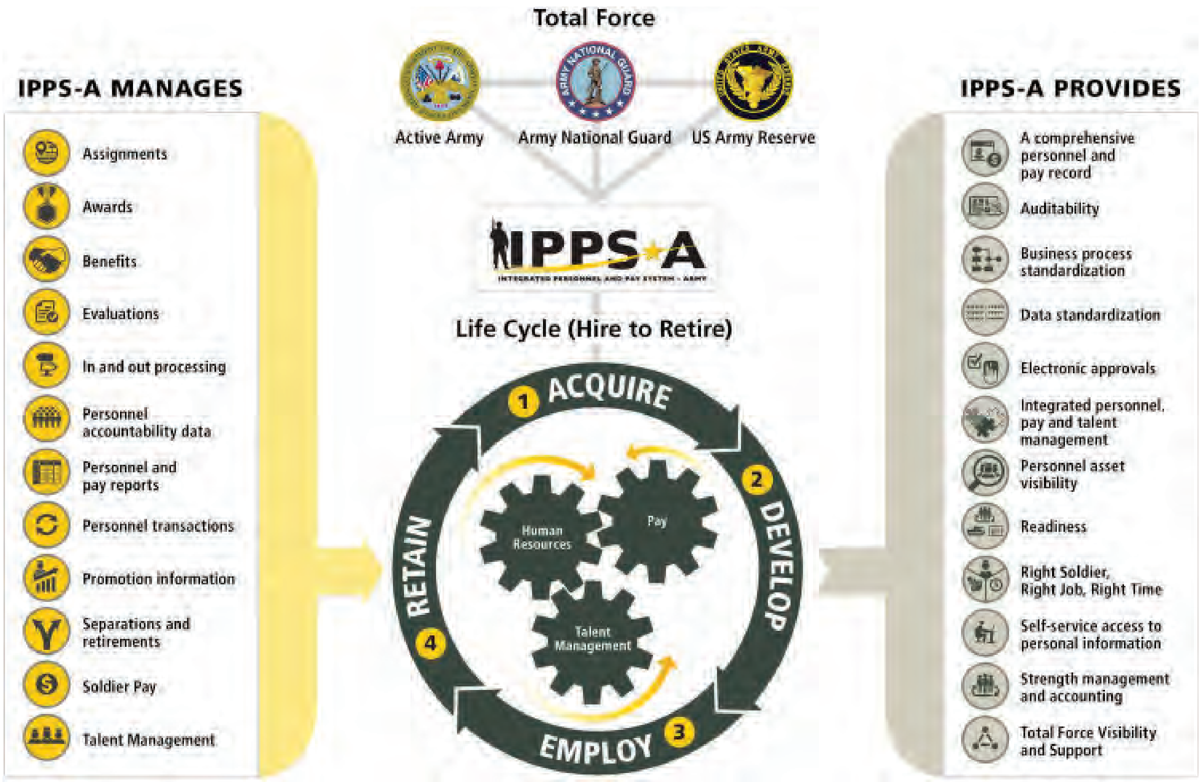
MISSION

Commanders will employ IPPS-A as a comprehensive system for personnel accountability and 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 during peacetime, war, through mobilization and demobilization, capturing timely and accurate data throughout.

PROGRAM

IPPS-A is a Business System Category 1 program for which DOT&E approved the IPPS-A Test and Evaluation Master Plan on August 9, 2018. Subsequently, DOT&E approved an update to the TEMP to address IPPS-A Release 3 on October 8, 2020. DOT&E also approved the Operational Test Plan for the IPPS-A Release 3 LUT on September 3, 2021.

The FY22 LUT will support an FY23 LD ATP decision on whether to allow deployment of the IPPS-A Release 3 software.



» MAJOR CONTRACTOR

- CACI Inc. – Chantilly, Virginia

TEST ADEQUACY

Army Test and Evaluation Command is conducting the LUT in two phases in accordance with the DOT&E-approved test plan. LUT Phase 1 was conducted from June 27 through August 5, 2022 in support of a LD. LUT Phase 2 is planned to be conducted during FY23 to determine whether the deployed version of IPPS-A Release 3 is operationally effective, suitable, and survivable.

Army Test and Evaluation Command conducted a cooperative vulnerability and penetration assessment cyber survivability test as part of LUT Phase 1. An adversarial assessment (AA) cyber survivability test will be conducted during Phase 2 of the LUT.

PERFORMANCE

» EFFECTIVENESS

The LUT Phase 1 demonstrated that IPPS-A Release 3 software does not provide all of the required capabilities to meet the existing functionality of legacy HR systems as many are not functional or require workarounds. IPPS-A Release 3 entered LUT Phase 1 with 55 severity-2 software deficiencies. Upon completion of LUT Phase 1, an additional 9 were identified, resulting in 64 severity-2 software deficiencies remained with 83 test problem reports to be adjudicated. An evaluation of operational effectiveness will be determined upon completion of LUT Phase 2.

» SUITABILITY

IPPS-A Release 3 has many capabilities that require workarounds to accomplish necessary tasks. An evaluation of operational suitability will be determined upon completion of LUT Phase 2.

» SURVIVABILITY

The cooperative vulnerability and penetration assessment completed during LUT Phase I demonstrated that the cyber survivability posture of the system has improved since IPPS-A Release 2. No high risk findings were identified during the cooperative vulnerability and penetration assessment. An evaluation of operational survivability will be determined upon completion of LUT Phase 2.

RECOMMENDATIONS

The Army should:

1. Resolve all IPPS-A Release 3 software deficiencies that do not have viable, user-approved workarounds prior to deploying the IPPS-A Release 3 software.
2. Complete cyber survivability testing of IPPS-A Release 3 to include an AA and verification of fixes (if required) in FY23.

Integrated Visual Augmentation System (IVAS)

The Army conducted an Operational Demonstration (Ops Demo) in May - June 2022 to support a production and rapid fielding decision. The Integrated Visual Augmentation System (IVAS) 1.0 did not demonstrate improvements to deficiencies identified during previous IVAS Capability Set (CS) 4 testing. Based on results of the Operational Demonstration (Ops Demo), the Army is adjusting the IVAS acquisition and fielding strategy. The IVAS 1.2 variant will be the full-rate production system, incorporating an improved form factor within 24 months.

SYSTEM DESCRIPTION

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

MISSION

The Army intends close combat infantry forces to employ IVAS during day (optional) and night missions to increase warfighter lethality through improved mobility, situational awareness, and marksmanship by providing the ability to train, rehearse, and fight on a single system.

Squads will train with IVAS in the Squad Immersive Virtual Trainer in a high fidelity, live and mixed reality, immersive environment, enabling rapid conduct and repetition of training scenarios.

PROGRAM

IVAS is a Middle Tier of Acquisition program in the rapid prototyping and fielding phases, intended to equip over 100,000 close combat soldiers. The rapid prototyping program used an iterative approach of four CSs. In December 2020, after the completion of CS 3 testing, the USD(A&S) approved the IVAS program to transition from rapid prototyping to rapid fielding, authorizing the Army to procure up to 10,000 CS 4 systems. The Army established IVAS as a Middle Tier of Acquisition rapid fielding program. USD(A&S) required the Army to fix problems noted during CS 3 testing and verify corrections prior to Ops Demo and CS 4 fielding.

The Army intended IVAS CS 4 to be a production-ready system addressing CS 3 deficiencies. Microsoft and the Army made changes to IVAS CS 4 and tested CS 4 Engineering Version (EV) 1 at Soldier Touchpoint (STP) 4 in April 2021 and CS 4 EV 2 at User Jury 4.3 in July 2021. Based on the results from STP 4 and User Jury 4.3, the Army delayed the IVAS Ops Demo from September 2021 until May-June 2022, to allow time for the IVAS program to correct deficiencies. The Army conducted STP 5 in March 2022 with CS 4 EV 3 and the Ops Demo with IVAS 1.0 to inform a fielding decision. DOT&E approved the IVAS T&E strategy in May 2022.

Based on results of the Ops Demo, the Army is adjusting the IVAS acquisition and fielding strategy. The updated acquisition strategy provides time for the Program Office and Microsoft to grow reliability, improve low-light performance, and develop a new form factor. The Army intends to field 5,000 IVAS 1.0 systems with improved reliability and 5,000 IVAS 1.1 systems that meet the reliability requirement and are equipped with an improved low-light sensor. The IVAS 1.2 variant will be the full-rate production system, incorporating an improved form factor within 24 months.

» MAJOR CONTRACTOR

- Microsoft Corp., – Redmond, Washington

TEST ADEQUACY

The IVAS Program Manager, with support from Army Test and Evaluation Command, conducted STP 5 with IVAS CS 4 EV 3 in March 2022 at Fort Bragg, North Carolina to validate performance and reliability improvements. STP 5 did not have a DOT&E-approved test plan, but was observed by DOT&E. STP 5 was adequate to support an assessment of military utility, user acceptance, human factors, training, and reliability of CS 4 EV 3.

The Army conducted the Ops Demo with IVAS 1.0 in June 2022 at Fort Bragg, North Carolina in accordance with the DOT&E-approved test plan, and was observed by DOT&E. The Ops

Demo was adequate to assess operational performance, military utility, user acceptance, reliability, and cyber and electronic warfare vulnerabilities. Testing included two 72-hour company-level missions with soldiers equipped with the IVAS, one 72-hour company-level mission with soldiers equipped with their current equipment, and three live fire ranges. The live fire ranges consisted of an individual static qualification, buddy team maneuvering, and squad maneuvering live fire iterations. Soldiers executed all three ranges in both daytime and nighttime with IVAS and with their current equipment.

PERFORMANCE

» EFFECTIVENESS

IVAS CS 4 EV 3 did not demonstrate improvements to deficiencies identified during STP 3 or STP 4. DOT&E recommended improvements to FWS-I integration, low-light sensors, HUD display, and field of vision. IVAS CS 4 EV 3 changes focused on improvement to the HUD display quality. Display quality improvement was variable between systems and did not translate into increases in soldier satisfaction with sensors or with their ability to detect and recognize enemy forces. Performance results are detailed in the IVAS CS4 EV 3 STP 5 report from June 2022.

In the Ops Demo, the infantry company was more successful accomplishing their operational missions with their current equipment than with IVAS 1.0. Soldiers hit fewer targets and engaged targets more slowly with IVAS 1.0 than with their current equipment on the buddy team life fire range. IVAS 1.0 did not demonstrate improvements in low-light sensors, HUD display, FWS-I integration and field of vision identified during previous IVAS CS 4 testing. IVAS 1.0 performance is detailed in the IVAS 1.0 Ops Demo report published October 2022.

» SUITABILITY

IVAS CS4 EV 3 demonstrated its requirement for mean time between system abort (MTBSA) during STP 5. Suitability results are detailed in the IVAS CS4 EV 3 STP 5 report.

The results of the Ops Demo show user acceptance remains low. Soldiers prefer their current equipment (Nett Warrior and PVS-14 and Enhanced Night Vision Goggle-Binocular night vision devices) to IVAS. The majority of soldiers reported at least one symptom of physical impairment to include disorientation, dizziness, eyestrain, headaches, motion sickness and nausea, neck strain and tunnel vision. Soldiers cited IVAS 1.0's poor low-light performance, display quality, cumbersomeness, poor reliability, inability to distinguish friend from foe, difficulty shooting, physical impairments and limited peripheral vision as reasons for their dissatisfaction. IVAS 1.0 MTBSA reliability metric declined during Ops Demo compared to IVAS CS4 EV2 in STP 4. Although the results were less favorable than STP 5, MTBSA is improving. Results for mean time between essential function failures have not improved between CS4 EV2, CS4 EV3 and 1.0. Suitability results are detailed in the IVAS 1.0 Ops Demo report published October 2022.

» SURVIVABILITY

IVAS 1.0 vulnerabilities in a cyber-contested and electromagnetic spectrum environment are detailed in the classified survivability annex to the IVAS 1.0 Ops Demo report published October 2022.

RECOMMENDATIONS

The Army should:

1. Correct the deficiencies identified in the Ops Demo and verify the corrections in developmental testing/operational testing prior to further operational testing to reduce resources and ensure better operational test results.
2. Revise the T&E strategy to support an assessment of performance for IVAS 1.1 and 1.2.

Javelin Antitank Missile System – Medium

Javelin is undergoing two separate, complementary upgrades the Army intends to control unit cost, reduce size and weight, and address component obsolescence while meeting or exceeding the current system performance. The Light Weight Command Launch Unit (LW CLU) is on track to undergo Operational Testing (OT) in FY23. The G-model missile will begin government-led flight testing in FY23.

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.

Javelin is undergoing two separate, complementary upgrades intended to control unit cost, reduce size and weight, and address component obsolescence while meeting or exceeding the current system 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 will be backward compatible with prior missile models and the G-model missile will be backward compatible with the current (Block 1) CLU.

The Army is developing a new Basic Skills Trainer and the Javelin Outdoor Trainer to be compatible with the upgraded Javelin.

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. IOT&E will inform the LW CLU Full-Rate Production decision planned in 2QFY24. The G-model missile will continue development and testing over the next 3 years and begin production upon the completion of a successful government qualification flight test series. DOT&E approved an updated test and evaluation master plan (TEMP) for the Javelin program in April 2020.

» MAJOR CONTRACTORS

- Raytheon Missiles & Defense – Tucson, Arizona
- Lockheed Martin – Orlando, Florida

TEST ADEQUACY

The Javelin TEMP describes extensive developmental, integrated, and operational testing to determine operational effectiveness, suitability, and survivability. Operational testing focuses on determining whether a unit equipped with the upgraded Javelin is more effective at identifying and engaging targets in various climate and terrain types while being lighter and more compact than the current Javelin.

The Army executed a cooperative vulnerability and penetration assessment (CVPA) of Javelin from August 31 to September 3, 2021. The CVPA was conducted in accordance with a DOT&E-approved test plan and was observed by DOT&E personnel. Future cybersecurity testing includes a follow-on CVPA in 2QFY23 on the Basic Skills Trainer and the operationally configured software loader hardware, a Javelin Adversarial Assessment (AA) in 4QFY23, and a CVPA in 4QFY23 and AA in 2QFY24 on the Javelin Outdoor Trainer.

The Javelin Project Office conducted a LW CLU Detection, Recognition & Identification (DRI) and Dirty Battlefield (DBF) demonstration with Soldiers and Marines from January – February, 2022 at Redstone Arsenal, Alabama. The purpose of the demonstration was to compare the ability of gunners to detect, recognize, and identify threat vehicles at various ranges using the Block 1 CLU and LW CLU. The Army will use the DRI-DBF demonstration and other DT results to assess LW CLU maturity prior to entering operational testing.

G-model missile flight testing began in FY22 in accordance with the DOT&E-approved TEMP. DOT&E personnel will observe select flight tests.

Army Test and Evaluation Command will execute OT at two locations: The Cold Region Test Center, Ft. Greely, Alaska in 2QFY23 and Yuma Proving Grounds, Arizona in 4QFY23. These tests are planned to be conducted in accordance with DOT&E-approved test plans. Due to some divergence of the LW CLU and G-model missile development schedules, these OTs will not include the G-model missile. A follow-on test will be required.

PERFORMANCE

» EFFECTIVENESS

Initial observations of the DRI-DRB demonstration indicate that the better camera resolution and higher zoom capability of the LW CLU makes detecting, recognizing, and identifying threat vehicles quicker and possible at longer ranges when compared with the Block 1 CLU.

Live Fire testing to date indicates that the new Javelin seeker does not reduce the effectiveness of the Javelin warhead that was demonstrated in F-model missile live fire test and evaluation.

» SUITABILITY

Feedback on the LW CLU has been positive. Gunners prefer the improved camera resolution and the smaller, lighter form factor. DT testing to date indicates that the LW CLU is on track to meet its reliability requirement.

The G-model missile experienced a failure during a contractor led confidence flight test. Flight testing has been halted, and the failure is under investigation as of this writing. A reliability estimate is not available at this time.

» SURVIVABILITY

The Army executed a CVPA of Javelin LW CLU and G-model missile August 31 to September 3, 2021 and reported four classified findings. Results of the CVPA will be used to inform the upcoming Javelin AA.

RECOMMENDATIONS

The Army should:

1. Develop a T&E concept for FOT&E that combines both the LW CLU and G-model missile.
2. Develop a T&E concept for demonstrating the new maximum effective range of the upgraded Javelin.

Joint Air-to-Ground Missile (JAGM)

The Joint Air-to-Ground Missile (JAGM) has completed operational and live fire testing. Operational and live fire testing was adequate to support a Full-Rate Production decision. A combined IOT&E and LFT&E report of test findings was published July 12, 2022. The JAGM exceeded key performance parameter hit requirements during operational testing. The Army used modeling and simulation to augment missile flight testing and optimize the overall test program.

SYSTEM DESCRIPTION

The JAGM is a precision munition that combines two sensor technologies – a semi active laser and a millimeter-wave radar – into a single seeker and guidance system while leveraging the warhead, motor, and flight control systems from the Helicopter Launched Fire-and-Forget (HELLFIRE) Romeo missile. Army and Marine Corps commanders will employ the JAGM from helicopters to engage enemy combatants in stationary and moving armored and unarmored vehicles, within building and bunker structures, in small boats, and in the open.

MISSION

Army AH-64E Apache and Marine Corps AH-1Z Viper aircrews will employ the JAGM for the destruction of high-value stationary, moving, and relocatable land and maritime targets from standoff range in day, night, adverse weather, and obscured battlefield conditions. Crews will utilize the JAGM to engage heavy and light armored vehicles; small boats; and personnel in buildings, in bunkers, and in the open.

PROGRAM

The JAGM is an Acquisition Category IC joint program led by the Army's Program Executive Office, Missile and Space and is executed in conjunction with the Navy's Program Executive Office, Unmanned Aviation and Strike Weapons. DOT&E approved the updated Test and Evaluation Master Plan on August 30, 2022. The Army completed the first phase of IOT&E in 3QFY20 and the Navy completed the second phase in 2QFY22. A combined IOT&E and LFT&E report of test findings was published July 12, 2022. The Army conducted a Full-Rate Production decision review in 4QFY22.

» MAJOR CONTRACTOR

- Lockheed Martin Corp. – Orlando, Florida

TEST ADEQUACY

The Army completed the first phase of IOT&E using AH-64E Apache helicopters from March 25 to May 10, 2019. DOT&E published an Operational Assessment in September 2020. The Navy completed the second phase of IOT&E using AH-1Z Viper attack helicopters in 2QFY22. The Navy flight testing included maritime targets at Eglin Air Force Base, Florida and ground targets at Yuma Proving Ground, Arizona from November 1 to December 17, 2021. Flight testing was supported by additional LFT&E, cybersecurity assessments, and developmental and integrated testing. Testing was adequate to evaluate the operational performance of JAGM when employed from the AH-64E and AH-1Z attack helicopters. Operational testing was conducted in accordance with the DOT&E-approved test plan and under DOT&E observation.

PERFORMANCE

» EFFECTIVENESS

The JAGM is operationally effective when employed from the AH-64E and AH-1Z, exceeding key performance parameter hit requirements. JAGM offers pilots increased tactical flexibility to overcome countermeasures or environmental restrictions compared to the HELLFIRE Romeo and the Longbow HELLFIRE missiles it is intended to replace. Effectiveness is reduced under high pilot workloads or in time-constrained conditions when employed from the AH-1Z due to interoperability deficiencies and a cumbersome pilot-vehicle interface (PVI). Deficiencies and PVI issues extended engagement times, caused preflight aborts, and caused AH-1Z pilots to miss one target out of 15 engagements.

The JAGM is lethal when employed from the AH-64E and AH-1Z and is at least as lethal as the HELLFIRE Romeo. Height-of-burst lethality could be improved with system refinements. Lethality against tanks with an active protection system requires additional testing and analysis to refine tactics, techniques, and procedures (TTPs).

The Army effectively utilized modeling and simulation, indicating that JAGM exceeds key performance parameter hit requirements across its operational envelope. Confidence in modeling is informed by thousands of agreements between actual missile performance and pre-shot predictions of trajectory, missile functionality, missile logic, arrival times, hit points, velocity vectors, and responses to changes in environment and target behavior.

» SUITABILITY

The JAGM is operationally suitable when employed from the AH-64E Apache but not when employed from the AH-1Z Viper due to shortcomings in aircraft-missile interoperability and the PVI. AH-1Z testing identified over 60 deficiencies, leading to high pilot workload and challenges using the PVI to conduct engagements. The JAGM itself demonstrated high preflight and inflight reliability, exceeding reliability requirements.

» SURVIVABILITY

JAGM is survivable against a nascent or limited cyber attacker. JAGM is not survivable against a moderate-to-advanced capability threat. The Army mitigated key vulnerabilities found in two cyber test events conducted in 2017. The most recent Navy testing revealed additional vulnerabilities.

RECOMMENDATIONS

The Joint Program Manager and Navy should:

1. Continue development and integration testing to correct AH-1Z deficiencies, and conduct follow-on testing to verify that they have been adequately addressed.
2. Develop an efficient PVI on the AH-1Z to reduce excessive pilot workloads.
3. Continue development and integration testing of the JAGM Captive Aircrew Training Missile while developing unique TTPs to ensure aircrew effectiveness.
4. Conduct additional tests to refine height-of-burst lethality.
5. Develop TTPs to effectively engage tanks equipped with active protection systems.

JAGM Test at Marine Corps Air Station Yuma, Arizona, December 2021

Joint Assault Bridge (JAB)

The Army redesigned several sub-systems and armor kits to mitigate vulnerabilities found in earlier live fire testing. The improvements do increase vehicle survivability over the previous design. The Joint Assault Bridge (JAB) mission-essential equipment is not survivable in a contested environment.

SYSTEM DESCRIPTION

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

MISSION

Commanders employ JAB to enable the ABCT to close with and destroy the enemy by fires and maneuvering freely over natural and man-made obstacles on the battlefield.

PROGRAM

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

2022 to build in the redesign and upgraded armor kits.

» MAJOR CONTRACTOR

- DRS Sustainment Systems Inc. – Bridgeton, Missouri

TEST ADEQUACY

Based on the vulnerabilities discovered during the LFT&E conducted from November 2017 to March 2018, the Army redesigned several sub-systems and added or upgraded armor kits to reduce the JAB's vulnerability to direct and indirect fires.

The Army conducted follow-on live fire testing from October 2021 to November 2021 at Aberdeen Test Center in Maryland to assess those improvements. Testing was adequate to evaluate the survivability of JAB against kinetic threats. The test was conducted in accordance with the DOT&E-approved test plan and DOT&E observed the test.

PERFORMANCE

» EFFECTIVENESS

The Army did not conduct any test events in FY22 to change the assessment of it being operationally effective.

» SUITABILITY

The Army did not conduct any test events in FY22 to change the assessment of it being operationally suitable.

» SURVIVABILITY

The JAB mission-essential equipment is not survivable in a contested environment. The sub-systems' redesign and additional armor to the JAB improve vehicle survivability over the previous design by reducing the sub-systems' exposed areas. The unit equipped with JAB may not be able to complete the mission after engagements with direct and indirect fire due to a loss or degradation of bridging capability.

The JAB crew will need maintenance support to conduct Battle Damage Assessment and Repair/Recovery (BDAR/R) to make the JAB mission-capable. The crew and maintainer, using the BDAR/R kit, could restore mission-essential equipment to operate at less-than-full mission capability. The JAB's weight exceeds the current heavy-duty tow bar and the tow provision lug-eyes' limits, which may impact safe vehicle recovery.

RECOMMENDATIONS

The Army should:

1. Improve tow provision lug-eyes to meet established weight requirements for the vehicle.
2. Provide the crew with BDAR/R solutions to restore full bridging capability.
3. Refine the armor coverings and attachments to make them easier for the crew to remove and operate.

Limited Interim Missile Warning System (LIMWS)

The Army's Limited Interim Missile Warning System (LIMWS) Quick Reaction Capability (QRC) testing demonstrated sufficient system effectiveness to support operations. Due to limited test data, suitability results are inconclusive. Based on the limited data thus far, the system is reliable, assuming mission durations based upon the Army's rotary wing operational mode/summary mission profile. Testing demonstrated LIMWS is survivable in a cyber-contested environment.

SYSTEM DESCRIPTION

LIMWS provides both infrared (IR)-guided missile warning and hostile fire indications for Army rotorcraft. LIMWS can cue the ALE-47 Improved Countermeasure Dispenser and the Common Infrared Countermeasure system to counter incoming IR-guided threats through flare dispenses and IR jamming respectively. LIMWS is a form-fit replacement for the Common Missile Warning System, which operates in the ultraviolet (UV) spectrum. Because LIMWS operates in the IR spectrum, it has performance advantages over a UV missile warning system. This improves missile warning declaration abilities and thus improves countermeasure effectiveness. LIMWS is composed of multiple imaging two-color IR sensors, a system processor, and a removable data module.

MISSION

Commanders employ Army rotorcraft equipped with LIMWS to conduct air assaults, air movements, casualty evacuation, attack, armed escort, reconnaissance, and security operations. During Army missions, LIMWS is intended to provide threat information to the aircrew and threat protection systems for rotary-wing aircraft against shoulder-fired and vehicle-launched IR surface-to-air missiles.

PROGRAM

The Army released a directed requirement for LIMWS. The specific details outlining the requirement are classified. The Army conducted test planning and execution as a QRC.

» MAJOR CONTRACTOR

- BAE Systems Information and Electronic Systems Integration – Nashua, New Hampshire

TEST ADEQUACY

The Army's QRC testing for LIMWS concluded in 3QFY22 and deviated from the original Army-approved test plan. The Army reduced the scope of the test matrices to shorten the duration of the test. DOT&E observed testing that generated test data from hardware-in-the-loop test results based on actual missile-to-warner-to-countermeasure handoff timelines measured during flight, along with performance data generated from flight tests in an operationally representative environment. In both cases, data supported assessing timely detection, countermeasure response, accurate reporting to aircrew of threats, and the false alarm rate. Testers coupled these data with data collected from free-flight missile tests using real missiles to evaluate system-of-system performance.

Testing to date has not generated adequate data to support a suitability assessment. Most of the suitability data are associated with reliability that came from flight hours on UH-60 and HH-60 platforms providing a single reliability measurement with limited confidence due to the limited number of flight hours.

The Army Test and Evaluation Command conducted cooperative vulnerability and penetration assessment testing, in collaboration with the Combat Capabilities Development Command Data and Analysis Center, in 2QFY21. Additionally, Army Test and Evaluation Command, supported by the Threat Systems Management Office, conducted an adversarial assessment in 2QFY21at Redstone Test Center, Alabama. Cyber survivability testing for LIMWS followed the DOT&E-approved test plans and included both Ethernet-based and Military Standard 1553 bus testing.

PERFORMANCE

» EFFECTIVENESS

LIMWS effectiveness was sufficient to support operations. Specific details are documented in DOT&E's classified LIMWS Interim Report of May 2022.

» SUITABILITY

Due to limited data, suitability results are inconclusive. The Army will need to continue to collect suitability data to assess the suitability of the system with confidence. Most suitability data are associated with reliability in which the system is reliable, assuming mission durations based upon the Army's rotary wing Operational Mode/Summary Mission Profiles. There were no reported safety issues for LIMWS during testing.

» SURVIVABILITY

Testing demonstrated LIMWS is survivable in a cyber-contested environment.

RECOMMENDATIONS

The Army should:

1. Continue collecting data to evaluate system suitability and make system and/or training modifications as necessary.
2. Address the recommendations documented in the classified DOT&E Interim Report.

Mobile Protected Firepower (MPF)

The Army completed the Middle Tier of Acquisition (MTA) phase for the Mobile Protected Firepower (MPF) and transitioned to a Major Capability Acquisition program at Milestone C in June 2022. The MTA phase included two vendors: BAE Systems and General Dynamics Land Systems (GDLS). The Army selected the GDLS design in June 2022 to support low-rate initial production. The MPF demonstrated satisfactory progress toward achieving operational effectiveness, reliability, and availability to support infantry brigade operations. The Army is working to correct vulnerabilities to threats discovered during the MTA phase. Due to the immaturity of the prototype, cyber survivability testing was conducted during developmental testing, but not operational testing. It will be evaluated during operational testing in support of the Full-Rate Production decision in 2QFY25.

SYSTEM DESCRIPTION

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

MISSION

BCTs will employ the MPF across a range of military operations, including forced and early entry operations in high Anti-Access/Area Denial environments, in direct support of infantry squads, platoons, and companies. The purpose of MPF is to engage and neutralize enemy personnel, bunkers, machine gun positions, fortifications, and strongpoints, as well as defeat light armored threats.

PROGRAM

MPF is now an Acquisition Category IB program of record following Milestone C. The Army completed the MTA phase for the MPF and entered Milestone C in June 2022. The MTA phase included two vendors: BAE Systems and GDLS. The Army selected the GDLS design in June 2022 to support low-rate initial production. DOT&E approved the MPF Milestone C Test and Evaluation Master Plan in May 2022.

» MAJOR CONTRACTOR

- General Dynamics Land Systems – Sterling Heights, Michigan

TEST ADEQUACY

During the MTA phase the Army Test and Evaluation Command conducted the Limited User Test from September 15 to November 3, 2021. Operational testing was conducted in accordance with DOT&E-approved test plans and was adequate to inform the Milestone C in June 2022. DOT&E observed the test and published an Operational Assessment Report in April 2022.

The Army Test and Evaluation Command conducted Live Fire testing from March 2019 to December 2021 in accordance with DOT&E-approved test plans, and observed by DOT&E. The MTA live fire events were sufficient to inform the survivability and force protection considerations for vendor down-select. Each contractor provided armor coupons and two ballistic hull and turret structures for live fire survivability testing. The Army's LFT&E program included: (1) armor coupon testing to assess performance of armor recipes against penetration from operationally relevant threats; (2) exploitation testing to evaluate integrated armor solutions and determine if welds, seams, bolts, hatches, and doors are vulnerable to penetration from direct and indirect fire threats; and (3) ballistic, hull, and turret testing to evaluate structural response to required threats. A classified LFT&E annex was included in the DOT&E Operational Assessment Report published in April 2022.

PERFORMANCE

» EFFECTIVENESS

The MPF's progress toward achieving operational effectiveness is satisfactory. Risk to achieving operational effectiveness include: minimizing the MPF's audible signature, improving compatibility of MPF and infantry target designators to allow sharing of target information, and improving the usability of the intercom system. The companies equipped with the MPF accomplished their missions more consistently than a unit without MPF support and took fewer casualties during force-on-force operations. During gunnery, the MPF crews qualified on gunnery tables developed for the MPF. The MPF platoon was able to communicate with the supported infantry unit, and their high-powered radios provided additional communications capability to the dismounted infantry soldiers.

» SUITABILITY

Vehicle reliability and availability support infantry brigade operations. The MPF shares many fire control components with the Abrams tank. The similarity in turrets will allow MPF crews to train on existing Abrams simulators, and reduces the vehicle-specific training that maintainers will need to support the MPF. Developmental testing found that the MPF had high levels of toxic fumes when firing the main gun, requiring modifications to crew procedures during gunnery to mitigate the build-up of fumes in the turret.

» SURVIVABILITY

Live Fire testing using operationally realistic threats revealed vulnerabilities. Details, including threat descriptions and survivability performance, can be found in the classified LFT&E annex to the DOT&E Operational Assessment Report published in April 2022. The classified annex assesses test adequacy and platform survivability of the MPF when exposed to relevant threats. The Army is implementing the survivability recommendations identified in the classified annex for GDLS. The Army will begin lethality and live fire testing of GDLS-produced low-rate initial production-representative vehicles in FY23.

RECOMMENDATIONS

The Army should:

1. Continue implementing system design fixes to reduce the high levels of toxic fumes when firing the main gun.
2. Continue improving the vehicle's cooling system to reduce preventive maintenance checks and services time required.
3. Continue addressing the survivability recommendations highlighted in the classified annex found in the DOT&E Operational Assessment Report published in April 2022.
4. Improve Real-Time Casualty Assessment capabilities to replicate target effects against non-vehicle targets such as bunkers and walls to improve combat realism and training value.

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

Left: GEN II MAPS Navigation Receiver | Right: GEN II Anti-Jam Antenna System

The Mounted Assured, Positioning, Navigation, and Timing System (MAPS) performed better than legacy Positioning, Navigation, and Timing (PNT) systems in GPS-degraded or denied environments during the 4QFY21 Limited User Test (LUT). The MAPS Generation (GEN) II program continued with developmental testing in FY22. MAPS transitioned from prototyping under an Other Transaction Authority contract to an Acquisition Category II program of record at Milestone C in June 2022.

SYSTEM DESCRIPTION

The GEN II MAPS will replace the legacy Defense Advanced GPS Receiver (DAGR) GPS receivers and antennas in a subset of the Army's ground vehicles. MAPS GEN II has non-GPS augmentation technologies and an anti-jam antenna allowing limited functionality of position and time accuracy in a GPS-contested environment. MAPS incorporates the new Military Code GPS satellite signal which is more resistant to jamming and spoofing than the current GPS signal used by the military.

MISSION

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

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

PROGRAM

In 2019, the Army Futures Command issued a directed requirement for the PNT Program Manager to conduct a technical assessment of the MAPS GEN II capability to inform requirements and follow-on programs of record. The Commanding General, Army Futures Command approved the MAPS Capabilities Development Document in September 2020. The Army intends MAPS GEN II to replace existing GPS receivers and antennas in a subset Army ground vehicle variants. Following competition between three vendors, the Army selected Collins Aerospace to provide the MAPS GEN II solution.

MAPS GEN II entered program of record status at Milestone C as an Acquisition Category II, Major Capability Acquisition program in June 2022. DOT&E approved the MAPS Milestone C Test and Evaluation Master Plan (TEMP) in April 2022.

» MAJOR CONTRACTOR

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

TEST ADEQUACY

The Army conducted the MAPS LUT in September 2021 in accordance with a DOT&E-approved test plan, and observed by DOT&E. The LUT was adequate to assess the performance of MAPS GEN II and the DOT&E MAPS LUT report informed the Army's decision to transition to an Acquisition Category II program of record at Milestone C.

Developmental testing of MAPS is ongoing as outlined in the MAPS TEMP. During May-June 2022, Army Test and Evaluation Command conducted environmental, electromagnetic interference, software safety, and acoustic noise testing at the Army's Electronic Proving Ground, Fort Huachuca, Arizona. Analyses of the developmental test data is ongoing by the Army.

The Army has addressed a DOT&E recommendation from the 2021 Annual Report and has found a suitable location to conduct IOT&E in 4QFY23 in accordance with the DOT&E-approved test plan.

PERFORMANCE

» EFFECTIVENESS

A unit equipped with MAPS demonstrated the ability to conduct reconnaissance and casualty evacuation missions in most contested GPS environments during the LUT. The MAPS improved situational awareness, assisted individuals and units with navigation, and allowed the unit to maintain tempo while moving to various objectives in contested GPS environments. The classified MAPS LUT report published in February 2022 provides details on system and unit performance.

» SUITABILITY

The MAPS demonstrated an operational availability exceeding the requirement. Training was sufficient for soldiers to operate MAPS. The classified MAPS LUT report provides details on operational suitability.

» SURVIVABILITY

An adversarial cybersecurity developmental test was conducted during the MAPS LUT. The results can be found in the classified MAPS LUT report. The Army plans to conduct an adversarial assessment in conjunction with the IOT&E in FY23.

RECOMMENDATION

The Army should:

1. Verify correction of system performance, suitability, and survivability deficiencies identified in the LUT prior to IOT&E.

Soldier Protection System (SPS)

The Army started fielding the Second Generation Modular Scalable Vest (MSV Gen II) and Third Generation Vital Torso Protection (VTP Gen III) hard armor plates in 4QFY21 and will field through 2QFY24. The Army completed First Article Testing (FAT) for multiple vendors for MSV Gen II, VTP Gen III (a combination of front/back and side plates), and Next Generation Integrated Head Protection System (NG-IHPS). The assessment of protection provided by VTP Gen III plates against non-standard threats, and comparison to legacy VTP plates, is not yet possible due to delays conducing expanded developmental testing.

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 protection equipment (PPE) at a reduced weight. The SPS is a modular system and provides soldiers the capability to configure the various components into different tiers of protection depending on the threat and their mission. The SPS subsystems are designed to protect a soldier's head, eyes, and neck region, the vital torso and upper torso areas (including the extremities), and the pelvic region. The SPS consists of three major subsystems shown on the following page.

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.

Soldier Protection Subsystems

PROGRAM

The SPS program is an Acquisition Category III program comprised of three major subsystems. Each of the three major subsystems are developed, tested, and fielded independently. The Army entered the Torso and Extremity Protection (TEP) full-rate production in September 2016, the IHPS in October 2018, and the VTP in December 2019. Each subsystem has follow-on engineering change proposal efforts:

- MSV Gen II is replacing the initial MSV in TEP
- VTP Gen III is replacing previous generations of VTP
- Next Generation IHPS is replacing IHPS

The Army is not planning a formal acquisition decision for the VTP Gen III, despite the significant design changes from VTP Gen II. The Army started early fielding of MSV Gen II and VTP Gen III plates in 4QFY21 to a select number of soldiers as authorized by the Army G8 on February 16, 2021. The target acquisition quantity is approximately 150,000 sets of each of the SPS subsystems.

» 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 (BCS)
- Carter Enterprises Industries Inc. – Brooklyn, New York (BCS)
- Eagle Industries Unlimited – Virginia Beach, Virginia (BCS)

VTP Vendors:

- Engense Armor Systems – Camarillo, California (ESBI)
- Florida Armor Group – Miami Lakes, Florida (ESBI)
- Leading Technology Composites – Wichita, Kansas (ESAPI, ESBI)

- TenCate Armor – Hebron, Ohio (ESAPI, XSBI)
- Avon Protection/Ceradyne – Irvine, California (XSAPI, ESAPI, XSBI)

NG IHPS Vendors:

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

TEST ADEQUACY

The Army completed FAT for multiple vendors to include: MSV, VTP (ESAPI and ESBI designs), and NG-IHPS. The designs that passed FAT proceeded to Lot Acceptance Testing. The Army completed all test series at Aberdeen Test Center, Maryland in accordance with DOT&E-approved test plans. DOT&E observed most of the FAT testing.

FAT consists of a series of non-ballistic and ballistic tests of a random sample of PPE from the first production lot, to ensure the effectiveness of the manufacturing process, equipment, and procedures. Lot Acceptance Testing (LAT) is similar to FAT, but is a reduced set of tests on a small random sample of subsequent PPE lots. LAT is used to ensure that the manufacturers continue to produce PPE in conformance with contract specifications. The Army has not yet begun an expanded developmental test series they proposed for 1QFY21 to compare legacy VTP and SPS VTP Gen III plates against fragmenting threats. The Army has delayed this test series until 1QFY23, prioritizing FAT and LAT testing. DOT&E approved the ballistic testing component of all test series (FAT, LAT, and expanded developmental test) in June 2021 and earlier.

The Army does not have the capability of assessing potential injuries to soldiers wearing body armor. In order to adequately assess soldier protection in the future, the Army must accredit the available Hybrid Foam Mannequin for evaluating penetrating injuries and model the body armor plates as a penetrable material.

PERFORMANCE

» SURVIVABILITY

All MSV Gen II designs tested met the ballistic FAT requirements. Five VTP designs (a combination of ESAPI and ESBI plates) were submitted for FAT in FY22; LAT is ongoing for the three designs that met the FAT ballistic requirements. Currently, there are no XSAPI Gen III designs that meet the ballistic FAT requirements. As of August 2022, over 150 LATs have been conducted with a failure rate of less than five percent. The assessment of protection provided by VTP Gen III plates against non-standard threats, and comparison to legacy VTP plates, is not yet possible due to delays conducting expanded developmental testing.

Two vendor designs completed FAT for NG-IHPS. One vendor failed to meet the ballistic test requirements. FAT failures for all commodities will necessitate a redesign of the ballistic layup, followed by retest.

RECOMMENDATIONS

The Army should:

1. Complete expanded developmental testing to enable the comparison of legacy VTP and SPS VTP Gen III plates against nonstandard threats.
2. Improve modeling and simulation capabilities so that penetration, threat breakup, and fragment behavior can be assessed on ceramic hard armor plates for a range of conditions not tested.
3. Reinitiate their efforts to accredit a mannequin as an evaluation tool for assessing injuries from penetrating threats in body armor testing.

Stryker Family of Vehicles (FoV)

Left: Stryker Common Remotely Operated Weapon Station – Javelin (CROWS-J) | Right: Stryker 30mm Medium Caliber Weapon System (MCWS)

The Army has not verified through testing that the issues identified in the November 2021 FOT&E report on the Stryker Common Remotely Operated Weapon Station – Javelin (CROWS-J) have been resolved. The Army should convene a failure review board, continue CROWS-J corrective actions, and evaluate unit performance in a subsequent FOT&E.

The Army plans to conduct FOT&E and LFT&E for Stryker 30mm Medium Caliber Weapon System (MCWS) in FY23.

SYSTEM DESCRIPTION

The Stryker CROWS-J and 30mm MCWS address lethality gaps in the existing Stryker Family of Vehicles (FoV). The CROWS-J lethality upgrade enables Stryker units to fire a Javelin Antitank Missile while under armor. The 30mm MCWS integrates the XM813 cannon (30x173mm) onto a Stryker Infantry Carrier Vehicle Double V Hull.

MISSION

Units equipped with the Stryker FoV provide Combatant Commands a medium-weight force, capable of rapid strategic and operational mobility to disrupt or destroy enemy military forces, control land areas including populations and resources, and conduct combat operations.

PROGRAM

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

The Army is currently fielding the CROWS-J under an Urgent Materiel Release and plans to field subsequent brigades under a Conditional Materiel Release, pending resolution of the issues identified in the November 2021 CROWS-J FOT&E report.

The Army executed a multi-vendor competition from August – December 2020 to select a design solution for the 30mm MCWS. The selected design from Oshkosh Defense is scheduled for FOT&E in May 2023. The Army intends to field the first unit under a Conditional Materiel Release, unless Stryker program delays require a change to an Urgent Materiel Release to meet the Army's Regionally Aligned Readiness and Modernization Model timeline.

» MAJOR CONTRACTORS

CROWS-J:

- Kongsberg Defense & Aerospace – Kongsberg, Norway (Primary System)
- Raytheon/Lockheed Martin JV– Tucson, Arizona (Components)
- General Dynamics Land Systems – Sterling Heights, Michigan (Integrator)

30mm MCWS:

- Oshkosh Defense, LLC – Oshkosh, Wisconsin

TEST ADEQUACY

DOT&E published an unclassified CROWS-J FOT&E report with a classified Survivability Annex in November 2021. At this time the Army does not have a plan to conduct a subsequent FOT&E to address the report's recommendations.

The Army plans to conduct FOT&E and LFT&E of the 30mm MCWS in FY23 to determine if a unit equipped with 30mm MCWS is operationally effective, suitable, and survivable. The Army will submit the FOT&E and LFT&E test plans to DOT&E for approval at which time DOT&E will determine test adequacy. DOT&E intends to publish a combined FOT&E and LFT&E report in 1QFY24 after testing is completed.

PERFORMANCE

There were no Stryker FoV test events in FY22.

RECOMMENDATIONS

The Army should:

1. Determine the cause of the issues identified in the November 2021 FOT&E report through a failure review board and address CROWS-J deficiencies identified during the operational and live fire assessments in FY21. A subsequent FOT&E of the CROWS-J should be conducted to verify the fixes.

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

The Stryker Nuclear Biological Chemical Reconnaissance Vehicle (NBCRV) Sensor Suite Upgrade (SSU) program is delivering capability in two phases referred to as Capability Sets (CS). The concept of operation and system design is focused on standoff sensing employing existing manned Stryker NBCRV flat bottom hull platforms with an upgraded suite of chemical, biological, and radiological sensors. The Stryker is teamed with a towed unmanned ground vehicle with the same sensor suite as the NBCRV and multiple small unmanned aerial vehicles that can be used for standoff biological sensing to expand the reconnaissance area. The Stryker NBCRV SSU CS 2.1 design is based on upgrading flat-bottom hull platforms that are less survivable to kinetic threats than Stryker Double V Hull platforms. The CS 2.1 design eliminates the existing NBCRV capability to detect and identify chemical agent on route surfaces, collect physical samples from within the collectively protected vehicle, and physically mark contaminated areas. The NBCRV SSU program has an aggressive test schedule with limited test articles. NBCRV SSU CS 2.1 component level testing conducted to date has identified individual sensor performance and reliability issues which should be fixed prior to integrated system developmental and operational testing. The program conducted a Soldier Touch Point in September 2022 to obtain soldier input for CS 2.2. The Army plans to conduct integrated developmental and operational testing and survivability testing of the CS 2.1 upgrade in FY23.

SYSTEM DESCRIPTION

The NBCRV SSU is a two phased program to develop and field upgrades to the Stryker NBCRV. The first phase, CS 2.1, will upgrade a limited number of existing Stryker NBCRV flat-bottom hull platforms with a new mission equipment package consisting of the Joint Chemical Agent Detector, Compact Standoff Detection Sensor, Improved Mobile Chemical Agent Detector (IMCAD), Merlin Applique and Imager radiological detectors, Viper radiological detector, and weather sensors mounted on the outside of the system. The NBCRV SSU will include a towed unmanned ground vehicle with a second mission equipment package and unmanned aerial vehicles (UAV) with interchangeable modular biological sensor package, and new servers and workstations.

MISSION

Army Armored Brigade Combat Teams (BCTs), Stryker BCTs, active Chemical Biological Radiological and Nuclear (CBRN) Hazard Response Companies, National Guard and Army Reserve BCT Hazard Response Company units equipped with the NBCRV SSU will provide point, standoff, and remote CBRN sensing capabilities to provide commanders 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. The Army intends units equipped with the NBCRV SSU to perform CBRN route, area, and zone reconnaissance on roads and cross-country; CBRN surveys to determine limits of contamination; and CBRN surveillance, as directed by the Maneuver Force Commander.

PROGRAM

The Stryker NBCRV SSU is a tailored Major Capability Acquisition (Acquisition Category III) effort to make engineering changes to the fielded M1135 Stryker NBCRVs and potentially to future Stryker Double V Hull platforms to improve survivability. The Army plans to apply the SSU as a Modification Work Order as directed by Tank-automotive and Armaments Command. The SSU effort is a phased effort with a Conditional Materiel Release in FY24 to field up to eight systems on existing NBCRV platforms. DOT&E approved the Test and Evaluation Master Plan for CS 2.1 on March 7, 2022.

» MAJOR CONTRACTORS

- FLIR Systems Inc. – Elkridge, Maryland

TEST ADEQUACY

DOT&E has repeatedly expressed concerns over the lack of sufficient sensors and NBCRV SSU integrated systems available for testing. These assets are needed to enable identification of system-to-system variability and operational testing of a unit equipped with the NBCRV SSU. The Program Office is working with the Army to develop backup plans should the two NBCRV SSU systems identified to support operational testing become non-mission capable. In FY22, DOT&E approved developmental/operational test plans for the NBCRV SSU component VIPER radiological detector, MERLIN radiological imager, Improved Mobile Chemical Agent Detector (IMCAD), and Biological Aerosol Detector. A small number of the planned test trials for the VIPER, MERLIN, and IMCAD were not completed due to limited time and other test facility commitments. The program is working to schedule follow-on testing to complete these trials. The Army Test and Evaluation Command conducted developmental testing of the UAV and Compact Standoff Detection System and the Joint Chemical Agent Detector components. DOT&E observed portions of the VIPER, MERLIN, and Biological Aerosol Sensor testing. Testing was conducted in accordance with the DOT&E-approved test plans. The Program Office conducted a NBCRV SSU Soldier Touch Point event in September 2022 which DOT&E observed.

PERFORMANCE

» EFFECTIVENESS

CS 2.1 eliminates the existing NBCRV capability to detect and identify surface samples on-the-move, safely collect samples from inside the collectively protected NBCRV for further laboratory analysis, and physically mark contaminated areas. The NBCRV SSU will have the capability to digitally mark contaminated areas using the Joint Battle Command-Platform but will lose the capability to mark areas to warn dismounted troops, allies using different digital mapping systems, and civilians. FY21 component testing of the Chemical Surface Detector identified performance deficiencies agent chamber testing and on-the-move simulant testing. The Program Manager has removed the Chemical Surface Detector from the CS 2.1 upgrade and plans to incorporate a different sensor for CS 2.2. FY22 radiological sensor component testing of the VIPER and MERLIN identified performance deficiencies that should be corrected and retested. The Program Office is working with the vendor to correct these deficiencies and plan regression testing prior to fielding.

» SUITABILITY

UAV flight characteristic testing identified battery deficiencies that limit flight time. The Program Office is working to identify solutions for CS 2.1.

» SURVIVABILITY

The NBCRV's flat-bottom hull platforms are less survivable to kinetic threats than Double V Hull platforms. Due to Army funding decisions and the Army's planned Conditional Material Release in FY24, the Program Office plans integrate the SSU onto existing M1135 NBCRV flat-bottom hull platforms instead of moving forward with a costlier and more time consuming engineering effort to integrate the CS 2.1 SSU onto Double V Hull platforms. The Army plans to conduct survivability testing of the CS 2.1 upgrade in FY23.

Laser vulnerability testing completed to date did not identify any survivability shortcomings in the NBCRV SSU UAV or IMCAD. Integrated NBCRV SSU system testing is planned in spring 2023.

RECOMMENDATIONS

The Program Office should:

1. Work with the UAV vendor to identify and test batteries for the UAV that provide sufficient power to enable the UAV to accomplish its mission.
2. Provide sufficient test articles to enable operational testing in accordance with the Army's concept of operation.

The Army should:

3. Consider conducting side-by-side operational testing of the NBCRV SSU with the currently fielded NBCRV system to demonstrate improved operational capability in support a procurement decision.
4. Identify and plan to integrate the SSU onto a more survivable platform to enable its employment in accordance with the proposed Army concept of operation. Testing should be repeated once the sensor suite upgrade is integrated onto a new platform to identify any changes to its operational effectiveness, suitability and survivability prior to fielding.

Terrain Shaping Obstacles (TSO)

The XM204 Interim Top Attack system will complete government testing in FY23 with an urgent materiel release (UMR) decision planned for late FY23. The Army intends XM204 to support the U.S. Army Europe (USAREUR) Operational Needs Statement (ONS) for an interim Top Attack (TA) anti-vehicle capability. The schedule-driven, compressed timeline of the XM204 system development resulted in an inadequate test strategy that does not support DOT&E's assessment of operational effectiveness and suitability across the operational environment.

SYSTEM DESCRIPTION

The XM204 is a U.S. landmine policy compliant, hand emplaced system that provides an interim TA anti-vehicle capability. The XM204 is designed to autonomously detect, track, and engage heavy and light tracked vehicles within its zone of authority when armed. It may be used as a standalone obstacle or be integrated with the XM343 Standoff Activated Volcano Obstacle (SAVO) to create a complex obstacle containing both top and bottom attack mines.

MISSION

The XM204 will provide Brigade Combat Teams and Engineer Brigades in a deliberate defense, the ability to create disrupt/fix or turn/block directed obstacles against enemy armored formations maneuvering across lightly vegetated, open, and rolling terrain. Directed obstacles are used by Brigade Combat Teams to slow the rate or alter the direction of advancing enemy armored formations.

PROGRAM

The Army intends the XM204 program to fulfill the interim TA capability required by USAREUR ONS 18-22702, which directed the acceleration of mature technology, development, and limited fielding of an interim Close Terrain Shaping Obstacle (CTSO) TA solution by 2023. The program plans to produce 500 units for USAREUR. The XM204 program does not have a defined acquisition pathway but is most aligned with the Urgent Capability Acquisition pathway. DOT&E will produce an Early Fielding Report to inform the Army UMR decision planned for late FY23, but will not be able to make an effectiveness and suitability determination due to the inadequate test strategy. There is a follow-on program of record known as CTSO Increment 1, which will become the Army's enduring TA capability.

DOT&E approved the XM204 Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan in July 2021, a Live Fire Test Design Plan in March 2022, an Adversarial Assessment (AA) Test Plan in April 2022, and an Operational Assessment (OA) Operational Test Plan in July 2022.

» MAJOR CONTRACTOR

- Textron Systems Corporation – Wilmington, Massachusetts

TEST ADEQUACY

The XM204 T&E strategy was constrained due to the Army's intent to reach initial operational capability by 4QFY23. The planned DT was not robust enough to support the modeling and simulation effort. The overall test strategy was not adequate to determine operational effectiveness and suitability across the expected operational environment to include various terrain types, weather conditions, and complex battlefield environments.

The majority of government-led DT and OT occurred in FY22 and all remaining testing is expected to be completed in FY23. This testing includes:

- A cyber CVPA in October 2021 and an AA in May 2022 conducted in accordance with DOT&E-approved test plans. Both were observed by DOT&E personnel.
- A third Soldier Touch Point conducted in January 2022.
- An OA in July and August 2022 conducted in accordance with a DOT&E-approved test plan and was observed by DOT&E personnel.
- Ongoing government-led System Verification Testing with planned completion in early FY23. System Verification Testing includes live warhead testing against light and heavy tracked vehicles and is being conducted in accordance with the DOT&E-approved Live Fire Test Design Plan.
- A DT series that will be completed in early FY23 to include Safety and Sequential Transportability, Adverse Environment, Electromagnetic Environment Effects, Explosive Ordnance Disposal, Final Hazard Classification, 1660 Pallet Unitization, XM343 SAVO initiation, and Self Destruct testing.

DOT&E will publish an XM204 early fielding report with classified annex to include an evaluation of completed operational and lethality testing in 2QFY23.

PERFORMANCE

» EFFECTIVENESS

Due to an abbreviated DT test program and limited number of full tactical system shots against realistic moving targets, the true hit performance and warhead lethality is difficult to estimate at this time. A final series of live shots against moving targets occurring in early FY23 will help support a more robust estimate.

Soldier feedback indicates that the training provided by the Army did not properly explain terrain conditions that may impact the performance of the XM204 sensors, resulting in soldiers emplacing the system in locations where it was not able to track enemy vehicles. Soldiers suggested that extending the firing range and having the ability to conceal the XM204 would improve its overall operational effectiveness.

» SUITABILITY

Contractor-led testing in FY21 identified several design and manufacturing issues and implemented fixes. Test articles that included these fixes were delivered to the Army in July of FY22 for government-led DT and the OA.

Government-led safety and sequential transportability testing resulted in several new failures that, as of this writing, are still under investigation. The XM204 does not appear to be on track to meet its reliability requirement.

Early results of the OA suggest that soldiers are able to transport and emplace the XM204 in open, lightly vegetated terrain under clear, hot weather conditions. They are able to quickly create point, gauntlet, and disrupt/fix directed obstacles per their Commander's intent. Soldiers are able to arm the system and egress to a safe distance within the safe separation time limits of the system.

» SURVIVABILITY

The Army Test and Evaluation Command conducted a CVPA and AA on the XM204. Results will be published in the classified annex to the early fielding report.

RECOMMENDATIONS

The Army should:

1. Address deficiencies found in the training materials to ensure that soldiers emplacing the XM204 understand the sensor limitations and avoid terrain features that would impact system performance.
2. Conduct DOT&E-approved follow-on testing in operationally realistic environments to support an effectiveness and suitability determination.

UH-60V Black Hawk Digital Cockpit

The Army completed IOT&E II on the UH-60V on August 8, 2022. Evaluation of test data is ongoing. Early observations from IOT&E II are positive. The Army addressed most of the faults and recommended corrective actions found during IOT&E I in 4QFY19.

SYSTEM DESCRIPTION

The UH-60V Black Hawk is designed to update the existing UH-60L analog architecture to a digital infrastructure enabling a Pilot-Vehicle Interface (PVI) similar to the UH-60M. The program will address current capability gaps while employing an evolutionary acquisition approach to leverage mature technologies that have been successfully integrated on other military aircraft, such as the FlightPro Gen III Mission Computer from the Marines H-1 program.

MISSION

Units equipped with UH-60V aircraft will conduct air assault, air movement, aerial command and control (C2), and aerial MEDEVAC missions. Garrison units equipped with the UH-60V will execute garrison support missions, training and training support, and test support. The UH-60V has two pilots assisted by two crew chiefs in the rear cabin. Aircraft and their crews are employed individually, in multi-ship formations, or as a company, as required by the unit mission.

PROGRAM

The UH-60V is an Acquisition Category II effort. The original Acquisition Program Baseline (APB) was approved in 2014 and with an APB revision in December 2020. DOT&E approved the updated Test and Evaluation Master Plan on October 27, 2021. The Army completed IOT&E II on August 8, 2022. The Army is anticipating a Full-Rate Production decision in 2QFY23.

» MAJOR CONTRACTORS

- Development and Engineering: Redstone Defense Systems – Huntsville, Alabama
- Avionics Enhancements: Northrup Grumman – Woodland Hills, California

TEST ADEQUACY

In 2019, the Army conducted IOT&E I, which was not adequate due to the software, hardware, and production process not being production representative. The Army completed an Adversarial Assessment on the UH-60V from 7-18 March 2022 at Redstone Arsenal, Huntsville, Alabama. It completed IOT&E II from July 25 to August 8, 2022 at Fort McCoy, Wisconsin to inform a future Full-Rate Production decision. Operational testing was conducted in accordance with the DOT&E-approved test plan, and observed by DOT&E. Evaluation of test data is ongoing.

PERFORMANCE

» EFFECTIVENESS

Assessment of the UH-60V operational effectiveness is pending completion of IOT&E II evaluation. Early observations indicate that the program has corrected many of the faults found during IOT&E I in 4QFY19. The IOT&E II report will be completed in 1QFY23.

» SUITABILITY

Assessment of the UH-60V suitability is pending completion of IOT&E II evaluation. Early observations indicate that the program has corrected many of the faults found during IOT&E I in 4QFY19. The IOT&E II report findings will be completed in 1QFY23.

» SURVIVABILITY

Assessment of the UH-60V survivability is pending completion of IOT&E II analysis. The IOT&E II report findings will be completed in 1QFY23.

RECOMMENDATION

The Program Manager should:

1. Address the recommendations that will be contained in the IOT&E II report.

DEPARTMENT OF THE NAVY PROGRAMS

Acoustic Rapid Commercial-off-the-Shelf Insertion (A-RCI)

The Navy commenced operational test (OT) of Acoustic Rapid Commercial-off-the-Shelf Insertion (A-RCI) for Sonar Advanced Processor Build (APB) 17 and APB 19 in 2022. The Navy partially completed an in-lab test of APB 17 and APB 19, but no at sea testing or cyber survivability evaluation. The availability of fleet assets for OT has not supported a timely evaluation of the submarine sonar system.

SYSTEM DESCRIPTION

The AN/BQQ-10 A-RCI sonar system is a collection of hardware and software components that control, process, and present acoustic information from sonar arrays, as well as environmental data, to fleet operators on all Navy submarines. Operators use the presented information to attain tactical control and situational awareness in all mission sets. The system, capable of employing both passive and active sonar, sends information on threat submarines and other waterborne objects (surface ships, mines, bottom features, etc.) to the AN/BYG-1 Combat Control system to further develop and refine position and velocity estimates for contacts.

MISSION

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

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

PROGRAM

The A-RCI system is an Acquisition Category III post-milestone C program. The Navy staggers updates to the software and hardware of the system biennially; software upgrades are released via APBs and hardware upgrades via Technical Insertions. DOT&E approved the A-RCI APB 17 and 19 combined Test and Evaluation Master Plan (TEMP) on March 10, 2022.

Installation of the Large Vertical Array (LVA), a newly developed hull-mounted sensor, on *Ohio*-class submarines began in 2021. The Navy intends to back-fit LVA on approximately half of the Block III and Block IV *Virginia*-class submarines over the next decade. DOT&E is working with the Navy to update the APB 17 and 19 combined TEMP for the T&E of A-RCI integrated with LVA.

» MAJOR CONTRACTOR

- Lockheed Martin Maritime Systems and Sensors – Manassas, Virginia

TEST ADEQUACY

In January 2022, the Navy commenced in-lab operator testing of APB 17 and APB 19 using the Naval Undersea Warfare Center facilities in Newport, Rhode Island, and Fall River, Massachusetts, in accordance with a DOT&E-approved test plan. DOT&E was present to observe this testing event. However, completion of the test was delayed due to connectivity issues between these facilities, primarily stemming from the Newport, Rhode Island facility.

In FY21, the Navy obtained data during a 2-day fleet exercise with an allied nation's diesel submarine. These data contribute to the assessment of APB 19 capability and its support of anti-submarine warfare.

In FY22, the Navy scheduled an OT of a submarine with APB 19 operating in an area with a high density of surface ships to evaluate the capability of APB 19 to provide the crew with situational awareness, and a focus area of APB improvement. However, the Navy canceled the event when the submarine identified a conflict with a higher priority requirement. The Navy plans to reschedule this event as soon as practicable.

In FY22, the Navy intended to execute an in-lab integrated cyber survivability testing period for APB 19 followed by on-hull testing. The Navy canceled the testing due to software readiness issues and now expects to test in FY23-24. APB 17 is not tested because changes with an effect on cyber survivability were only in APB 19.

The Navy is significantly delayed in testing the APB 17 and APB 19 capabilities that have been installed on submarines commencing in August 2019 and November 2020, respectively. The availability of fleet assets for OT has not supported a timely evaluation of the submarine sonar system.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Not enough data are available to provide preliminary assessments of APB 17 or APB 19 operational effectiveness, suitability, and survivability.

RECOMMENDATIONS

The Navy should:

1. Assess the integration of OT with fleet operations.
2. Complete OT of APB 17 and APB 19.
3. Complete an update to the A-RCI TEMP that includes the test strategy and resources to evaluate the integrated capability of A-RCI with LVA as installed on *Ohio*- and *Virginia*-class Block III/ Block IV submarines.
4. Improve connectivity and reliability of the A-RCI lab consoles at the Newport, Rhode Island facility.

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

The Navy conducted Two Advanced Anti-Radiation Guided Missile – Extended Range (AARGM-ER) developmental free-flight tests from F/A-18E/Fs in January 2022 (Developmental Test 2 (DT2)) and April 2022 (DT3). The AARGM-ER IOT&E is scheduled to begin in 3QFY23, following the final three DT shots (DT4, DT5 and DT6).

SYSTEM DESCRIPTION

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

MISSION

Aircrews will employ AARGM-ER to suppress and/or destroy enemy air defenses. The primary targets are relocatable, integrated air-defense radars and other targets that may utilize shutdown tactics. AARGM-ER counters enemy shutdown capability with the multi-mode seeker.

PROGRAM

AARGM-ER is an Acquisition Category IB program. DOT&E approved the AARGM-ER Milestone C Test and Evaluation Master Plan in May 2021, but required the Navy to submit an updated cybersecurity test strategy for DOT&E approval, which occurred in August 2022. The Navy held a Knowledge Point-4 program review in July 2021 that supported entry into the Production and Deployment phase and the award of the low-rate initial production contract. The AARGM-ER IOT&E is scheduled to begin in 3QFY23.

» MAJOR CONTRACTOR

- Alliant Techsystems Operations LLC, a subsidiary of Northrup Grumman Corporation – Northridge, California

TEST ADEQUACY

At the time of this report, the program has completed three of six developmental test shots (DT1 in FY21 and DT2-DT3 in FY22) intended to identify and fix problems prior to beginning integrated operational testing, in accordance with the DOT&E-approved Test and Evaluation Master Plan. The final three DT shots are anticipated in the first half FY23. All DT shots were launched from an F/A-18 at the Point Mugu Sea Range, California. After each test event, discrepancies were noted and fixes were implemented prior to the delivery of the Flight Test Vehicle for the next shot. The time necessary to analyze data, develop, and incorporate these fixes resulted in delays to Flight Test Vehicle delivery and the test schedule.

Additionally, the extended range and advanced capabilities of AARGM-ER exceed the capabilities of most test range infrastructure. As a result, range scheduling has been a challenge for the program, resulting in adjustments to the test plan and contributing further to schedule delays.

The program is using developmental test events to collect data for verification and validation (V&V) of modeling and simulation. The data collection plan assumes that the current model will successfully predict performance in future test events. If this assumption proves to be incorrect, additional test events, to include captive-carry events, may be required to complete V&V and accreditation.

The Navy conducted the first two AARGM-ER warhead arena ground testing events in the first half of FY22. Due to production delays, the remaining warhead arena test events were rescheduled for 1QFY23. DOT&E plans to observe select future test events, and will report on the adequacy of arena testing after receipt of data from all events.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Not enough data are currently available to provide a preliminary assessment of AARGM-ER operational effectiveness, suitability, or survivability.

RECOMMENDATIONS

The Navy should:

1. Consider scheduling additional captive-carry events prior to live-fire flight test events in order to discover discrepancies prior to flight test and increase data collection to V&V of modeling and simulation.
2. Coordinate with DOT&E and the Test Resource Management Center to ensure test range infrastructure limitations are addressed.

Aegis Modernization Program

In July 2022, the Navy conducted three Standard Missile 2 (SM-2) live fire events against adversary anti-ship cruise missile surrogates using the Capability Package 22-1 variant of the Aegis Combat System's Advanced Capability Build 16 (ACB 16). DOT&E expects to release an ACB 16 Early Fielding Report in 1QFY23 because the Navy intends to field Capability Package 22-1 ships before operational testing is complete. The Navy expects to complete the ACB 16 testing in FY24. DOT&E will issue a final ACB 16 report at the completion of all ACB 16 testing, but test adequacy is at risk because the program lacks an approved Test and Evaluation Master Plan (TEMP)

SYSTEM DESCRIPTION

The Aegis Combat System is an advanced weapon control system comprised of sensors, control elements, and weapons to detect, track, engage, and destroy adversary targets. The Aegis Combat System's key components include: 1) an Aegis Weapon System that includes the AN/SPY-1 three-dimensional multi-function radar; 2) a Phalanx Close-In Weapon System; 3) a 5-inch diameter gun system; 4) the Vertical Launch System that can launch Tomahawk missiles, SM-2, SM-3, and SM-6, Evolved Sea Sparrow Missiles, and Vertical Launch Anti-Submarine

Rockets; and 5) an AN/SQQ-89 undersea warfare suite, which also incorporates integration with the MH-60R helicopter. The Navy's Aegis Modernization Program updates the Aegis Weapon System to improve Aegis Combat System integration and capabilities on CG 47-class Aegis guided missile cruisers and DDG 51-class Aegis guided missile destroyers.

MISSION

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

- Area and self-defense anti-air warfare in defense of the strike group;
- Anti-surface warfare and anti-submarine warfare;
- Strike warfare, when armed with Tomahawk missiles;
- Integrated air and missile defense; and
- Operations independently or in concert with carrier or expeditionary strike groups and with other joint or coalition partners.

PROGRAM

The Aegis Modernization Program is not an acquisition program. The Navy has updated Aegis through quadrennial ACBs comprised of hardware and software modifications to improve capability. The latest upgrade is the ACB 16. The Navy intends four incremental deliveries within ACB 16: Baseline 9.2.0, Baseline 9.2.1, Baseline 9.2.2, and Capability Package 22-1 (previously referred to as Baseline 9.2.3). The evaluation of ACB 16 will be accomplished as a cumulative collection of operational test data from all baseline variants, with completion expected in FY24. The ACB 16 evaluation will inform deployment decisions and determine delivered capability for ACB 16 and its variants.

In coordination with DOT&E in FY19, the Navy developed an Aegis TEMP revision, which included the test strategy for the first three ACB 16 baselines, but the Navy never provided it for DOT&E approval. The Navy has subsequently updated the draft TEMP to incorporate an additional phase of development, Capability Package 22-1, but has not yet finalized or submitted the TEMP for DOT&E approval.

The Navy intends to deliver initial capability of the next Aegis ACB, ACB 20, in FY24 and in coordination with the DDG 51 Flight III ship's IOT&E. IOT&E will continue until at least FY27 due to the delayed ability of the Navy to test some capabilities, including integrated air and missile defense. The Navy, in coordination with DOT&E, developed a single TEMP describing the initial testing strategy for ACB 20 (Baseline 10), DDG 51 Flight III, and the Air and Missile Defense Radar (AN/SPY-6(V)1). DOT&E approved the combined TEMP on September 23, 2022. Another Aegis TEMP is planned to capture additional ACB 20 test events in FOT&E.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

In FY22, the Navy elected to add Capability Package 22-1, in which the Navy intends to resolve technical issues with certain hardware configurations and provide additional capabilities, to ACB 16. Capability Package 22-1 creates additional testing requirements and new combat-system-related deficiencies, such as operator training and documentation, have been observed.

In July 2022, the Navy conducted two integrated live SM-2 firing events against cruise missile surrogate targets using Capability Package 22-1 and a single SM-2 Block IIIC firing event to support the Block IIIC program using Capability Package 22-1. Testing also included Capability Package 22-1 tracking capability against aircraft employing electronic attack and against small boats. The test event against the small boats additionally exercised live fire of the integrated 5-inch diameter gun against the targets.

All testing was conducted in accordance with the DOT&E-approved test plans, and observed by DOT&E. The Navy intends to complete the remaining Capability Package 22-1 testing in FY23.

The Navy cancelled planned operational testing of Baseline 9.2.1 in FY20, due to the unavailability of the test ship, and plans to conduct operational testing on Baseline 9.2.1 in FY23 and FY24. The Navy intends to complete Baseline 9.2.2 testing in FY23.

The Navy has yet to schedule cyber survivability testing to include a cooperative vulnerability and penetration assessment and an adversarial assessment. Adequate test depends upon the completion of this cyber security evaluation, as well as the remaining operational tests for Baseline 9.2.1, 9.2.2, and the Capability Package 22-1. The lack of an approved TEMP risks the availability of required resources to execute the remaining test.

PERFORMANCE

» EFFECTIVENESS

The assessment of the Baseline 9.2.0 capability is summarized in a classified Early Fielding Report published in March 2020. Preliminary evaluation of Baseline 9.2.2 testing suggests anti-air and anti-surface warfare performance is consistent with legacy Aegis capability. Initial assessments of Baseline 9.2.2 and Capability Package 22-1 will be summarized in a classified Early Fielding Report in FY23. The determination of ACB-16 operational effectiveness of ACB 16 is expected in FY24 after completion of Baseline 9.2.1, 9.2.2, and Capability Package 22-1 testing, and will be published in an ACB 16 OT&E report.

» SUITABILITY

Not enough data are yet available to assess ACB 16 operational suitability. Preliminary analysis highlights reliability concerns with the Aegis Display System and the SPY-1 radar.

» SURVIVABILITY

Not enough data are yet available to assess cyber survivability of any baseline variant of ACB 16.

RECOMMENDATIONS

The Navy should:

1. Submit, for DOT&E approval, an ACB 16 TEMP that details an adequate test strategy and test resources to assess the operational effectiveness and suitability of ACB 16.
2. Schedule ACB 16 cyber testing to include cooperative vulnerability and penetration assessments and adversarial assessments for ACB 16 variants as soon as feasible to identify and mitigate any cyber vulnerabilities, especially for ships currently employing ACB 16 in the fleet.
3. Determine and correct the cause of reliability issues with the Aegis Display System and SPY-1 radar.
4. Identify the cause of deficiencies found during Capability Package 22-1 testing and prioritize the correction of those deficiencies for deploying ships.
5. Submit, for DOT&E approval, an Aegis TEMP to adequately test ACB 20 capabilities not covered in the combined DDG 51 FLT III, Baseline 10, and Air and Missile Defense Radar TEMP.
6. Complete the ACB 16 operational test campaign.

Air Warfare (AW) Ship Self-Defense Enterprise

Air Warfare Ship Self-Defense components include, from left to right: Close-in Weapons System, Rolling Airframe Missile, and Evolved Sea Sparrow Missile

In FY22, the Navy commenced development of a next-generation Air Warfare (AW) Ship Self-Defense Enterprise Test and Evaluation Master Plan (TEMP) for the determination of the ship self-defense capability of PCU *John F. Kennedy* (CVN 79), USS *Bougainville* (LHA 8), and USS *Harrisburg* (LPD 30) against threat anti-ship cruise missiles (ASCMs). DOT&E and the Navy have not yet agreed on the required test resources for adequate test. Further, the Navy has yet to complete tests in the original Enterprise TEMP (2008) for littoral combat ships (LCS) and USS *Gerald R. Ford* (CVN 78).

SYSTEM DESCRIPTION

The AW Ship Self-Defense Enterprise is a Navy test strategy to assess the Probability of Raid Annihilation (PRA) requirements for several ship classes (mostly aircraft carriers and amphibious ships). The system under test is the combat system that enables the ship to execute self-defense against ASCMs. The combat systems aboard ships are a system-of-systems, including: 1) interacting combat systems elements with continuously evolving software; 2) radars for target detection; 3) target trackers; 4) an electronic warfare system; 5) a command and control system that integrates input from the sensors and trackers to calculate engagement options; 6) interceptor missiles; and 7) guns.

The systems that contribute to the PRA are:

- SPQ-9B horizon search radar;
- SPS-48 and SPS-49 air search radars;
- SPY-6(V)2 and SPY-6(V)3 Enterprise Air Surveillance Radars;
- Mk 9 Tracker Illuminator System;
- SLQ-32 electronic warfare system;
- SPY-3 Multi-Function Radar;
- SPY-4 Volume Search Radar;
- SeaRAM Ship Defense System;
- Cooperative Engagement Capability;
- Rolling Airframe Missile Block 2, 2A, and 2B;

- Evolved Sea Sparrow Missile (ESSM) Block 1 and 2;
- Close-In Weapon System; and
- Ship Self-Defense System (SSDS) Mk 2 Baseline 10 and Baseline 12.

The Navy has two AW Ship Self-Defense Enterprise T&E programs. The original AW Ship Self-Defense Enterprise TEMP from 2008 covers LCSs, *America*-class (LHA 6-class) amphibious assault ships, USS *Zumwalt*-class (DDG 1000-class) destroyers, and the USS *Gerald R. Ford* (CVN 78). The new, or next-generation, AW Ship Self-Defense Enterprise TEMP covers CVN 78-class with CVN 79 modifications, second flight LHA 6-class, second flight LPD 17-class, and back-fit of SSDS Mk 2 Baseline 12 on existing ships in the fleet. Ship self-defense testing of the USS *Zumwalt* transitioned to the PMS 500 Program Office and is reported within the DDG 1000 entry of this Annual Report.

MISSION

The Navy depends on the integrated combat system to enable the crews of the ships to defend themselves against threat ASCMs. The goal of the AW Ship Self-Defense Enterprise program is to quantify the PRA that the ships can achieve against raids of ASCMs. Because of the high cost, as well as safety risk, of live test events against ASCM surrogates, the Navy cannot cover the operational space of threat ASCMs and scenarios in live test events alone. The Navy strategy depends upon limited live testing against threat ASCM surrogates to demonstrate a limited capability and then to validate modeling and simulation (M&S) used to quantify performance with statistical confidence and to expand the tested operational space.

PROGRAM

In 2005, the Navy started the AW Ship Self-Defense Enterprise T&E program to leverage testing across multiple ships and combat system element-level test programs, and reduce the overall resources needed to evaluate PRA and program specific test requirements. In 2008, the Navy formalized the strategy in the AW Ship Self-Defense Enterprise TEMP. In July 2021, a Naval Capabilities Board approved the continuance of an Enterprise test strategy for follow-on capability, including that of the CVN 79, LHA 8, and LPD 30. The Navy expects to deliver a TEMP for DOT&E approval in FY23.

» MAJOR CONTRACTORS

- SSDS: Lockheed Martin, Rotary and Mission Systems – Moorestown, New Jersey
- SPY-3: Raytheon Integrated Defense Systems – Tewksbury, Massachusetts
- SPY-4: Lockheed Martin – Moorestown, New Jersey
- SPY-6: Raytheon Missiles & Defense – Marlborough, Massachusetts
- Rolling Airframe Missile and ESSM: Raytheon Missiles and Defense – Tucson, Arizona
- Cooperative Engagement Capability: Raytheon Co. – Largo, Florida
- SLQ-32 with SEWIP Block 1: General Dynamics Mission Systems – Fairfax, Virginia
- SLQ-32 with SEWIP Block 2: Lockheed Martin Corp., Rotary Mission Systems – Liverpool, New York

TEST ADEQUACY

The program's test strategy uses a three-phase approach for both the 2008 Enterprise and the next-generation Enterprise:

- Phase 1: Live missile firings of ASCM surrogates against a self-defense test ship (SDTS) configured with the integrated combat system of the ship under test.
- Phase 2: Live missile firings of ASCM surrogates against the ship under test (primarily the lead ship of a ship class).
- Phase 3: M&S runs in the Enterprise test bed against ASCM threat models.

2008 Enterprise:

In FY22, the Navy conducted no operational test of self-defense capability of LCS against ASCMs. Both *Independence*-class and *Freedom*-class ships have deployed without operational test of this capability.

In FY22, the Navy conducted no operational test of the self-defense capability of CVN 78 against ASCMs. The Navy plans to conduct live fire missile against the lead ship (phase 2) and M&S runs (phase 3) necessary to evaluate the operational effectiveness and suitability of the integrated combat system of the CVN 78 in FY24. However, the Navy must complete development and validation of the intended M&S suite to support the phase 3 testing.

Next-generation Enterprise:

In FY22, the Navy started development of the next-generation AW Ship Self-Defense Enterprise TEMP to determine an overarching test strategy and test resources to assess the self-defense capability of CVN 79, LHA 8 and LPD 17 Flight II ships against threat ASCMs. DOT&E and the Navy have not yet agreed on required test resources for adequate test.

The Navy may not have a sufficient excess of ESSM Block 1 missiles in fleet inventory to support operational testing of CVN 79 and LHA 8. These missiles, required for combat system testing in FY25 and beyond, are no longer in production. The Navy acknowledges the ESSM limitation and intends to work with DOT&E to overcome this limitation and maintain an adequate test.

The Navy scheduled repairs to the existing SDTS (e.g., former USS *Paul F. Foster*) in FY24. The availability of an unmanned test capability will be required to execute the test strategy.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Performance evaluations of ships covered by the 2008 Enterprise are included in the SSDS and ship class articles of this Annual Report. Effectiveness, suitability, and survivability of ships covered by the 2008 Enterprise are included in the SSDS and ship class articles of this Annual Report.

No data are available yet to assess ships covered by the next-generation AW Ship Self-Defense Enterprise.

Cyber survivability is reported within ship-class and SSDS program articles of this Annual Report.

RECOMMENDATIONS

The Navy should:

1. Address all recommendations for ship self-defense testing against threat ASCMs provided in the SSDS and ship class articles of this Annual Report, which include the development and validation of the M&S suite for CVN 78 testing.
2. Monitor funding and execution of SDTS repairs to ensure its readiness to support integrated combat system testing of CVN 79, LHA 8 and LPD 17 Flight II ships.
3. Evaluate options for adequate test should excess ESSM Block 1 missiles in fleet inventory be insufficient to support operational test.
4. Monitor the development and test of the elements of the integrated combat system elements. If needed, take actions to ensure their availability to support the AW Ship Self-Defense Enterprise test strategy.

Amphibious Combat Vehicle – Command and Control Variant (ACV-C)

The U.S. Marine Corps regiment or battalion command group equipped with the Amphibious Combat Vehicle – Command and Control variant (ACV-C) is operationally effective as a stationary command post. The ACV-C is suitable and survivable to most threshold ballistic threats. It is vulnerable to cyberattack from nearsiders with physical access to the ACV-C.

SYSTEM DESCRIPTION

The ACV-C is a mission-role variant in the Amphibious Combat Vehicle (ACV) family of vehicles. It shares a common hull, powertrain, drivetrain, water propulsion system, and survivability suite with the baseline Amphibious Combat Vehicle – Personnel variant (ACV-P) and integrates additional radios, antennas, and a larger battery pack to support silent watch operations. The ACV-C is equipped with seven radios that allow secure voice and data communications.

MISSION

The ACV-C serves as a tactical-echelon command post for the U.S. Marine Corps regiment or battalion, allowing the Commander to provide under armor command and control (C2) of the maneuver formation, as well as enabling the staff to develop operational situational awareness, perform operations planning, process intelligence, coordinate the delivery of fire support assets, and coordinate logistics support.

PROGRAM

The ACV family of vehicles is an Acquisition Category IB program with four variants: Personnel (ACV-P), Command and Control (ACV-C), Maintenance and Recovery (ACV-R), and Medium Caliber Cannon (ACV-30). DOT&E reported on the ACV-P in November 2020. The U.S. Navy made a production decision in March 2022 to produce the ACV-C. The U.S. Marine Corps is still developing and testing the ACV-30 and ACV-R variants.

» MAJOR CONTRACTOR

- BAE Systems Land & Armaments L.P. – Sterling Heights, Michigan

TEST ADEQUACY

ACV-C testing was adequate to support the evaluation of operational effectiveness, operational suitability, and survivability. The Marine Corps Operational Test and Evaluation Activity conducted the FOT&E and an adversarial assessment at the Marine Corps Base Camp Pendleton, California from January 20 to February 11, 2022. The Army Aberdeen Test Center conducted ACV-C LFT&E in Aberdeen, Maryland from May 2021 to January 2022. All testing was conducted in accordance with DOT&E-approved test plans and DOT&E observed the test.

PERFORMANCE

» EFFECTIVENESS

The ACV-C is operationally effective as a stationary command post but not operationally effective as a mobile command post. The ACV-C does not have enough secure beyond-line-of-sight (BLOS) voice and data nets to support the C2 mission. When the ACV-C is stationary, embarked staff can set up additional BLOS external antennas to support communication demands. The embarked staff is limited to a single BLOS net when the ACV-C is mobile.

» SUITABILITY

The ACV-C is operationally suitable. It exceeded the operational availability requirement, and the maintainers were able to remedy failures quickly, reducing system down time. The ACV-C did not meet its reliability requirement. Frequent communication failures degraded the ACV-C's C2 mission effectiveness. The embarked staff need more hands-on training in troubleshooting frequent communication problems.

» SURVIVABILITY

The ACV-C is survivable and meets the threshold-level force protection requirements against most required kinetic threats. It is vulnerable to nearsider attacks with physical access to the vehicle in a cyber-contested environment. The ACV-C's segmentation of communication and automotive networks helps mitigate some cybersecurity vulnerabilities.

RECOMMENDATIONS

The Marine Corps should:

1. Provide additional BLOS voice and data networks to support the C2 mission.
2. Improve the reliability of the communication system.
3. Train ACV-C crews to adequately support the C2 mission.
4. Consider employing two ACV-C sections to support units' C2 until the ACV-C is effective as a mobile command post.
5. Mitigate the identified vulnerabilities to kinetic and cyber threats.

CH-53K King Stallion

Marine Operational Test and Evaluation Squadron One (VMX-1) conducted IOT&E from July 30, 2021 to April 11, 2022 in accordance with the DOT&E-approved test plan. The United States Marine Corps declared Initial Operational Capability (IOC) in April 2022 based on the Service's assessment of the CH-53K's operational effectiveness, suitability, and survivability demonstrated in IOT&E. DOT&E's assessment of the CH-53K's performance will be detailed in the IOT&E report and its classified annex in 1QFY23. The Navy has not funded the Phase II Live Fire test and evaluation (LFT&E) program which is necessary to evaluate the CH-53K's survivability against operationally relevant threats in accordance with the DOT&E-approved Test and Evaluation Master Plan.

SYSTEM DESCRIPTION

The CH-53K is a dual-piloted, multi-engine helicopter. Composite material construction, new engine design, a glass cockpit, and fly-by-wire flight controls are indicative of the improved technology designed throughout the CH-53K when compared to the 1980s era CH-53E. The Marine Corps will assign CH-53Ks to existing Marine heavy helicopter squadrons to replace their current fleet of CH-53Es.

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

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

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

PROGRAM

The CH-53K is an Acquisition Category IC program. DOT&E approved the Milestone C Test and Evaluation Master Plan (Revision C) in February 2017 and the Alternative LFT&E Strategy (Revision C) in May 2010. DOT&E approved the OT-C1 IOT&E Plan in June 2021. IOT&E data and analysis will support the Full-Rate Production decision scheduled for 1QFY23. The United States Marine Corps declared IOC in April 2022.

» MAJOR CONTRACTOR

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

TEST ADEQUACY

VMX-1, under the auspices of the Navy's Operational Test and Evaluation Force (OPTEVFOR), conducted IOT&E equipped with four CH-53Ks from July 30, 2021 to April 11, 2022 in accordance with the DOT&E-approved test plan and observed by DOT&E. VMX-1 conducted flight events at Marine Corps Air-Ground Combat Center (MCAGCC) Twentynine Palms, California; Marine Corps Air Station (MCAS) New River, North Carolina; and aboard USS *Iwo Jima* (LHD 7) operating off the coast of North Carolina. Naval Air Warfare Center, Aircraft Survivability Division, China Lake, California, collected data during Phase I live fire testing from 2QFY14 to 4QFY22.

CH-53K testing was adequate to support the evaluation of operational effectiveness, operational suitability, cybersecurity, and live fire testing. Aircraft survivability equipment testing was not adequate. The Navy's test design was insufficient to acquire the necessary data in the necessary conditions and issues with the test execution further restricted the data acquired. Additional DECM testing is scheduled for 2QFY23.

During IOT&E, VMX-1 accumulated 451.1 flight hours over 114 flights. These flights occurred in desert, mountainous, and forested environments and aboard ships during the day and at night. VMX-1 transported internal cargo ranging in weight from 2,500 to 10,000 pounds in all environments. Externally transported loads included Light Armored Vehicles, M777 Howitzers, and High Mobility Multipurpose Wheeled Vehicles. External loads also included the unplanned and successful recovery of a 15,200-pound Navy MH-60S from its crash site located at 12,000 feet above mean sea level. VMX-1 did not conduct troop transport missions with 30 combat equipped troops down to minimum fuel due to incomplete aircraft center of gravity developmental testing.

IOT&E operations did not assess CH-53K secondary missions of air evacuation, forward arming and refueling point operations, air delivery, or rapid insertion and extraction operations. CH-53K operational testing of these missions is scheduled for 2QFY23.

A CH-53K structural repair manual was not available for evaluation during IOT&E. The program expects to deliver the structural repair manual in FY25.

IOT&E did not assess initial accession training curricula (scheduled for delivery in October 2022) and logistics supportability (material support date scheduled for January 2024).

Phase I of the LFT&E program began with risk reduction testing in 2008, major component testing in 2QFY14, and completed in 4QFY22. Risk reduction tests addressed design questions on high risk components prior to the approval of the Alternate LFT&E Strategy. The test plans were individually concurred with and tests observed by DOT&E. Phase I tested critical components and the Ground Test Vehicle against threshold and some objective threats. The Navy conducted ballistic testing at Naval Air Warfare Center, China Lake, California.

Sikorsky completed tail rotor blade endurance testing to evaluate threat-damaged test articles to representative fly-home loads in 4QFY22.

From 2QFY21 to 1QFY22, the Navy conducted Ground Test Vehicle testing to dynamically evaluate high-risk shots, including gearboxes, structure, flight controls, the hydraulic accumulator, and engine bay fire suppression systems under representative flight conditions.

The Navy performed ballistic vulnerability analyses supplementing the extensive live fire testing to assess the CH-53K overall ballistic vulnerability. The assessment did not include a threat-specific radio frequency or infrared tests. Electromagnetic effects were primarily assessed through electromagnetic environmental testing. In accordance with the DOT&E-approved strategy, no high-altitude electromagnetic pulse or electromagnetic pulse testing was performed. These threats should be evaluated in future survivability testing.

The Program Office has continued to defer Phase II of the LFT&E program due to lack of funding. Phase II of the LFT&E program, defined in the DOT&E-approved Alternative LFT&E Strategy, is essential for a complete survivability assessment of the CH-53K against operationally relevant threats expected to be encountered in combat. The majority of Phase II testing was originally planned to occur prior to the Full-Rate Production decision and will test components not tested in Phase I and components added or modified during aircraft development.

Cybersecurity Red Teams from OPTEVFOR and Naval Air Warfare Center – Aircraft Division Patuxent River conducted a cooperative vulnerability and penetration assessment and an adversarial assessment at MCAS New River from March 14 – 25, 2022. This testing included the Personal Computer Memory Card International Association Card, Military Standard 1553 Non-Internet Protocol and Ethernet network testing, and ARC-210 very high frequency/ultra-high frequency radio transceiver testing. The Navy did not test ARINC 429 buses onboard the CH-53K. Comprehensive integrated cyber-survivability testing is scheduled for 2QFY24.

The Navy tested the DECM system on January 12 and 19, 2022 during transit and on-site at Ingalls Field in Hot Springs, Virginia, and at the Atlantic Test Range at Patuxent River Naval Air Station, Maryland in February 2022. The DECM system was in an “interim” configuration. The Navy will upgrade and test the aircraft’s survivability equipment to the Data Transfer Unit DECM System Replacement in FY23, which will require additional integration and flight testing for an updated survivability determination.

The test data are not adequate to determine if the AAQ-24 and APR-39C(V)2 systems were properly integrated on the platform or to determine effects on CH 53K survivability. DOT&E did not have enough data to determine the detailed performance of the system. The data provided by the Navy for the APR-39C(V)2 were time-to-detect. Without additional data pertaining to the simulated threats and system performance, aircraft survivability cannot be determined. Issues during the conduct of the test also led to inconsistent system configurations that the Navy should correct for FOT&E.

PERFORMANCE

» EFFECTIVENESS

United States Marine Corps declared IOC in April 2022 based on the Service's assessment of the CH-53K's operational effectiveness demonstrated in IOT&E. DOT&E's assessment of the CH-53K's effectiveness will be described in detail in the IOT&E report in 1QFY23.

» SUITABILITY

United States Marine Corps declared IOC in April 2022 based on based on the Service's assessment of the CH-53K's operational suitability demonstrated in IOT&E. DOT&E's assessment of the CH-53K's suitability will be described in detail in the IOT&E report in 1QFY23.

» SURVIVABILITY

United States Marine Corps declared IOC in April 2022 based on based on the Service's assessment of the CH-53K's operational survivability demonstrated in IOT&E and LFT&E. DOT&E's assessment of the CH-53K's survivability will be described in detail in classified IOT&E report annex in 1QFY23.

RECOMMENDATIONS

The Navy should:

1. Fund and complete the planned Phase II LFT&E program to fully assess CH-53K vulnerability against operationally relevant threats.
2. Complete additional center-of-gravity developmental testing for transporting 30 combat-equipped Marines.
3. Review internal cargo loading procedures to optimize loading heavy pallets.
4. Expedite structural repair manual to facilitate combat damage repair at the organizational level
5. Conduct Data Transfer Unit DECM System Replacement operational testing prior to fielding to characterize aircraft susceptibility to threat weapon systems.
6. Conduct additional cybersecurity testing on wireless intercommunications system, deterministic Ethernet, and ARINC 429 network to fully characterize cyber threats.
7. Address recommendations found in DOT&E's IOT&E report and classified annex for effectiveness, suitability, and survivability.

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

United States Navy declared Initial Operational Capability (IOC) in December 2021 based on the Service's assessment of the CMV-22B's operational effectiveness, suitability, and survivability demonstrated in FOT&E period OT-D1. Operational Test and Evaluation Force is drafting the FOT&E OT-D2 test plan in collaboration with DOT&E. The data collected during this test, combined with integrated test (IT) data qualified for operational test (OT), will be used to support an initial fielding decision for the CMV-22B Communications Upgrades Suite by the V-22 Program Office (PMA-275) in late-FY23.

SYSTEM DESCRIPTION

The CMV-22B Osprey is a tiltrotor vertical/short takeoff and landing aircraft the Navy intends to replace the C-2A Greyhound, the legacy carrier onboard delivery aircraft. The CMV-22B is based on the MV-22B design, equipped with increased fuel capacity, fuel jettison, integrated public address system, high-frequency radio, and cabin and cargo lighting. The CMV-22B must be capable of conducting operations in a permissive threat environment, day and night, in all weather conditions. The CMV-22B is assigned to Navy Fleet Logistics Multi-Mission Squadrons (VRMs). Each VRM will deploy detachments of aircraft to forward logistics sites located within their theater of operations. A detachment of three CMV-22B aircraft will operate from each forward logistics site to support a Carrier Strike Group.

MISSION

Fleet Logistics Multi-Mission Squadrons (VRM 30/40) detachments equipped with CMV-22B perform the primary mission of airborne resupply/logistics for seabasing. Secondary missions include: vertical onboard delivery; vertical replenishment; medical evacuation; Naval Special Warfare support; missions of state; and search and rescue support.

The CMV-22B fills the Joint Force Maritime Component Commander time-critical logistics air connector requirements by transporting personnel, mail, and priority cargo from advance bases to the Seabase.

PROGRAM

The CMV-22B, as part of the overall V-22 Program of Record, is an Acquisition Category IC program, which entered full-rate production in 2005. The CMV-22B has been incorporated with the current V-22 production line and deployed to the fleet. It achieved IOC in December 2021 and will reach full operational capability in FY23. DOT&E approved the CMV-22B Test and Evaluation Master Plan and the Alternative LFT&E plan in March, 2020. The FOT&E OT-D2 test plan is in development and expected to be approved by DOT&E in early-FY23. Additional fuel cell survivability testing is expected in mid-FY23 with final survivability analysis completed by the end of FY23.

» MAJOR CONTRACTOR

- Bell-Boeing Joint Project Office – Amarillo, Texas

TEST ADEQUACY

Air Test and Evaluation Squadron 21 (HX-21) conducted IT on the CMV-22B communications upgrades suite from August 2021 to June 2022. The in-scope communications upgrades are a federated communication system designed to provide Link 16 and Satellite Phone capabilities to meet CMV-22B interoperability requirements and Federal Aviation Administration/International Civil Aviation Organization/military Air Traffic Control requirements. The system will require permanent installation of components into the existing CMV-22B airframe.

Operational testers from Air Test and Evaluation Squadron 1 (VX-1) participated in the IT events. HX-21 flew 18.7 flight hours over seven IT events. Data collected during the IT test events will support the Operational Test Readiness Review to certify CMV-22B to enter OT-D2 in 1QFY23. DOT&E witnessed the IT events, and will witness FOT&E OT-D2 and LFT&E events in FY23.

Operational Test and Evaluation Force is drafting the OT-D2 test plan in collaboration with DOT&E. The primary purpose of this test is to evaluate the effectiveness, suitability, and cyber survivability of the CMV-22B aircraft with communications upgrades performing roles of logistics, search and rescue support, and mobility as part of the Carrier Strike Group. The data collected during this test, combined with IT data qualified for OT, will be used to support an initial fielding decision for the CMV-22B communications upgrades by the V-22 Program Office (PMA-275) in late-FY23.

OT-D2 will verify corrections of deficiencies that were discovered during OT-D1 in FY21, as well as provide an initial evaluation for previously untested training syllabi and simulators for pilots, aircrew, and maintainers. It will include a cybersecurity cooperative vulnerability penetration assessment and an adversarial assessment.

PERFORMANCE

» EFFECTIVENESS

United States Navy declared IOC in December 2021 based on the Service's assessment of the CMV-22B's operational effectiveness demonstrated in OT-D1. DOT&E's assessment of the CMV-22B's effectiveness is described in detail in the OT-D1 report published in June 2022. At the OT-D2 Operational Test Readiness Review, scheduled for 1QFY23, it is expected that OTRR Air Test and Evaluation Squadron One (VX-1) and Air Test and Evaluation Squadron Two One (HX-21) will recommend that CMV-22B proceed into OT-D2 based on communications upgrades performance during IT.

SUITABILITY

United States Navy declared IOC in December 2021 based on the Service's assessment of the CMV-22B's operational suitability demonstrated in OT-D1. DOT&E's assessment of the CMV-22B's suitability is described in detail in the OT-D1 report. At the OT-D2 Operational Test Readiness Review, scheduled for 1QFY23, it is expected that VX-1 and HX-21 will recommend that CMV-22B proceed into OT-D2 based on communications upgrades performance during IT.

SURVIVABILITY

United States Navy declared IOC in December 2021 based on the Service's assessment of the CMV-22B's survivability demonstrated in OT-D1. DOT&E's assessment of the CMV-22B's survivability is described in detail in the classified OT-D1 report annex. At the OT-D2 Operational Test Readiness Review, scheduled for 1QFY23, it is expected that VX-1 and HX-21 will recommend that CMV-22B proceed into OT-D2 based on CU performance during IT. Additional live fire testing of the wing auxiliary fuel tanks will take place in mid-FY23. The final survivability analysis is expected to be completed by the end of FY23, following the completion of all live fire tests.

RECOMMENDATIONS

The Navy should:

1. Continue to implement the recommendations in DOT&E's OT-D1 report and classified annex.
2. Continue to plan and conduct OT-D2 to provide a determination of effectiveness, suitability, and survivability of the CU suite prior to fleet introduction.

CMV-22B Osprey operational test on USS Carl Vinson *(CVN 70), December 2021*

Conventional Prompt Strike (CPS)

Flight testing of the Conventional Prompt Strike (CPS) prototype All-Up Round (AUR) began in June 2022 with Joint Flight Campaign–1 (JFC-1). During JFC-1, the missile experienced an in-flight anomaly which prevented data collection over a portion of the planned flight profile. The Navy reports identification of the root cause and implementation of corrective actions for the anomaly, and is preparing to execute JFC-2. The Navy has four JFCs planned though 4QFY24 to develop and demonstrate a hypersonic, cold-gas launched missile system prototype capability. The Army plans to employ the prototype AUR from mobile land-based launchers as part of the Long Range Hypersonic Weapon (LRHW) program. The Navy intends to transition to rapid fielding aboard the *Zumwalt*-class destroyer in FY25 and achieve initial operational capability aboard the *Virginia*-class submarine in FY29.

SYSTEM DESCRIPTION

CPS is a conventional, boost-glide hypersonic weapon system. The CPS all-up-round missile includes a two stage solid rocket motor booster and a Common Hypersonic Glide Body containing a kinetic energy projectile warhead.

MISSION

U.S. Combatant Commanders will launch CPS from *Zumwalt*-class destroyers and *Virginia*-class submarines to penetrate air defenses to strike high-value, time-sensitive targets.

PROGRAM

The Navy currently has a three phase acquisition strategy to deliver CPS: 1) Phase 1, Middle Tier of Acquisition (MTA) Rapid Prototyping, to develop and demonstrate a hypersonic, cold-gas launched missile system prototype capability; 2) Phase 2, MTA Rapid Fielding, to field CPS onboard a *Zumwalt*-class destroyer; and 3) Phase 3, transition to a Major Defense Acquisition Program at Milestone C, to field CPS onboard *Virginia*-class submarines and the remaining *Zumwalt*-class destroyers.

The Navy's CPS program will provide the all-up-round missiles and elements of the weapons control system for the Army's LRHW (Dark Eagle) program in FY23. The Army will integrate the common all-up-rounds with their weapon control system into a prototype LRHW Battery Operations Center and transporter-erector-launcher system.

In 2019, the Navy developed a Master Test Strategy (MTS) for Phase 1 of CPS. In June 2021, DOT&E placed CPS under oversight. The Navy is updating the MTS to address programmatic changes and additional performance metrics, and plans to provide for DOT&E approval in 1QFY23. However, the alignment of weapon system requirements to flight test objectives across all three phases of the program is not yet mature and is being worked by the Navy. The Navy intends an additional update to the MTS in 1QFY24 that will provide an overall test strategy with alignment of planned missile flights to the planned advances in missile capability for each phase of CPS delivery.

The Navy has yet to identify test conditions and associated test resources that will be evaluated across the three CPS phases to adequately assess lethality and operational effectiveness in the threat-contested environment. The Navy is considering inclusion of the threat-contested environment in Phase 1 testing, but has yet to commit due to developmental test requirements. These data are necessary to validate and use model and simulation for operational testing, and delays in data collection could increase operational test cost in later CPS phases. DOT&E will work with the Navy to maximize efficiencies within the test strategy provided in the follow-on update to the Phase 1 MTS.

» MAJOR CONTRACTOR

- Lockheed Martin Space – Littleton, Colorado

TEST ADEQUACY

The Phase 1 test strategy was developed to demonstrate an operational capability of the CPS prototype. Phase 1 includes five JFC events to evaluate flight performance of the CPS all-up-round and common components of the hypersonic weapon systems within mission-relevant scenarios. The Navy expects Phase 1 test data to support modeling and simulation validation. The Navy plans to evaluate the operational effectiveness, operational suitability, survivability, and lethality of CPS in a contested environment through the completion of all three phases. However, the test strategies for phases 2 and 3 are not developed.

In June 2022, the Navy conducted the first JFC event, JFC-1, to test a single CPS all-up-round at the Pacific Missile Range Facility. The test was a DT event and did not require DOT&E approval; however, DOT&E observed the test event. JFC-1 experienced an in-flight anomaly that prevented data collection for portions of the planned flight profile. The Navy has determined the cause, implemented corrective actions, and is preparing to execute JFC-2.

The second flight test, JFC-2, will be launched from the prototype Army weapon control system, Battery Operations Center, and transporter-erector-launcher with soldier observation during the test. The test will occur at Cape Canaveral Space Force Station, Florida.

The third flight test event, JFC-3, will launch from the prototype Army transporter-erector-launcher and provide a demonstration of launch capability for the Army's Dark Eagle program. The final events in Phase 1, JFC-4 and JFC-5, are intended to demonstrate the Navy's cold-gas launch capability and residual operational capability.

PERFORMANCE

» EFFECTIVENESS

The Navy is early in test and has not yet demonstrated an operational capability for the CPS prototype. DOT&E will provide an assessment of demonstrated capabilities and limitations of the CPS prototype at the completion of Phase 1 flight tests in FY24. DOT&E will report CPS operational effectiveness within an IOT&E report upon the completion of Phase 3 testing in FY29.

CPS sled and flight tests have not included operationally representative targets and consequently do not provide direct evidence of the weapon's lethal effects against intended targets. The Navy could attain both lethality and effectiveness data by incorporating representative targets into the JFC tests and/or ground tests, but currently does not intend to do so. A lack of lethality data using representative targets could limit the Navy's ability to validate weaponeering models.

» SUITABILITY

The Phase 1 CPS prototype is not sufficiently mature to assess suitability metrics. DOT&E will report suitability metrics for the Phase 1 CPS prototype at the completion of flight tests in FY24. DOT&E will report CPS operational suitability within an IOT&E report upon the completion of Phase 3 testing in FY29.

The program intends to complete an initial Life Cycle Support Plan by FY25 to address product support and fielding aboard both the *Zumwalt*-class destroyer and the *Virginia*-class submarine.

» SURVIVABILITY

The Navy has not demonstrated the effect of a contested environment on CPS prototype performance. The Navy's standing plan for Phase 1 is to rely on a combination of flight environment modeling and simulation, component testing in a simulated environment, and a full hardware-in-the-loop evaluation to incorporate a contested environment into their performance assessment of the CPS prototype. The Navy has yet to provide an overarching strategy to assess CPS performance in contested environments across all three phases of acquisition, risking an inefficient test design across the three phases and the potential need for unplanned test resources in Phases 2 and 3. The Navy intends to detail their performance and test objectives in each of the three phases within an update to the Phase 1 MTS. DOT&E will report CPS survivability upon completion of IOT&E in Phase 3.

RECOMMENDATIONS

The Navy should:

1. Provide an update to the Phase 1 MTS with intended modifications to CPS and an overarching test strategy for the CPS program as soon as feasible, as this will maximize test efficiency across all three phases of test.
2. Incorporate operationally representative targets and flight environments into CPS ground and flight tests in order to provide lethality demonstrations against intended targets and to identify survivability vulnerabilities that can be fixed early in system development.
3. Develop and execute an LFT&E strategy as soon as feasible to ensure data collection necessary for the verification and validation of modeling and simulation tools and to enable a credible lethality assessment.

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

In FY22, USS *Gerald R. Ford* (CVN 78) completed its first Planned Incremental Availability (PIA, a 6-month maintenance period), conducted 84 days underway, transitioned from developmental test to integrated test to IOT&E, and continued operationally representative integration with its carrier air wing. Reliability challenges with systems critical for flight operations, including catapults, arresting gear, jet blast deflectors, and radar continue to pose the most risk to CVN 78 demonstrating operational effectiveness and suitability in IOT&E, which is scheduled to last through 4QFY24. Executing planned sortie generation and self-defense tests will be crucial to evaluating the ship's effectiveness and survivability, along with accrediting high-fidelity operational and Probability of Raid Annihilation (PRA) models, essential for evaluating key performance parameters and life-of-class sustainment.

SYSTEM DESCRIPTION

CVN 78 is a new class of nuclear-powered aircraft carriers based on the CVN 68 *Nimitz*-class hull, with significant design changes intended to enhance CVN 78's ability to launch, recover, and service aircraft while reducing 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 catapults and electromechanical arresting gear. CVN 78 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. The CVN 78 Integrated Combat System incorporates several changes, including the following:

- A new Dual Band Radar (DBR) that combines the phased-array SPY-4 Volume Search Radar and the SPY-3 Multi Function Radar. *Ford* is the only ship in the Navy with DBR. It will be replaced with the SPY-6(V)3 Enterprise Air Surveillance Radar fixed variant, the SPQ-9B horizon search radar, and Mk 9 Tracker Illuminator System on PCU *John F. Kennedy* (CVN 79) and follow-on carriers.
- Ship Self-Defense System Mk 2 Mod 6 Baseline 10 combat management system, which will be upgraded to the new capability build, Baseline 12, on CVN 79 and follow-on carriers.
- Cooperative Engagement Capability USG-2B tracking, data fusion, and distribution system, which will be upgraded to Cooperative Engagement Capability Block II on CVN 79 and follow-on carriers.
- SLQ-32(V)6 electronic surveillance and warfare system, equipped with Surface Electronic Warfare Improvement Program Block 2.
- Rolling Airframe Missile (RAM) Block 2 and the Evolved Sea Sparrow Missile (ESSM) Block 1. CVN 79 and follow-on carriers will be upgraded to a mix of new RAM variants Block 2A and 2B, plus a mix of ESSM Block 1 and Block 2.

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. CVN 78 includes a new Heavy Underway Replenishment system capable of transferring cargo loads of up to 12,000 pounds.

MISSION

Carrier Strike Group 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 in a joint and/or allied maritime expeditionary force in response to crises; and
- Carry the war to the enemy through joint multi-mission offensive operations by
  - Operating and supporting aircraft to attack enemy forces ashore, afloat, or submerged, independent of forward-based land facilities;
  - Protecting friendly forces from enemy attack through the establishment and maintenance of battlespace control, independent of forward-based land facilities; and
  - Engaging in sustained operations in support of the United States and its allies, independent of forward-based land facilities.

PROGRAM

CVN 78 is an Acquisition Category IC program. DOT&E approved Revision E of the Test and Evaluation Master Plan (TEMP) and the first of two phases of the IOT&E Test Plan in September 2022. The CVN 78 TEMP will be updated by 1QFY24 to refine the self-defense test strategy and resourcing to test CVN 79's self-defense capability. The CVN 78 test plan will be updated before the second phase of IOT&E, which is planned to begin in 2QFY24.

The first ship in the *Ford* class, CVN 78, was delivered to the

Navy in 2017. It completed Post Delivery Test and Trials in 2021 to demonstrate the basic functionality of the carrier, certify the flight deck, embark an air wing, and serve as the East Coast carrier qualification (CQ) platform for student and fleet naval aviators. Based on the Navy's assessment, it declared Initial Operating Capability in December 2021. CVN 79 delivery is scheduled for 2024 and will be capable of supporting F-35 operations upon completion of Post Shakedown Availability. *Enterprise* (CVN 80) construction began in 2017, and *Doris Miller* (CVN 81) construction began in 2021.

» MAJOR CONTRACTOR:

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

TEST ADEQUACY

The Navy began CVN 78 IOT&E in September 2022. The Navy is conducting IOT&E in accordance with TEMP Revision E and the IOT&E Test Plan, which involves 10 underway periods (including integrated test), extensive modeling, and spans 2 years.

The first of three land-based cyber survivability tests was completed on the Electromagnetic Aircraft Launch System (EMALS) and Advanced Arresting Gear (AAG) in June 2022. This test was executed in accordance with a DOT&E-approved test plan and DOT&E observed the test. The planned test was limited in scope due to the Navy's lack of robust cyber testing capability on industrial control systems that are common on modern ships. The Navy Surface Warfare Center Philadelphia Division's Strategic Cyber-Physical Initiative is attempting to address this limitation. Land-based cyber testing will continue in FY23, and a shipboard test is scheduled for FY24.

The Navy conducted self-defense testing against unmanned aerial vehicles and unmanned small boats in July 2022, in accordance with a DOT&E-approved test plan that was executed during Combat Systems Operational Rehearsal Event Phase 2. DOT&E observed the testing, and the results are still undergoing analysis.

Additionally, CVN 78 conducted sea trials after its PIA and six underway periods that included fixed-wing flight operations, two of which were in accordance with a DOT&E-approved test plan and one was observed by DOT&E. Four of these underway periods involved training squadrons and two involved a portion of its carrier air wing. To date, CVN 78 has conducted 10,826 catapult launches (2,699 of which were in FY22) and 10,826 arrested landings (2,699 of which were in FY22). During these underway periods, the crew also performed two ammunition onloads and a RAM live fire. One of the ammunition onloads was part of a DOT&E-approved test plan, and the live fire was part of a Carrier Strike Group 12 self-defense exercise. DOT&E observed one ammunition onload and the RAM live fire. Although not part of the IOT&E test plan, the data from the RAM live fire will be adjudicated for score and is planned to contribute to the PRA model.

In April 2022, DOT&E submitted a classified report to Congress detailing system performance during planned test events against the Self Defense Test Ship (SDTS) configured to represent CVN 78's capability. This report covers testing between December 2018 and December 2020, during which the Navy completed three of the four planned test events against the SDTS, including the employment of RAMs and/or ESSMs.

There may not be enough data to determine the operational effectiveness and suitability of the self-defense capability of CVN 78 against anti-ship cruise missiles (ASCMs) due to test data that will not be available for reasons discussed in the Ship Self-Defense System article of this Annual Report. The self-defense tests planned in the Revision E TEMP will provide the only remaining live fire self-defense data points in IOT&E, and will not inform performance against some types of ASCM threats. It is vital that the Navy successfully verify, validate, and accredit the high-fidelity PRA model being developed by the Program Executive Office for Integrated Warfare Systems in order to gain adequate understanding of the Anti-Air Warfare mission capability by completion of IOT&E.

The Navy plans to eventually upgrade the combat systems suite on CVN 78 to match CVN 79 and follow-on ships. Due to the differences between the combat systems, and the fact that CVN 79 will be the enduring self-defense configuration for the class, it is imperative that CVN 79 self-defense capabilities are adequately tested.

PERFORMANCE

» EFFECTIVENESS

Combat System

In April 2022, DOT&E submitted a classified interim report to Congress on the operational effectiveness of CVN 78's self-defense capability against ASCMs.

Regarding the self-defense testing against unmanned aerial vehicles and unmanned small boats in July 2022, no preliminary assessment is available because analysis is not yet complete.

Sortie Generation

The reliability of CVN 78 catapults, arresting gear, and jet blast deflectors (JBDs) continues to have an adverse effect on sortie generation and flight operations efficiency. During an underway period in August of 2022, the ship returned early due to unexpected problems with its JBDs. The early return was necessary to facilitate JBD repairs and did not allow completion of CQ. The ongoing reliability problems with these critical subsystems remains the primary risk to the successful completion of CVN 78 IOT&E. Executing the planned sortie generation-rate testing, as outlined in the Revision E TEMP, will be crucial to evaluating the ship's combat effectiveness and accrediting the high-fidelity Sea Strike/Sea Basing Aviation Model, an essential tool for evaluating the sortie generation rate key performance parameter and supporting life-of-class upgrades.

» SUITABILITY

The low or unproven reliability of the following five CVN 78 systems pose the most significant challenge to flight operations:

EMALS

During testing from March through June 2022 (after the PIA), EMALS achieved a reliability of 614 mean cycles between operational mission failures (MCBOMF) during 1,841 catapult launches (where a cycle is the launch of one aircraft). While this reliability is well below the requirement of 4,166 MCBOMF, EMALS showed slight improvement in reliability from FY21 (460 MCBOMF throughout 1,758 catapults). However, during the first underway of IOT&E in September 2022, EMALS reliability appeared to regress and slowed CQ. While the data are still being analyzed, the adverse effect to operations on two of the ten days of CQ was significant. Naval Air Systems Command is working on short- and long-term improvements to address EMALS reliability degraders. Short-term improvements are focused on improving component reliability and are expected to be incorporated on *Gerald R. Ford* by the end of FY23.

AAG

During testing from March through June 2022 (after the PIA), AAG achieved a reliability of 460 MCBOMF during 1,841 aircraft recoveries (where a cycle is the recovery of a single aircraft). While this reliability is well below the requirement of 16,500 MCBOMF, AAG showed slight improvement in reliability from FY21 (115 MCBOMF throughout 1,758 catapults). However, during the first underway of IOT&E in September 2022, AAG reliability appeared to regress and slowed CQ. While the data are still being analyzed, the adverse effect to operations on three of the ten days of CQ was significant. Naval Air Systems Command is working on short- and long-term improvements to address AAG reliability degraders. Short-term improvements are focused on improving indications and software and are expected to be incorporated on Gerald R. Ford by the end of 2QFY23.

JBDs

During early developmental testing, reliability concerns were identified with the Electro Mechanical Actuators (EMA) that are used to raise and lower the JBDs on the *Ford* class. Several modifications were implemented on CVN 78 during the PIA to improve reliability. During the August 2022 CQ, the ship experienced EMA failures on all four JBDs, which caused the ship to cancel the remainder of CQ and return early. The cause of the EMA failures was corroded fasteners in various components of the EMA. The root cause of the fastener corrosion is being addressed, and repairs were completed prior to September's CQ. During the September CQ, JBD performance did not adversely affect flight operations.

Advanced Weapons Elevators (AWE)

The Navy conducted a partial ammunition onload in April 2022 and a full ammunition onload in September 2022. DOT&E observed the September ammunition onload; data are still being analyzed. Observation of the lower stage AWE performance was very promising as the ordnance was transferred from the hangar bay to the magazines more efficiently than on a *Nimitz*-class carrier. Through the first 19,767 elevator dispatches, 109 individual elevator failures were reported. AWE system reliability will be critical as the Navy develops standard procedures for moving ordnance from magazines to the flight deck. The Navy's planned service-retained employment of CVN 78 in 1QFY23 will provide the first operationally representative opportunity to fully stress the AWE system.

DBR

Through June 2022, DBR demonstrated a reliability of 100 hours mean time between operational mission failures, which does not meet the minimum threshold of 339 hours mean time between operational mission failures. DBR was operationally available 94% of the time, compared to the 98% requirement.

» SURVIVABILITY

An adequate survivability assessment depends upon a combination of Full Ship Shock Trials (FSST), extensive modeling based on surrogate testing, and a total-ship survivability test (TSST). Sufficient data to assess ship survivability against close-aboard explosions should be available by the end of FY23.

From June-August 2021, the Navy conducted FSST on CVN 78 including three shock events of increasing effect. The FSST identified several survivability improvement opportunities for CVN 78 against underwater threat engagements. In 1QFY23, DOT&E will publish a classified FSST report that details these results.

The Navy plans for the Naval Surface Warfare Center Carderock Division to provide model-based vulnerability assessment reports that assess the class's vulnerability to threat weapons in 2QFY23.

The TSST is scheduled for 3QFY23. TSST is an onboard, extensive damage-control test of both the crew and associated systems.

The Revision E TEMP outlines a strategy to use land-based cyber testing in 2022 and 2023 to build up to a shipboard cybersecurity test in 2024. The first cybersecurity test event was a cyber-survivability assessment of EMALS and AAG, using systems installed at Joint Base McGuire-Dix-Lakehurst, New Jersey in June 2022. Many subsystems on the ship were tested to various degrees in both developmental and operational testing on other ship platforms. However, required CVN 78 platform-level testing has not yet occurred, and some systems specific to CVN 78 have yet to undergo any operational cyber survivability assessments.

The survivability of CVN 78 in a contested and congested electromagnetic spectrum environment has not been evaluated. Tests to do so in FY24 are part of the second phase of the test plan.

RECOMMENDATIONS

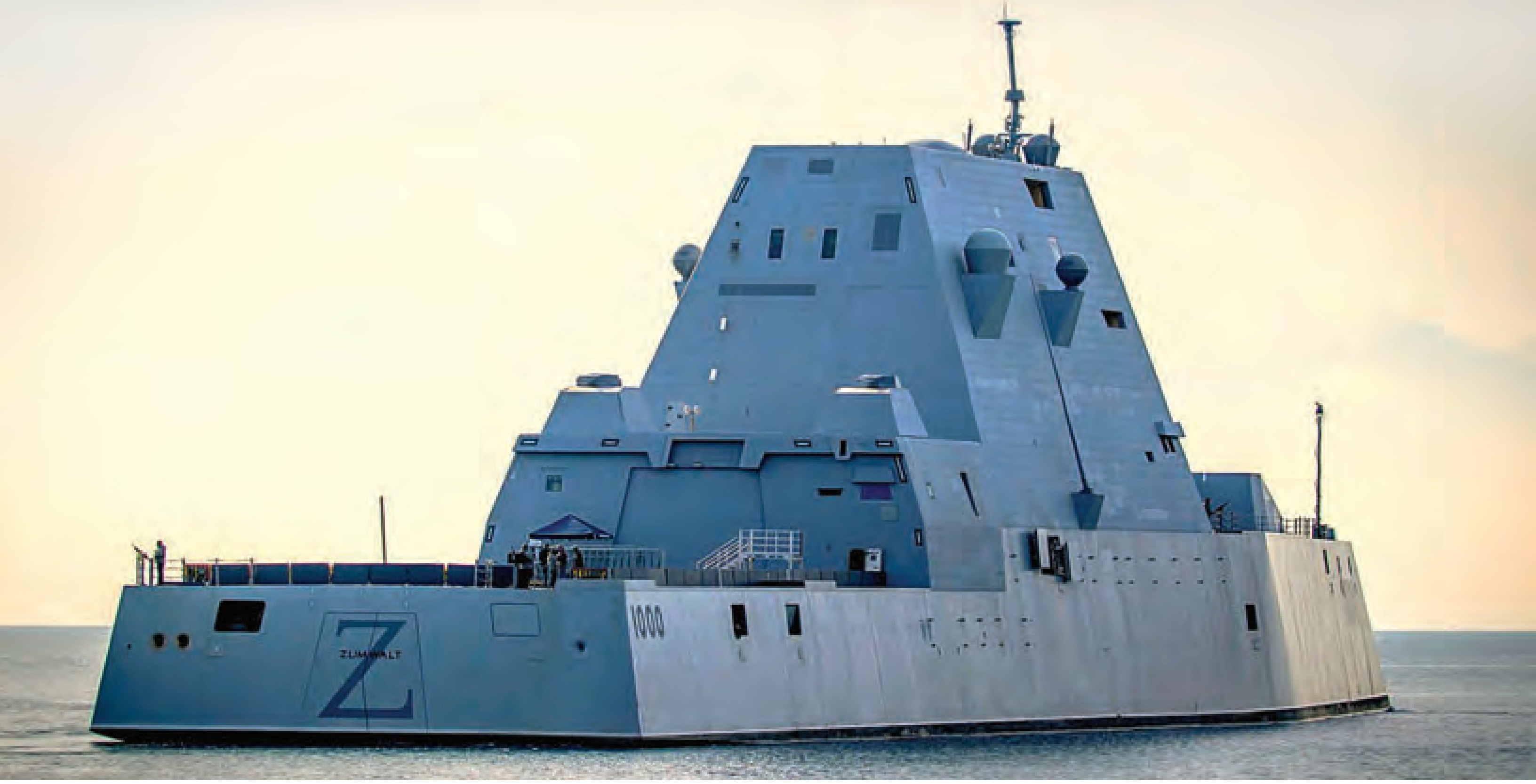
The Navy should:

1. Continue to improve reliability for EMALS, AAG, JBDs, DBR, and AWE.
2. Execute planned sortie generation and self-defense tests, as outlined in the Revision E TEMP and the IOT&E Test Plan.
3. Address combat system deficiencies identified in the classified USS *Gerald R. Ford* (CVN 78) Self-Defense Interim Assessment report, dated April 2022.
4. Continue to develop more robust capabilities to test the cyber survivability of shipboard industrial control systems.
5. Fund the modeling and simulation suite required to assess the CVN 78 PRA requirement.

6. Upon release of DOT&E's CVN 78 FSST report, develop and resource a way forward to correct deficiencies and provide it to DOT&E.
7. Complete and deliver the vulnerability assessment reports and supporting documentation.
8. Update the CVN 78 TEMP to complete the test strategy and provide resources for requirements to adequately test the combat system on CVN 79.
9. Continue to fund the maintenance availability for the SDTS to ensure its readiness to support CVN 79 combat systems testing.
10. Update the IOT&E Test Plan to complete the test requirements and scheduling for the second phase of IOT&E.

An F/A-18E Super Hornet from Carrier Air Wing EIGHT lands on CVN 78 as part of strike group integration operations, marking the ship's 9,000th arrested landing, April 2022

DDG 1000 – *Zumwalt*-Class Destroyer



The Navy commenced *Zumwalt*-class IOT&E in October 2021. Due to competing operational commitments and system readiness, initial operational testing will continue through at least FY24. Surface Warfare (SUW) operational testing is complete, but all other primary and secondary mission areas require additional testing.

SYSTEM DESCRIPTION

Zumwalt-class ships are long-range, low observable, destroyers. They are equipped with: 1) modified AN/SPY-3 Multi-Function (X-band) radar that adds a volume search capability; 2) 80 vertical launch cells to employ Tomahawk Land Attack Missiles, Standard Missiles (SM-2/SM-6), Vertical Launch Anti-Submarine Rockets, and Evolved Sea Sparrow Missiles; 3) an integrated undersea warfare system with a mid-frequency bow-mounted sonar; and 4) two Mk 46 30mm close in gun systems.

MISSION

The Joint Force Maritime Component Commander can employ *Zumwalt*-class destroyers primarily for forward-deployed offensive surface strike (OASuW) missions. Secondary missions include undersea and surface warfare dominance. The Zumwalt-class is designed for independent operations but can be integrated into Carrier or Expeditionary Strike Group operations.

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 and USS *Michael Monsoor* (DDG 1001) in 2019, and expects the delivery of USS *Lyndon B. Johnson* (DDG 1002) in FY24. The Navy is updating the *Zumwalt*-class Test and Evaluation Master Plan (TEMP) due to significant modifications to the operational requirements and warfighting concept of operations. In 2019, the Navy changed the *Zumwalt*-class's primary mission to open-ocean OASuW and codified additional changes in a June 2021 revision to the Operational Requirements Document. The *Zumwalt*-class IOT&E started in October 2021 and will inform the fleet of the class's operational performance.

» MAJOR CONTRACTORS

- Bath Iron Works – Bath, Maine
- Huntington Ingalls Industries – Pascagoula, Mississippi
- Raytheon Co., Raytheon Missiles & Defense – Tewksbury, Massachusetts
- Raytheon Missile Systems – Tucson, Arizona

TEST ADEQUACY

DDG 1000 testing to date was conducted in accordance with the DOT&E-approved test plan, observed by DOT&E, and progressed towards an adequate collection of data to support operational effectiveness and suitability assessments. FY22 testing assessed Anti-Submarine Warfare (ASW), SUW, and Anti-Air Warfare (AAW).

- ASW: USS *Michael Monsoor* executed Torpedo Defense testing in October 2021 in Nanoose Bay, Canada. Testing of the ship's ASW capability against a submarine was postponed.
- SUW: USS *Zumwalt* executed SUW testing in November and December 2021 in the Southern California operational area. The SUW operational test (OT) is complete and adequate for DOT&E to make an assessment.
- AAW: USS *Zumwalt* performed six integrated developmental/operational test events and an OT event in 2Q/3QFY22 that were adequate to support DOT&E's AAW assessment. The Navy intends to conduct additional AAW OT events in FY24. The Navy continues to develop the combat system modeling and simulation (M&S) test bed, which is required to complete OT. The Navy expects to commence AAW M&S testing in FY24.

Cyber survivability testing is planned in FY23 on USS *Zumwalt*. Strike Warfare operational testing is targeted in FY23 and FY24 on USS *Michael Monsoor*. The Navy is developing an OASuW operational test strategy for DOT&E approval in the next TEMP revision.

The Navy has not funded or planned an adequate ship survivability assessment against underwater threat weapons, to include a demonstration of residual mission capability after such engagements, through a full-ship shock trial. This assessment was not complete prior to initial deployment of USS *Zumwalt* in 4QFY22. DOT&E issued an Early Fielding Report in November 2022.

The Navy has not updated vulnerability and recoverability M&S meant to support the LFT&E survivability assessment of the DDG 1000 class to reflect the ship as built. Further, the Navy does not intend to update, validate, or accredit LFT&E survivability assessments prior to completing their LFT&E program in FY23. DOT&E will not be able to provide an assessment of the Zumwalt class's vulnerability to threat weapons without the results from validated survivability M&S that models the ship design as built.

In FY22, the Navy completed a series of Failure and Recoverability Mode (FARM) tests aboard USS *Michael Monsoor* to assess the capability of the class's mission systems to recover from system failures and to determine the effectiveness of damage control response. The scope of these tests were limited due to ongoing installation of *Zumwalt*-class mission systems and communication systems, as well as software updates and availability of auxiliary equipment due to ongoing maintenance. Despite the test limitations, FARM testing provided valuable insight into how integrated systems and software respond to non-standard operating environments that can result from battle damage.

PERFORMANCE

» EFFECTIVENESS

Not enough data are yet available to provide a preliminary assessment of DDG 1000 operational effectiveness. The AAW live missile events conducted on the DDG 1000 and previously on the Self Defense Test Ship highlighted performance limitations that may restrict operational effectiveness in the AAW mission. Final assessment of *Zumwalt*-class offensive surface strike effectiveness will be reported in a classified report following the completion of the live missile events in FY27. DOT&E issued an Early Fielding Report in November 2022 due to the Navy's deployment of USS *Zumwalt* in 4QFY22.

» SUITABILITY

Not enough data are yet available to provide a preliminary assessment of *Zumwalt*-class operational suitability.

» SURVIVABILITY

Due to vulnerability and recoverability M&S not yet being validated or reflecting the ship as-built, data are insufficient to assess *Zumwalt*-class survivability against threat weapons. Further, no data are yet available to assess DDG 1000 in a cyber-contested environment.

FARM testing aboard DDG 1001 identified equipment responses that were previously unknown. The Navy will evaluate potential changes as part of class modernization and sustainment.

RECOMMENDATIONS

The Navy should:

1. Complete IOT&E in accordance with the DOT&E-approved test plan.
2. Complete revision of the TEMP that includes an adequate test strategy for the delivered OASuW capability.
3. Complete development and validate the combat system M&S test bed, to include debris, missile, radar, and electronic warfare models.
4. Document the risk to the warfighter associated with incomplete component shock qualification and lack of full-ship shock trial prior to deployment.
5. Work with DOT&E to develop an updated LFT&E strategy in FY23 to evaluate the as-built survivability of the DDG 1000 class with the next TEMP update, including updated survivability M&S and remaining shipboard testing.
6. Sufficiently fund modernization and sustainment of the DDG 1000 class to include improvements determined from FARM testing.

E-2D Advanced Hawkeye

In FY22, the Navy conducted integrated testing (IT) on E-2D Delta System Software Configuration Build 4 (DSSC-4). DSSC-4 improves the Hawkeye's command and control capability and is the fourth in a series of biennial hardware and software upgrades to the E-2D. The Navy intends to begin operational testing of DSSC-4 in 1QFY23 to support a planned fleet release in 3QFY23.

SYSTEM DESCRIPTION

The E-2D Advanced Hawkeye is a carrier-based, airborne, early warning, and command and control platform. Its sensor and communication 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:

- The AN/APY-9 phased array radar that combines mechanical and electronic scan modes
- Tactical Targeting Network Technology data link
- Multi-Functional Information Distribution System

- Cooperative Engagement Capability
- Satellite communications
- Electronic Support Measures
- Electronic Protection
- Aerial refueling

The E-2D Advanced Hawkeye system also includes all simulators, interactive computer media, and documentation to conduct maintenance, as well as aircrew initial and follow-on training.

MISSION

The E-2D Advanced Hawkeye provides all-weather airborne early warning, airborne battle management, and command and control functions, and supports Navy Integrated Fire Control and theater air and missile defense missions for the Carrier Strike Group and Joint Force Commander. 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 that is in its fourth FOT&E period (OT-D4). DSSC-4 improves beyond line-of-sight communications and sensor integration and incorporates tactical targeting networking technology. During OT-D4, the Navy intends to assess DSSC-4 upgrades and Hawkeye Integrated Training Systems. DSSC-4 serves as the baseline integration of capabilities that will be fully delivered in DSSC-5 and later upgrades.

In February 2022, DOT&E approved the DSSC-4 and DSSC-5 Test and Evaluation Master Plan and the Navy's data collection plan for DSSC-4 IT. The Navy is finishing development of the DSSC-4 operational test plan and an operational test readiness review is scheduled for early 1QFY23. The evaluation of DSSC-4 will occur through a cumulative collection of integrated and operational test data. IT began in 2QFY22, and operational testing is scheduled to begin in 1QFY23. The evaluation will inform an FY23 deployment decision and determine fielding risks and delivered capabilities for DSSC-4. DSSC-5 is scheduled to begin OT in FY25.

Since the last Annual Report on E-2D, DSSC-3.1 was incorporated into the Advanced Hawkeye. DSSC-3.1 is a minor upgrade that involves the E-2D's Multi-Functional Information Distribution System Joint Tactical Radio System Concurrent Multiple Netting 4 terminal and other navigation and communications systems.

» MAJOR CONTRACTOR

- Northrop Grumman Aerospace Systems – Melbourne, Florida

TEST ADEQUACY

The major IT events executed in FY22 were conducted in accordance with the DOT&E approved data collection plan at White Sands Missile Test Range in May and at Exercise Gray Flag at Point Mugu, California in August. The scenarios at Gray Flag were robust, operationally representative Large Force Exercises involving IT and OT across the joint force and were observed by DOT&E. Data from these events are still being analyzed. An assessment of OT-D4 test adequacy is pending the Navy's completion of the operational test plan.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Not enough data are yet available to evaluate DSSC-4's operational effectiveness, suitability, and cyber survivability. DOT&E will provide an assessment after operational testing is complete in FY23.

During DSSC-4 IT, shortfalls in aircraft availability and systems reliability have challenged collecting adequate data which contributed to a short delay in beginning DSSC-4 OT. While recent fleet data has demonstrated gradual improvements in reliability, availability, and logistic supportability, improvements in these areas are still warranted.

Developmental testing of DSSC-3.1 (with operational test assistance) was completed in July 2021. The Navy's Operational Test and Evaluation Force completed an assessment of operational capability identifying several deficiencies, the results of which were released in a classified report on March 14, 2022.

RECOMMENDATIONS

The Navy should:

1. Submit an OT-D4 test plan for DOT&E approval that details an adequate test strategy and sufficient test resources to assess the operational effectiveness, suitability, and cyber survivability of DSSC-4.
2. Continue to improve E-2D reliability, availability, and logistic supportability.
3. Continue to correct the deficiencies identified in the classified OPTEVFOR DSSC-3.1 report.

Evolved Sea Sparrow Missile (ESSM) Block 2

In July 2022, the Navy delivered initial rounds of the Evolved Sea Sparrow Missile (ESSM) Block 2 for Aegis platforms to fleet inventory, prior to the completion of IOT&E. DOT&E submitted a classified Early Fielding Report (EFR) in September 2022 that includes anomalies that the Navy should address prior to the expected completion of IOT&E in FY25. Due to IOT&E being incomplete, insufficient data are available to determine operational effectiveness, suitability, lethality, or survivability in a contested environment.

SYSTEM DESCRIPTION

The ESSM Block 2 is a short-to-medium-range, ship-launched, guided missile intended to provide defensive, hard-kill engagement capability against anti-ship cruise missiles. ESSM Block 2 leverages Standard Missile 6 technology to reduce reliance on illuminator support and mitigate challenges in missile sequencing that are inherent in high-density stream raids. Semi-active guidance (using shipboard illuminators) is retained from ESSM Block 1. The ESSM Block 2 also features a new blast fragmentation warhead. The Navy intends the ESSM Block 2 seeker upgrade to improve performance against stressing air warfare threats (including stream raids) in challenging electromagnetic spectrum environments.

The full capability of the ESSM Block 2 is not available without an update to the Aegis Weapon System that remains in development. The legacy combat system can employ the ESSM Block 2 but initializes the weapon as an ESSM Block 1 missile. Although initialized as an ESSM Block 1 missile, the ESSM Block 2 functions as an ESSM Block 2 but without some enhancements. The Navy will evaluate this functional compatibility mode in the first phase (Phase 1) of IOT&E. The Navy will evaluate the full capability, or the optimized capability mode, in a second phase (Phase 2) of IOT&E when the updated Aegis Weapon System is available. Operational testing of ESSM Block 2 employed from Ship Self Defense System platforms is planned for FOT&E.

MISSION

The Joint Force Commander utilizes the ESSM Block 2 as a ship self-defense weapon against anti-ship cruise missiles as part of a layered defense of Aegis cruisers/destroyers and Ship Self Defense System Mk 2 platforms, to include aircraft carriers and amphibious ships.

PROGRAM

The ESSM Block 2 is an Acquisition Category II program. In December 2021, the Navy declared ESSM Block 2 initial operational capability for Aegis platforms. DOT&E approved the ESSM Block 2 Test and Evaluation Master Plan in March 2022. In July 2022, the Navy delivered initial rounds of the ESSM Block 2 for Aegis platforms to fleet inventory. DOT&E submitted a classified EFR in September 2022 based on the limited test conducted to date. The Navy expects to complete Phase 1 IOT&E in FY23 and commence Phase 2 in FY25.

» MAJOR CONTRACTOR

- Raytheon Missiles and Defense – Tucson, Arizona

TEST ADEQUACY

In August 2021, the Navy commenced Phase 1 IOT&E in accordance with a DOT&E-approved test plan, and observed by DOT&E. Data from both phases of IOT&E are required for determination of operational effectiveness, suitability, and cyber survivability of the ESSM Block 2. The Navy expects to complete Phase 2 IOT&E in FY25.

Although the Navy intends to use modeling and simulation (M&S) in Phase I IOT&E, the Navy has not accredited the intended M&S for operational evaluation. The Navy has not yet scheduled cyber survivability testing.

The Navy completed lethality testing in FY20 but has not completed associated analysis or provided a lethality assessment report.

PERFORMANCE

» EFFECTIVENESS

Data are insufficient to determine operational effectiveness. Analysis of live test flights of ESSM Block 2 identified anomalies that are detailed in the DOT&E EFR published in September 2022.

» SUITABILITY

Data are insufficient to determine operational suitability, including missile in-flight reliability and launch availability. Early estimates of suitability metrics are detailed in the DOT&E EFR published in September 2022.

» SURVIVABILITY

Data are insufficient to determine survivability. The Navy has yet to conduct operational cyber survivability assessment or assess performance in a contested electromagnetic spectrum environment.

» LETHALITY

No assessment of lethality can be made due to Navy analysis and reporting of lethality testing being incomplete. A summary of the lethality tests is detailed the DOT&E EFR published in September 2022.

RECOMMENDATIONS

The Navy should:

1. Determine and correct the root cause of the anomalies identified in the September 2022 EFR prior to Phase 2 IOT&E.
2. Complete cyber survivability assessment prior to operational deployment.
3. Complete development and accredit ESSM Block 2 M&S capability prior to Phase 2 IOT&E.
4. Complete post-test lethality analysis and final reporting of the lethality assessment as soon as feasible.

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

F/A-18 Infrared Search and Track (IRST) Block II operational testing is delayed until 2QFY24 due to hardware and software delivery delays. To be operationally effective, the IRST Block II program needs to resolve several open deficiencies from previous IRST versions, as well as those discovered during Block II developmental testing with prototype systems. The proposed schedule allows minimal time for problem discovery and deficiency resolution prior to the planned start of IOT&E, which could delay delivery of production-representative software and have a negative impact on effectiveness and suitability during IOT&E. The Navy did not conduct test events during FY22.

SYSTEM DESCRIPTION

The ASG-34A(V)1 F/A-18E/F IRST is a centerline-mounted pod with a long-wave infrared sensor which 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, thus reducing the fuel capacity of the FPU-13/A to 340 gallons compared to the 480-gallon FPU-12/A centerline fuel tank it replaces. Therefore, IRST integration results in less fuel available and reduced time-on-station for the F/A-18E/F. The IRST acts as a complementary sensor to the AN/APG-79 fire control radar in a heavy electronic attack or radar-denied environment. It operates autonomously, or in combination with other sensors, to support the guidance of beyond-visual-range air-to-air missiles, including the AIM-120 Advanced Medium-Range Air-to-Air Missile and AIM-9X Sidewinder Block II.

PROGRAM

The F/A-18 IRST Block II is an Acquisition Category IC program. DOT&E approved the Milestone C Test and Evaluation Master Plan in May 2021. IOT&E is scheduled to begin in 2QFY24 in support of full-rate production. The Navy intends to field the IRST Block II system to carrier-based F/A-18E/F Super Hornet squadrons to improve lethality and survivability in air superiority missions against advanced threats.

MAJOR CONTRACTORS

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

TEST ADEQUACY

The Navy plans to conduct IOT&E between March and July 2024 and has not yet submitted the IOT&E plan to DOT&E for approval.

PERFORMANCE

» EFFECTIVENESS

To be operationally effective, the IRST Block II program needs to resolve several deficiencies existing from previous IRST versions, as well as those noticed during Block II developmental testing (DT) of prototype systems. Additionally, the Navy must improve the Super Hornet's operating software and correct existing deficiencies to enable IRST to be an effective contributor to aircraft fire control solutions. The IRST Block II prototype pod demonstrated tactically relevant detection ranges against operationally relevant targets during initial DT events. However, integration into the overall F/A-18E/F software solution must convert long-range target detections into stable system tracks to facilitate weapons employment. The ability of the Navy and the contractor to fix the critical issues on schedule is the most significant performance risk to successful IOT&E.

» SUITABILITY

IRST Block II prototype systems used in DT demonstrated reliability well below the Navy's requirements. Additionally, the prototype systems do not possess fault detection and identification, which makes troubleshooting and fault correction verification detection difficult for maintainers and aircrew. The production-representative versions of the system slated for use in IOT&E are delayed, which creates uncertainty for maintenance process maturity and reliability growth and could negatively affect suitability during IOT&E.

» SURVIVABILITY

IRST Block II contributes to the survivability of the F/A-18E/F by providing target tracks in a contested and congested electromagnetic spectrum environment, but it has yet to be tested in an operational environment.

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

RECOMMENDATIONS

The Navy should:

1. Address the known IRST Block II and Super Hornet operating hardware and software deficiencies.
2. Continue to test unproven capabilities in developmental testing to prepare the system for IOT&E in order to adequately demonstrate operational effectiveness, suitability, and survivability.

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

Both the F/A-18E/F Super Hornet and EA-18G Growler programs experienced development challenges in the latest software configuration set (SCS) update. As a result, Phase II of SCS H16 operational test (OT) was approved in May 2022 for both Block II and Block III F/A-18E/F Super Hornet variants, and for the EA-18G Growler, while FOT&E events commenced in 4QFY22. The Navy expects to complete F/A-18E/F Block II and Block III OT in 1QFY23 with fleet release in December 2022. The EA-18G Growler OT will continue into 2023.

SYSTEM DESCRIPTION

The F/A-18E/F Super Hornet is a twin-engine, supersonic, all-weather, carrier-capable, multirole combat aircraft performing a variety of roles, including air superiority, fighter escort, suppression of enemy air defenses, reconnaissance, forward air control, close and deep air support, day and night strike, and aerial refueling. The F/A-18E/F Super Hornet is the replacement for the F/A-18A through D and the F-14, and it complements the F-35C in a carrier environment. The F/A-18E/F Block III Super Hornet aircraft leverages ongoing production of the Kuwaiti Super Hornet; it is also available as a Block II aircraft retrofit. F/A-18E/F Block III Super Hornets include upgraded hardware, advanced cockpit displays, and improved networking capability.

The EA-18G Growler is a two-seat, electronic attack variant of the F/A-18E/F Super Hornet that can provide standoff, escort, and self-protection jamming using both noise and deception techniques against land-based and airborne radar systems. The EA-18G Growler carries up to five AN/ALQ-99 tactical jammer system pods mounted under the wings and fuselage, which integrate with the internal AN/ALQ-218 electronic warfare system for detection and jamming. The EA-18G Growler also employs 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 ALQ-249 (Next Generation Jammer – Mid Band) on the EA-18G Growler to eventually replace the ALQ-99.

The F/A-18E/F Super Hornet and EA-18G Growler are both supported by the same SCS product line. The currently fielded SCS for both aircraft is H14. The next SCS, H16, is currently undergoing testing in accordance with the DOT&E-approved operational test plan. SCS H16 brings improved capabilities to the APG-79 radar for both aircraft and includes two developmental branches: one for Block II F/A-18E/F and E/A-18G, and one for Block III F/A-18E/F. SCS H18, which is scheduled to begin operational test in FY23 in support of a phased fleet deployment approach, is intended to merge the two SCS H16 branches in to a single product line. SCS H18 integrates with EA-18G Growler capability modifications, such as ALQ-249, and brings EW and radar software improvements to the F/A-18E/F Super Hornet along with new weapons integration.

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 to provide organic aerial refueling capability to the 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 EA platform, organic to the carrier strike group or integrated in the Joint Force. It can also be used in a tactical reconnaissance role.

PROGRAM

The F/A-18E/F Super Hornet is an Acquisition Category 1C program. In 2021, DOT&E approved SCS H16 phased entry into OT. DOT&E approved the second phase of F/A-18E/F and E/A-18G SCS H16 testing in May 2022. The F/A-18E/F Block II and Block III Super Hornet SCS H16 OT commenced with events in August and September 2022 to support the planned decision to field SCS H16 to the fleet by December 2022, but SCS H16 has shown reliability and performance issues throughout operational test. SCS H18 FOT&E is scheduled to begin during 3QFY23 after operational test readiness review is conducted in April 2023. SCS H18 will include EW and radar enhancements from SCS H16, along with weapons integration software for the Long-Range Anti-Ship Missile, Small Diameter Bomb II, and Joint Advanced Tactical Missile for the F/A-18E/F Super Hornet.

The Navy is also leveraging production of the Kuwaiti Super Hornet to purchase F/A-18E/F Block III aircraft, which include upgraded hardware, advanced cockpit displays, and improved networking capability. Boeing delivered multiple F/A-18E/F Block III Super Hornets in 2021 and the Navy plans to retrofit existing Block II aircraft with the Block III upgrades.

The EA-18G Growler is an Acquisition Category 1D program. DOT&E placed the EA-18G Growler back on oversight in 2022 due to significant planned upgrades and testing required for SCS H16 and H18. Operational testing of EA-18G Growler capability modifications were deferred to SCS H18 due to delays in EA-18G Growler hardware upgrades.

» MAJOR CONTRACTORS

- The Boeing Company, Integrated Defense Systems – St. Louis, Missouri
- Raytheon Intelligence and Space – Forest, Mississippi
- General Electric Aviation – Evendale, Ohio
- Northrop Grumman Corporation – Bethpage, New York
- Lockheed Martin, Missiles and Fire Control – Orlando, Florida

TEST ADEQUACY

In accordance with the DOT&E-approved test plan, the Navy is using continuous response variables to evaluate SCS H16 instead of relying on binary response data. This approach will improve test adequacy and result in a more robust evaluation of F/A-18E/F Super Hornet performance as compared to OT of previous SCS releases. DOT&E is also working with the Navy to incorporate Open Air Battle Shaping and high-fidelity threat radar emulators with Active Electronically Scanned Arrays (AESA) into future test events, to include SCS H18 OT. F/A-18E/F Block II and III Super Hornet OT was delayed until September 2022.

The Navy executed the DOT&E-approved cyber test plan for F/A-18E/F Block II and E/A-18G SCS H16, but chose to defer planned cybersecurity testing for Block III SCS H16 until SCS H18 OT due to hardware delivery and resource constraints, and to resolve SCS H16 Block III software deficiencies.

PERFORMANCE

» EFFECTIVENESS

Past effectiveness evaluations of SCS versions prior to H16 concluded that the F/A-18E/F Super Hornet is effective in both air-to-air and air-to-surface environments. The SCS H16 FOT&E evaluates new and enhanced F/A-18E/F Super Hornet capabilities intended to bolster platform mission effectiveness. Effectiveness evaluations for F/A-18E/F Super Hornet Block II and Block III SCS H16 are anticipated to complete in FY23. The Navy has yet to conduct an end-to-end multiple AIM-120 missile test to demonstrate the APG-79 AESA radar can support this required capability.

Due to delays in hardware capability modifications for the EA-18G Growler, the Navy deferred OT for most of the capabilities introduced by SCS H16 to the FOT&E phase for SCS H18. The initial builds of SCS H16 were designed to integrate with EA-18G Growler hardware modifications such as Next Generation Jammer – Mid Band (NGJ-MB), but since hardware upgrade delivery dates proved unpredictable, SCS H16 testing will continue with a focus on software improvements. As a result, EA-18G Growler SCS H16 FOT&E will focus on changes in software performance when compared to the EA-18G Growler performance threshold established with SCS H14, while hardware related capability improvements will be tested with SCS H18.

» SUITABILITY

Although DOT&E previously determined the Super Hornet to be operationally suitable, the APG-79 AESA radar has not met its reliability requirements outlined in the Operational Requirements Document. DOT&E will include an updated AESA radar evaluation as part of the final assessment of Block II SCS H16 operational suitability in the Block II SCS H16 report in 4QFY23.

» SURVIVABILITY

The Navy is leveraging completed developmental cybersecurity testing to inform the evaluation of Block II SCS H16 survivability in a cyber-contested environment. Additional SCS H16 cybersecurity testing was delayed due to software deficiencies and hardware delivery and resource constraints. The Navy has not yet addressed previous cybersecurity deficiencies nor developed a comprehensive roadmap to inform future cybersecurity testing.

RECOMMENDATIONS

The Navy should:

1. Complete planned SCS H16 and H18 operational test in order to evaluate needed capability improvements to the FA-18E/F Super Hornet and EA-18G Growler fleet.
2. Conduct comprehensive F/A-18E/F Super Hornet and EA-18G Growler cybersecurity testing and address previously identified cybersecurity deficiencies.
3. Improve the reliability of the APG-79 AESA radar.
4. Incorporate Open Air Battle Shaping and high-fidelity AESA threat radar emulators into future test events, to include SCS H18 FOT&E.

FFG 62 *Constellation*-Class – Guided Missile Frigate

In FY22, the Navy conducted an early operational assessment (EOA) of the *Constellation*-class (FFG 62-class) design in accordance with a DOT&E-approved test plan. Also in FY22, the Navy modified the FFG 62 design to include the Thales Combined Active Passive Towed Array Sonar-4 (CAPTAS-4) system, a variable depth sonar.

SYSTEM DESCRIPTION

The FFG 62 will be smaller and less capable than U.S. Navy destroyers and cruisers, but will have more offensive capability and survivability than previous small surface combatants (e.g., Littoral Combat Ships). Major weapons systems of FFG 62 include:

- Aegis Combat System
- Enterprise Air Surveillance Radar (AN/SPY-6(V)3F)
- Surface Electronic Warfare Improvement Program Block 2 (AN/SLQ-32(V)6)
- Mk 41 Vertical Launch System with Evolved Sea Sparrow Missiles and Navy Standard Missiles
- Mk 49 Guided Missile Launching System with Rolling Airframe Missile
- AN/SQQ-89(V)16 Undersea Warfare Combat System

- AN/SLQ-25 Nixie
- AN/SPS-73(V)18 Next Generation Surface Search Radar
- Mk 110 57-mm Gun (with Advanced Low-Cost Munitions Ordnance)
- Over-the-Horizon Weapon System
- MH-60R Seahawk helicopter (configurable to fire surface attack Hellfire missiles and MK 54 Lightweight torpedoes)
- MQ-8C Fire Scout Vertical Take-off and Landing Tactical Unmanned Aerial Vehicle with MD-4A Mission Control System

MISSION

The Maritime Component Commander will employ the *Constellation*-class to support the National Defense Strategy across the full range of military operations. Specific mission areas include anti-air warfare, anti-submarine warfare, surface warfare, electronic warfare/information operations, and intelligence, surveillance, and reconnaissance missions.

PROGRAM

The FFG 62-class is an Acquisition Category IB Major Defense Acquisition Program that achieved Milestone B in April 2020. The Navy approved the award of the Detail Design and Construction contract for the first ship, with options for up to ten additional ships, and entry into the Detail Design and Construction (Production) phase with a low-rate initial production quantity of twenty ships. The Navy intends to deliver the lead ship by September 2026.

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

DOT&E approved the FFG 62 LFT&E strategy in April 2020. The FFG 62 LFT&E strategy included full-ship shock trials with the option of pursuing a modeling and simulation (M&S)-based shock trial alternative. However, after conducting a scoping study, the Navy concluded that an adequate shock trial alternative for FFG 62 would cost approximately two and half times more than a comparable full-ship shock trial. Therefore, the Navy will go forward with a full-ship shock trial in 3QFY30.

» MAJOR CONTRACTOR

- Fincantieri Marinette Marine Corporation – Marinette, Wisconsin

TEST ADEQUACY

Between February 2022 and July 2022, the Navy conducted an EOA of the FFG 62 ship design. This was done in accordance with a DOT&E-approved test plan, and observed by DOT&E. Subject matter experts in operations and maintenance reviewed the FFG 62 design to identify risks that could affect operational effectiveness and suitability. The EOA provides the Navy with opportunity to identify and consider modifications to the ship design and informs operational testers in their development of an IOT&E test strategy.

In FY22, the Navy conducted testing against a large scale-model of a generic ship incorporating characteristics typical of Navy standard ship structure to generate response data of the test article to underwater explosions. This was done in accordance with the DOT&E-approved test plan, and observed by DOT&E. These tests subjected 100-foot long hulls constructed similar to Navy ships to damage that resulted in plastic deformation. The results from these tests will be used for validation of survivability models used to predict damage magnitude and extent from threat weapons.

PERFORMANCE

» EFFECTIVENESS

Not enough data are yet available to assess operational effectiveness due to the ship's early stage of development.

Preliminary assessment from the EOA suggest:

- Reduced developmental risk primarily due to the inclusion of previously fielded systems in the FFG 62 ship design.
- Some areas that could provide integration and/or performance challenges:

- FFG 62 will not include a tracker illuminator system typically installed on other Aegis platforms.
- In FY22, the Navy modified the FFG 62 design to include the foreign-designed, Thales CAPTAS-4 system, a variable depth sonar. While the Navy believes the integration of the CAPTAS-4 to the AN/SQQ-89 and the platform is low risk, DOT&E is unable to assess the integration risk at this time.
- FFG 62 crew size is limited to an estimated 193 officers and enlisted sailors with an additional 27 personnel that serve in the embarked aviation detachment. Mission success and sustainability will depend upon effective system autonomy/automation and human system interfaces.

DOT&E will submit a classified EOA report upon completion of analysis, expected in 2QFY23.

» SUITABILITY

Not enough data are yet available to assess operational suitability due to the ship's early stage of development.

» SURVIVABILITY

Not enough data are yet available to assess ship survivability.

Ongoing LFT&E testing, which include near-contact explosive testing, extended distance multiple plate ballistic testing, and large scale underwater explosion testing, have closed outstanding vulnerability knowledge gaps and are expected to enable M&S validation.

In FY22, the Navy continued to update M&S to incorporate new capabilities, including improvements to their blast and whipping codes. DOT&E continues to work with the Navy on M&S plans that will support validation and accreditation of these tools to support the Detail Design Survivability Assessment Report in FY25.

RECOMMENDATIONS

The Navy should:

1. Provide an update to the FFG 62 TEMP that includes the strategy to test anti-air warfare mission capability by FY24.
2. Procure available and appropriate CAPTAS-4 technical data to mitigate performance risk and potentially reduce scope of operational testing.
3. In collaboration with operators and operational testers, closely monitor the development of the mission system autonomy/automation components in the ship design to minimize risk to mission performance and system maintenance capability.

LHA 6 Flight 0 Amphibious Assault Ship

Between March and April 2022, the Navy and Marine Corps demonstrated capability of the USS *Tripoli* (LHA 7) to operate in the F-35B-heavy configuration consisting of 20 F-35B Joint Strike Fighter aircraft, 3 SH-60S Seahawk helicopters, a Marine Aviation Combat Element, and a Marine Command Element. No preliminary assessment of performance attributes can be made from this FOT&E event as analysis remains in progress. DOT&E expects to deliver an FOT&E report in 2QFY23.

SYSTEM DESCRIPTION

The USS *America* (LHA 6) class are large-deck amphibious assault ships intended to provide transportation and operational support for deployed Marine Corps forces, aircraft squadrons (including the F-35B Joint Strike Fighter, the AV-8B, the MV-22, the CH-53, the AH-1, the UH-1, and the H-60), and the Marine Air Ground Task Force. The LHA 6 Flight 0, commencing with USS *America* (LHA 6), maximizes aviation capability (i.e., flight deck and hangar deck) and includes no well deck. The LHA 6 Flight 1 variant, commencing with USS *Bougainville* (LHA 8), reduces aviation capability to support a well deck capable of deploying two Landing Craft Air Cushion hovercraft. LHA 6 class ships are equipped with the Ship Self-Defense System, the primary control and decision system that integrates air search radars, trackers, an electronic warfare system, and hard-kill and soft-kill weapons to provide self-defense against anti-ship cruise missiles.

MISSION

Joint Force Commanders will employ the USS *America* (LHA 6) class amphibious assault ships as the primary command ship and aviation platform for an Amphibious Ready Group or Expeditionary Strike Group and associated Marine Expeditionary Unit/Marine Air-Ground Task Force.

PROGRAM

The LHA 6 program (formerly the LHA (R) program) is an Acquisition Category IC program. The Navy completed the LHA 6 Flight 0 IOT&E in 2017 and an operational assessment of the LHA 6 Flight 1 design in 2020. The Navy is revising the Test and Evaluation Master Plan to include the test strategy and resources for OT&E and LFT&E of LHA 6 Flight 1 and expects to deliver it for DOT&E approval in FY23. The Navy expects to deliver the USS *Bougainville* (LHA 8) in FY25 and subsequently conduct FOT&E.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

Between March and April 2022, the Navy and Marine Corps tested the USS *Tripoli* (LHA 7) in the F-35B-heavy configuration consisting of 20 F-35B Joint Strike Fighter aircraft, 3 SH-60S Seahawk helicopters, a Marine Aviation Combat Element, and a Marine Command Element. Testing evaluated the ability to embark, operate, support and maintain the fixed and rotary wing aircraft in this configuration. The Navy conducted this FOT&E period of the LHA 6 Flight 0 in accordance with a DOT&E-approved test plan, and tests were observed by DOT&E. Testing was adequate for demonstration of capability. Additionally, the test will inform future F-35B-heavy operational concepts and tactics, techniques, and procedures.

In FY22, the Navy conducted no LFT&E of LHA 6 Flight 0 or operational test of LHA 6 Flight 1. DOT&E and the Navy have yet to agree on a LFT&E strategy to evaluate the survivability of the LHA 6 Flight 1 to air delivered or underwater kinetic threats.

PERFORMANCE

» EFFECTIVENESS

Under the operational conditions imposed during FOT&E, the LHA 6 Flight 0 demonstrated capability to operate in the F-35B-heavy configuration consisting of 20 F-35B Joint Strike Fighter aircraft, 3 SH-60S Seahawk helicopters, a Marine Aviation Combat Element, and a Marine Command Element. However, no preliminary assessment of mission performance attributes can be made from this FOT&E event as analysis remains in progress. DOT&E expects to deliver an LHA 6 Flight 0 FOT&E report in 2QFY23.

» SUITABILITY

Insufficient data are available to determine operational suitability from the FOT&E, however LHA 6 Flight 0 suitability was evaluated as satisfactory during IOT&E. FOT&E suitability evaluation is limited to reliability, maintainability, logistics supportability, and availability of ship's systems that directly supported F-35B operations. DOT&E observed no significant issues related to suitability, but analysis remains in progress. DOT&E expects to deliver an LHA 6 Flight 0 FOT&E report in 2QFY23.

» SURVIVABILITY

No data are available to change the lethality assessment of LHA 6 Flight 0 from IOT&E or assess survivability of LHA 6 Flight 1.

RECOMMENDATION

The Navy should:

1. Collaborate with DOT&E to deliver an LFT&E strategy that adequately evaluates the survivability of the LHA 6 Flight 1 with the update to the TEMP in FY23.

F-35B onboard USS Tripoli *(LHA 7) for FOT&E event, April 2022*

Littoral Combat Ship (LCS)

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

In August 2022, the Navy commenced IOT&E of the Littoral Combat Ship (LCS) Mine Countermeasure (MCM) Mission Package (MP) and scheduled completion of the remaining LCS MCM MP operational test events in FY23. In February 2022 and August 2022, the Navy conducted cyber survivability testing of the LCS Surface Warfare (SUW) MP Increment 3. DOT&E released the LCS SUW MP Increment 3 IOT&E report in May 2022 with an update for cyber survivability expected in 2QFY23. The President's Budget 2023 includes a complete divestment of the LCS Anti-Submarine Warfare (ASW) MP, initiating a Nunn-McCurdy breach of the LCS MCM and SUW MP programs.

SYSTEM DESCRIPTION

The LCS is a small surface combatant designed for littoral operations, but also capable of executing open ocean missions. The LCS comprises two seaframe variants: the *Freedom* variant and the *Independence* variant. The *Freedom* variant is a mono-hull design constructed of steel (hull) and aluminum (deckhouse) with two steerable and two fixed-boost waterjets driven by a combined diesel and gas turbine main propulsion system.

The *Independence* variant is an aluminum trimaran with two steerable waterjets driven by diesel engines and two steerable waterjets driven by gas turbine engines. LCS seaframes host and derive mission capability from the SUW and MCM MPs.

The SUW MP derives capability from the following components:

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

The MCM MP derives capability from the following baseline components:

- AN/ASQ-235 Airborne Laser Mine Detection System (ALMDS)
- AN/AQS-20C Minehunt
- Airborne Mine Neutralization System (AMNS)
- Unmanned Influence Sweep System

The MCM MP will incorporate the following systems pending continued system development:

- Knifefish Block I unmanned undersea vehicle
- AN/DVS-1 Coastal Battlefield Reconnaissance and Analysis Block II
- Barracuda Mine Neutralization System

MISSION

The Maritime Component Commander will employ LCS to conduct MCM or SUW tasks based upon the MP installed in the seaframe. Because of capabilities inherent to the seaframe, commanders can employ LCS in a maritime presence role with either MP and support deterrence operations. In addition, with the Maritime Security Module installed as part of the SUW MP, the ship can conduct Maritime Security Operations including visit, board, search, and seizure of ships suspected of transporting contraband.

The Navy employs LCS alone, or within a group of ships, to prepare the environment for joint forces access to littoral regions by conducting MCM and SUW operations, possibly under an air defense umbrella.

PROGRAM

The LCS seaframes and the combined MPs are each Acquisition Category IC programs. Further, several components within the MPs are individual programs of record themselves. In 2018, DOT&E approved an update to the LCS Test and Evaluation Master Plan (TEMP) that accounted for changes in the test design to evaluate the MPs on the two seaframe variants.

The President's Budget 2023 included a complete divestment of the LCS ASW MP. The Navy originally planned to purchase 11 ASW MPs, but the Navy now contends that changes in threat capabilities and limitations in space, weight, and power on the LCS variants no longer support the continued development of the ASW MP. This divestment of the ASW MP triggered a significant Nunn-McCurdy breach due to the reduction of the aggregate MPs procured. The reduction results in a 37.3 percent increase to the cost of the remaining MPs, exceeding the 30 percent threshold for a significant Nunn-McCurdy breach.

The Navy intended to make an update to the TEMP in FY21 to account for additional changes in the test program for the MCM MP. However, the Navy now intends to deliver the update for DOT&E approval in FY23 and include the ASW MP divestment. Additionally, the Navy expects to provide the TEMP for the MCM Unmanned Surface Vehicle (USV) with Minehunt payload to DOT&E for approval in 1QFY23.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

In August 2022, the Navy conducted operational test of the LCS MCM MP from the USS *Cincinnati* (LCS 20) in the Southern California Operating

Areas. The Navy evaluated the capability of the LCS MCM MP to execute mine clearance missions against threat-representative mine surrogates. Testing was sufficient to demonstrate coordinated command and control of the baseline capabilities of the MCM MP. The Navy further conducted IOT&E of the MCM USV with the Minehunt payload in conjunction with these test events of the LCS MCM MP. Tests were in accordance with DOT&E-approved test plans, and observed by DOT&E.

In February 2022 and August 2022, the Navy conducted the cooperative vulnerability and penetration assessment and the adversarial assessment to evaluate the cyber survivability of LCS SUW MP Increment 3. Testing was in accordance with a DOT&E-approved test plan and observed by DOT&E. Additionally, the Navy scheduled evaluation of the cyber survivability of the LCS MCM MP in FY23.

The Navy fielded the AMNS and ALMDS components of the MCM MP in 2016 without conducting IOT&E for either component. Limited testing of these two components are included in the August 2022 IOT&E for the LCS MCM MP. As such, insufficient data are available from operational tests to characterize the performance of these components or their contribution to the LCS MCM MP effectiveness. DOT&E is working with the Navy to identify representative performance data of these components from fleet training and certification events. Should insufficient data exist to characterize the performance of these components, testing of the LCS MCM MP will not be adequate to assess operational effectiveness. The Navy is evaluating options for additional test should this be the case.

PERFORMANCE

» EFFECTIVENESS

Insufficient data are available to assess operational effectiveness of the LCS MCM MP. No preliminary assessment of performance metrics are available as analysis remains in progress.

» SUITABILITY

Insufficient data are available to assess operational suitability of the LCS MCM MP. No preliminary assessment of suitability metrics are available as analysis remains in progress.

» SURVIVABILITY

The Navy completed the LFT&E survivability assessment of the LCS seaframes in FY19. LFT&E analysis highlighted several LCS design features that drive survivability performance of each variant against selected kinetic threat categories.

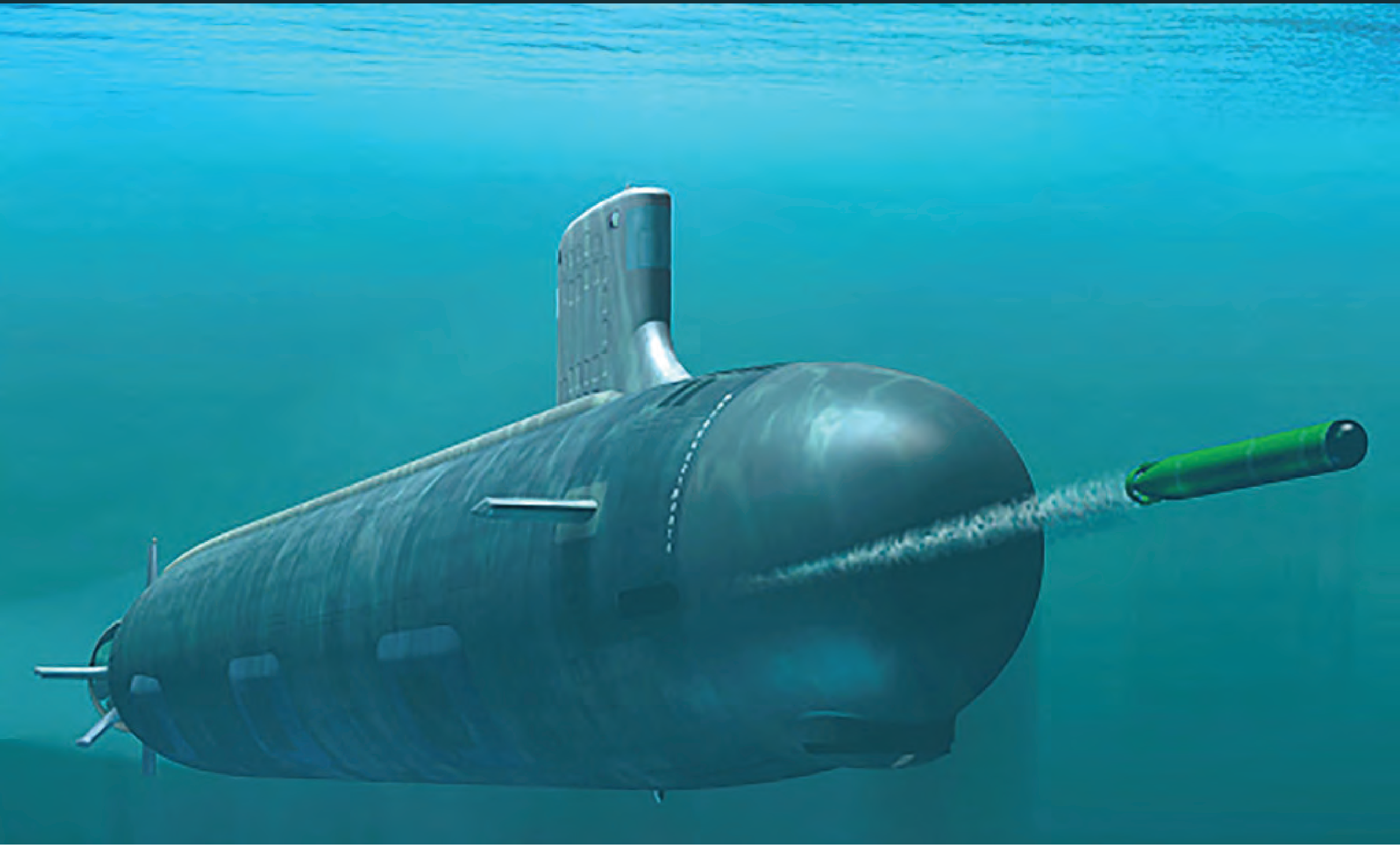
Analysis of the data from the LCS SUW MP cyber survivability assessments is in progress with a DOT&E report expected in 2QFY23. Insufficient data are available to assess the cyber survivability for the LCS MCM MP.

RECOMMENDATIONS

The Navy should:

1. Complete operational testing of the LCS MCM MP and MCM USV with Minehunt payload.
2. If insufficient data are available to characterize the performance of ALMDS and AMNS, plan additional test to obtain these data, as data are required to adequately test the LCS MCM MP capability.
3. Submit an update to the LCS MP TEMP for DOT&E approval as soon as feasible and that reflects the current MCM MP test strategy.
4. Submit the MCM USV with Minehunt payload TEMP for DOT&E approval as soon as feasible.

Mk 48 Torpedo Modifications



With DOT&E concurrence, the Navy concluded Mk 48 Mod 7 torpedo Advanced Processor Build (APB) 5 IOT&E in September 2021. DOT&E submitted a classified IOT&E report to Congress in April 2022, finding the Mk 48 Mod 7 APB 5 demonstrated operational effectiveness and suitability. However, some test scenarios were deferred until more representative threat surrogates are available and to reprioritize existing resources to accelerate testing of APB 5-Plus (5+). The cyber survivability of the APB 5 torpedo is classified and addressed in the April 2022 IOT&E report.

In January 2022, the Navy commenced in-water testing of APB 5+. The Navy expects to complete FOT&E of APB 5+ in 1QFY23.

SYSTEM DESCRIPTION

The Mk 48 is a submarine-launched heavyweight torpedo that directs itself towards a target submarine or surface ship based on an operator-developed targeting solution. The Mk 48 uses organic sensors to detect, classify, localize, and close its target.

The Navy intends the latest fielded improvement of the Mk 48 torpedo, APB 5, to improve the torpedo's ability to detect and classify threat submarines and surface ships. A follow-on improvement, APB 5+, transfers targeting functions from the submarine combat system to the torpedo itself, provides the torpedo with higher data exchange rates, and improves operator interface with the torpedo. The next major improvement, APB 6, will deliver capability improvement through software modifications on the Mk 48 Mod 7, and then incorporate Mk 48 Mod 8 hardware improvements that include an upgraded sonar array designed to expand the torpedo's acoustic frequency range and improve spatial resolution.

MISSION

The 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. The Navy's latest torpedo improvement program, the Mk 48 Mod 7 torpedo variant, is an Acquisition Category III program and a shared development effort with the Royal Australian Navy. APB 5 is primarily software development with minor hardware updates. DOT&E approved the APB 5 Test and Evaluation Master Plan in November 2017.

In September 2021, the Navy ended test for IOT&E of Mk 48 Mod 7 APB 5. DOT&E submitted a classified IOT&E report in April 2022.

In 2020, the Navy started developmental testing of APB 5+. In December 2021, the Navy determined APB 5+ was ready for operational test. In January 2022, DOT&E approved an APB 5+ update to the APB 5 Test and Evaluation Master Plan, with the test strategy and test resource plan for the evaluation of APB 5+ in FOT&E. The Navy expects to complete FOT&E in 1QFY23.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

Mk 48 Mod 7 APB 5 testing was adequate to assess operational effectiveness (in most but not all mission environments), suitability, and survivability. No test events occurred in FY22. In September 2021, DOT&E agreed with the Navy to defer some planned APB 5 testing to either APB 5+ or the future APB 6 program, due to unavailability of a representative threat surrogate or to enable test resources to support the timely delivery of the APB 5+ capability. As a result, APB 5 test data were insufficient to assess the torpedo's effectiveness against submarines evading with certain countermeasures and submarines operating in acoustically challenging environments. The Navy executed APB 5 test events in accordance with DOT&E-approved test plans; DOT&E observed some, but not all, test events due to space limitations on the firing platforms.

In November 2020 and March 2021, the Navy conducted APB 5+ modeling and simulation testing that included fleet operators on representative combat systems. Testing was adequate to characterize the APB 5+ operational interface improvements. The Navy further intends to use modeling and simulation testing at the Environment Centric Weapon Analysis Facility (ECWAF) to validate that APB 5+ modifications do not degrade its effectiveness in comparison to APB 5.

Between January 2022 and February 2022, the Navy completed one dedicated test event and collected data from one fleet training event to support operational test requirements for APB 5+. These included five anti-submarine warfare scenarios and 12 anti-surface warfare scenarios. The Navy executed APB 5+ test events in accordance with DOT&E-approved test plans; DOT&E observed some, but not all, test events due to space limitations on the firing platforms. The Navy expects to conduct the remaining seven anti-submarine warfare scenarios by the end of 1QFY23. APB 5+ will not be assessed for cyber survivability, as it has no modifications with the potential to impact cybersecurity.

Test adequacy of future APBs depends on representative threats and threat capability surrogates. The Navy is pursuing improved capabilities in this area.

The deferral of test events within some test environments in the APB 5 IOT&E reduces live data available to validate the ECWAF for use in future APB 6 IOT&E. Prior to APB 6 IOT&E, the Navy will need to collect data from fleet events conducted in these environments to validate and accredit the ECWAF for its full use. The full use of the ECWAF will reduce live tests in APB 6 by approximately half of those planned for APB 5 IOT&E.

PERFORMANCE

» EFFECTIVENESS

Although the program did not complete testing, DOT&E was able to determine that APB 5 is operationally effective and provides a significant improvement in the capability to destroy surface ships. APB 5 demonstrated similar or improved performance in anti-submarine warfare scenarios. Classified details are in the April 2022 IOT&E report.

Preliminary analysis suggests that APB 5+ is operationally effective. Test events to date have demonstrated that APB 5+ simplifies operator control of the torpedo, and modeling and simulation showed torpedo effectiveness of APB 5+ to be equivalent to that of APB 5. DOT&E expects to submit an FOT&E report in FY23 after the Navy completes testing.

» SUITABILITY

APB 5 is operationally suitable, demonstrating operationally sufficient reliability, availability, and maintainability.

Preliminary data suggest that APB 5+ is trending toward meeting its suitability requirements. DOT&E expects to submit an FOT&E report in FY23 after the Navy completes testing.

» SURVIVABILITY

The APB 5 cyber survivability assessment is classified. Details are in the April 2022 IOT&E report. APB 5+ will not receive a separate cyber survivability assessment, because its modifications do not affect cybersecurity.

RECOMMENDATIONS

The Navy should:

1. Address all recommendations in the April 2022 IOT&E report.
2. Obtain performance data from test environments deferred in APB 5 IOT&E to support validation of the ECWAF and its use in APB 6 IOT&E.
3. Complete development and validation of surface ship models and reverberation models in the ECWAF and validate their use in APB 6 IOT&E.
4. Fund continued improvements in representative threats and threat capability surrogates.

Mk 48 onload on USS Hampton *(SSN 767), October 2021*

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

In December 2021, the Navy fielded the Mk 54 Mod 1 Increment 1 torpedo prior to the completion of IOT&E. DOT&E submitted a classified Early Fielding Report in June 2022 that details demonstrated capabilities of the Mod 1 Increment 1. Data were insufficient to assess operational effectiveness and suitability, including performance in an acoustically challenging environment, a primary focus of improvement for this variant of the Mk 54 torpedo. The Navy has not yet scheduled remaining test events for IOT&E.

In January 2022, the Navy tested Operational Flight Program (OFP) software update 3.5 for the High Altitude Anti-Submarine Warfare (ASW) Weapon Capability (HAAWC). HAAWC with OFP 3.5 remains operationally effective, expands employment to lower altitudes than demonstrated during IOT&E, but remains not operationally suitable. DOT&E submitted a classified FOT&E report in July 2022 that details observed performance.

SYSTEM DESCRIPTION

The Mk 54 lightweight torpedo is the primary anti-submarine weapon employed from U.S. surface ships, aircraft, and helicopters. Mod 1 Increment 1 includes a new sonar array and torpedo software to provide a clearer picture of the intended target within the undersea environment. Mod 1 Increment 1 incorporates Advanced Processor Build 5 software from the Mk 48 heavyweight torpedo program. The Navy has not approved Mod 1 Increment 1 for Vertical Launch Anti-Submarine applications.

HAAWC is a combined Mk 54 torpedo and Air Launch Accessory wing kit. P-8A operators can employ HAAWC from much higher altitudes than conventional released Mk 54s. The Air Launch Accessory glides the Mk 54 down to an acceptable deployment altitude and then releases it to enter the water at a location assigned by the aircraft's combat system. The Navy updated HAAWC with OFP 3.5 to address deficiencies identified during the program's IOT&E.

MISSION

Commanders employ naval surface ships, aircraft, and helicopters equipped with the Mk 54 torpedo to defeat threat submarines. Operators place the Mk 54 in the vicinity of a threat submarine through either aircraft/helicopter release or firing the Vertical Launch Anti-Submarine missile. The Mk 54 autonomously seeks and attacks the threat submarine upon water entry. Surface ships may expeditiously deploy the Mk 54 torpedo from a surface vessel torpedo tube, in the general direction of the submarine, when identifying a submarine that is too close to offensively target.

Commanders employ HAAWC to conduct ASW from P-8As by enabling torpedo release across a larger range of P-8A altitudes.

PROGRAM

The Mk 54 is an Acquisition Category III program first fielded in 2004. The Navy has introduced incremental improvement with follow-on torpedo variants. The Navy intends to deliver the Mk 54 Mod 1 torpedo variant in two increments. The Navy commenced IOT&E of Mod 1 Increment 1 in December 2019 and released it for fleet employment in December 2021, prior to completion of IOT&E. The Navy intends to commence operational test of Mod 1 Increment 2 in FY26 and a Mod 2 variant in FY27. DOT&E approved the Mod 1 Milestone C Test and Evaluation Master Plan in February 2020. The Navy intends to submit the Mod 2 Milestone B Test and Evaluation Master Plan for DOT&E approval in 1QFY23.

The HAAWC is an Acquisition Category III program. The Navy conducted operational test of the software update, OFP 3.5, in January 2022 and the program entered full-rate production in August 2022.

» MAJOR CONTRACTORS

- Raytheon Integrated Defense Systems – Portsmouth, Rhode Island
- Progeny Systems Corp. – Manassas, Virginia
- Boeing Co. – St. Louis, Missouri

TEST ADEQUACY

Between November 2021 and January 2022, the Navy conducted 11 Mod 1 Increment 1 torpedo firings as part of IOT&E. During execution of the DOT&E-approved test plan, the fleet moved the location of the test due to an operational concern. This test event was not observed by DOT&E due to COVID travel restrictions. Post-test analysis of the test event revealed that six of the firings did not include environmental conditions required by the operational test design. As a result, six torpedo firings did not contribute test data required within the operational test design to determine Mod 1 Increment 1 operational effectiveness. The inclusion of the five valid torpedo firings in FY22 for the operational test design brings the achieved firings to 34 of the 86 planned torpedo firings. The Navy has yet to schedule remaining torpedo firings for Mod 1 Increment 1.

In June 2022, DOT&E submitted a classified Early Fielding Report that provides an interim assessment of the Mod 1 Increment 1 capability. Test data were insufficient to assess operational effectiveness and suitability, particularly in an acoustically challenging environment for which improvements are expected to have the greatest effect on torpedo performance. Test data were sufficient to assess cyber survivability.

In January 2022, the Navy employed eight HAAWC (two with exercise Mk 54 torpedoes and six with ballistic air test vehicles) from a P-8A at the Pacific Missile Range Facility Barking Sands in accordance with a DOT&E-approved test plan. DOT&E did not observe this test event due to COVID travel restrictions. Testing was adequate to assess effectiveness and suitability of the OFP 3.5 software update. The Navy did not test cyber survivability of HAAWC with OFP 3.5 due the software introducing no changes in the HAAWC interfaces or cyber-protective elements.

PERFORMANCE

» EFFECTIVENESS

The Mod 1 Increment 1 torpedo shows no degradation in torpedo effectiveness from its previous variant, the Mk 54 Mod 0 Block Upgrade, but analysis is limited to employment in deep water environments. Details are in the June 2022 report. Preliminary analysis of shallow water performance indicates that the torpedo is trending toward meeting its requirement in some scenarios, but no data are available to assess performance in acoustically challenging environments.

The HAAWC remains operationally effective with the OFP 3.5 upgrade. OFP 3.5 introduced improved flight models that effectively expanded the operational release envelope to include lower HAAWC release altitudes from the P-8A than demonstrated in IOT&E. Details are in the July 2022 report. P-8A aircraft require certification to improve HAAWC deployment flexibility.

» SUITABILITY

Preliminary data suggest the Mod 1 torpedo is trending towards meeting its suitability requirements, but insufficient data are available to assess operational suitability of Mod 1 Increment 1.

The HAAWC with OFP 3.5 did not demonstrate an improvement in reliability from IOT&E and remains not operationally suitable.

» SURVIVABILITY

Mod 1 torpedo vulnerability to a cyber-contested environment is classified; details from this evaluation are in the June 2022 report.

HAAWC with OFP 3.5 retains the same cyber survivability identified in the June 2021 classified HAAWC FOT&E report.

RECOMMENDATIONS

The Navy should:

1. Address all recommendations in the June 2022 report for Mod 1 Increment 1 and August 2022 report for HAAWC.
2. Complete Mod 1 Increment 1 IOT&E as soon as feasible, with priority placed on torpedo firings in an acoustically challenging shallow water environment.
3. Monitor HAAWC with OFP 3.5 reliability during fleet exercises.
4. Conduct P-8A certifications to maximize loadout flexibility for HAAWC and conventionally released Mk 54s.

MQ-4C Triton

In FY23, the Navy intends to conduct an IOT&E of the first increment of the restructured MQ-4C Triton program. This testing will inform an initial operational capability (IOC) deployment decision as part of the Navy's plan to retire the EP-3E. The Navy deferred some planned integrated testing to maintain the developmental test schedule, leaving mission critical capabilities unexercised and unevaluated. Any deferred integrated testing will need to be completed during IOT&E, adding to the schedule and risk of discovering significant deficiencies in IOT&E.

SYSTEM DESCRIPTION

The MQ-4C Triton is a high-altitude, long-endurance intelligence, surveillance, and reconnaissance unmanned aircraft intended to support global naval operations by collecting, processing, and distributing target track data, signals intelligence (SIGINT), and imagery intelligence data to fleet tactical operation centers and intelligence exploitation sites.

MISSION

Commanders will employ the MQ-4C to provide persistent maritime surveillance to detect, classify, identify, track, and assess maritime and littoral targets in support of surface warfare, intelligence operations, strike warfare, maritime interdiction, amphibious warfare, homeland defense, and search and rescue missions.

PROGRAM

The MQ-4C Triton is an Acquisition Category IC program and a critical component of the Navy's Maritime Intelligence, Surveillance, Reconnaissance, and Targeting transition plan to retire the EP-3E Aries II aircraft in accordance with the requirements in Section 112 of the FY11 National Defense Authorization Act.

The MQ-4C Triton program is following an incremental development approach after restructuring in 2021. The first increment is designed to deliver SIGINT capability sufficient to support the MQ-4C's portion of the transition plan. The Navy intends to conduct an IOT&E of this first increment and field it as an IOC in FY23. The follow-on increment(s) will deliver the remaining capabilities required by the updated Capability Development Document. Updates to the Acquisition Program Baseline, Acquisition Strategy, and Test and Evaluation Master Plan are ongoing.

» MAJOR CONTRACTOR

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

TEST ADEQUACY

Developmental delays are causing the program to defer test points from the integrated test plan to maintain the IOC date, leaving mission capabilities unexercised or unevaluated before the start of IOT&E. Deferring evaluation of these capabilities until IOT&E adds additional risk to IOC and the timely completion of IOT&E. Test periods at open-air ranges are crucial to characterize the SIGINT capabilities of the system and are particularly sensitive to schedule changes or delays. Due to the compressed schedule, any further delays in developmental or integrated testing will compound this risk.

The program completed a test period in the anechoic chamber at the Air Combat Environment Test and Evaluation Facility in May 2022. The test period was reinstated after being canceled in FY21, as noted in last year's Annual Report. During this chamber period, the program did not accomplish the planned degraded or denied GPS testing. The Navy will be unable to conduct related flight testing during IOT&E until this testing is completed during the next scheduled chamber period in August 2023.

The Navy does not have a method to extract data from the Minotaur mission management software for analysis. Operators use Minotaur to control MQ-4C sensors, view sensor data, and build the common operating picture. The only mitigation available for the test team is to manually record data from operator screens during test events or from a mission replay system after test events. This limitation will prolong data collection and analysis and may limit the depth of analysis for developmental test, integrated test, and in IOT&E. This limitation also affects all other Navy programs that use or intend to use Minotaur.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Not enough data are currently available to provide a preliminary assessment of the MQ-4C operational effectiveness, suitability, and survivability.

RECOMMENDATIONS

The Navy should:

1. Develop a method to extract mission data from the Minotaur system.
2. Complete the integrated test program and correct major deficiencies prior to proceeding into IOT&E.

MQ-4C arrives in Mayport, Florida
December 2021

MQ-8 Fire Scout

The Navy resumed evaluation of the MQ-8C Surface Warfare (SUW) Increment in November 2021, following a fleet-wide operational pause of all MQ-8 operations. In May 2022, the Navy commenced operational testing of MQ-8C SUW Increment as employed from a Littoral Combat Ship (LCS); however, the Navy truncated the test event after seven days due to system availability and high sea state. The Navy intends to complete operational test in FY23.

SYSTEM DESCRIPTION

The MQ-8C is a helicopter-based tactical unmanned aerial system designed to support intelligence, surveillance, and reconnaissance; SUW; and mine countermeasures (MCM) payloads. The air vehicle (AV) is a modified Bell 407 airframe intended to support LCS missions.

The MQ-8C SUW Increment consists of a Leonardo AN/ZPY-8 radar and associated Weapons Replaceable Assemblies, Minotaur software, and supporting AV and Mission Control Systems software. The AN/ZPY-8 radar capabilities include long- and short-range maritime search and detection, Inverse Synthetic Aperture Radar imagery, and Synthetic Aperture Radar imagery.

MISSION

Commanders employ LCS equipped with the MQ-8C SUW Increment to improve open ocean search and maritime target detection capability. From the LCS perspective, the SUW Increment provides an over-the-horizon detection capability by providing contact and track information for battlespace awareness. The system will also support the cuing of targets for employment of the Naval Strike Missile.

PROGRAM

The MQ-8 Fire Scout is an Acquisition Category IC program that entered Milestone C in 2017. The MQ-8C has three expected increments of capability: the Endurance Baseline Increment, SUW Increment, and MCM Increment. The Navy accepted 38 Endurance Baseline Increment MQ-8Cs and has no additional procurement planned. DOT&E approved the Test and Evaluation Master Plan in February 2022.

The President's Budget 2023 included a significant divestment within the MQ-8 program that will remove from fleet inventory all MQ-8B AVs by the end of FY22 and reduce the MQ-8Cs from 38 to 10 AVs by the end of FY23. The Navy intends to use eight of the remaining AVs for fleet employment and two of the AVs for training and test events, respectively.

» MAJOR CONTRACTOR

- Northrop Grumman – San Diego, California

TEST ADEQUACY

In May and June 2022, the Navy conducted initial testing of the MQ-8C SUW Increment with employment from the USS Montgomery (LCS 8). However, the Navy truncated the event to seven days due to system availability and high sea state. Testing to date has been conducted in accordance with the DOT&E-approved test plan and observed by DOT&E. Additional test of the MQ-8C SUW Increment from an LCS is required to assess the MQ-8C's integration into the LCS combat systems and its ability to support the LCS SUW mission. The Navy intends to complete operational test of the MQ-8C SUW Increment in 2QFY23.

PERFORMANCE

» EFFECTIVENESS

Not enough data are available to provide an assessment of the operational effectiveness of the MQ-8C SUW Increment as employed from LCS.

» SUITABILITY

Not enough data are available to provide an assessment of the operational suitability of the MQ-8C SUW Increment as employed from LCS.

» SURVIVABILITY

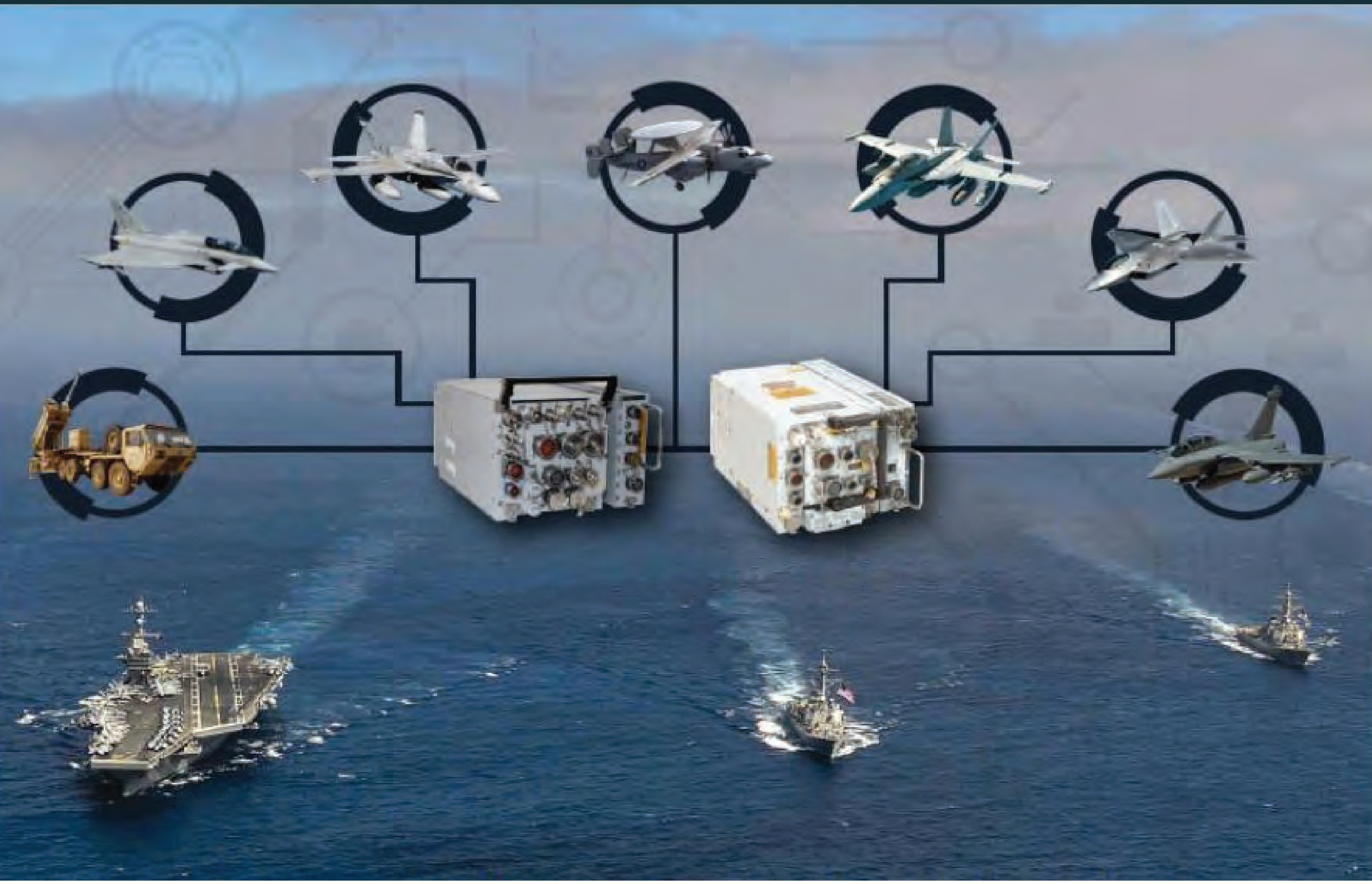
Not enough data are available to provide an assessment of the survivability of the MQ-8C SUW Increment in a cyber-contested environment. The Navy is leveraging developmental test and evaluation results to prepare the MQ-8C for a cooperative vulnerability and penetration assessment and an adversarial assessment that will occur after the last software release planned for FY23.

RECOMMENDATION

The Navy should:

1. Complete remaining operational test of the SUW Increment as soon as feasible.

Multi-Functional Information Distribution System (MIDS)



Component-level cyber testing by the Navy's Operational Test and Evaluation Force and Naval Air Systems Command occurred in September 2022. Operational testing for the Block Upgrade 3 is planned for FY23.

SYSTEM DESCRIPTION

The Multi-Functional Information Distribution System (MIDS) Joint Tactical Radio System (JTRS) core terminal set provides Link 16 digital datalink, Link 16 digital voice communications, and Tactical Air Navigation (TACAN) capabilities.

The MIDS JTRS terminals with Concurrent Multi Net-4 (CMN-4) reception have improved digital receivers, improved message buffering, and faster processing to enable host aircraft to simultaneously receive additional Link 16 messages during periods of assured high message exchange rates to meet mission requirements.

The MIDS JTRS terminals with Tactical Targeting Network Technology (TTNT) provide the host aircraft with higher throughput and lower information latency communications, supported by applications that enable faster updates of precise target locations and identification data, while using an expanded radio frequency range. The Internet Protocol design also supports faster routing of messages and balancing of message traffic among the participating nodes.

The system under test includes the MIDS JTRS TTNT terminal set and the host platform components such as controls, displays, antennas, and external power amplifiers that support delivery of the MIDS JTRS communications, navigation, and identification capabilities.

The MIDS Program Office is managing the design of a tailored MIDS JTRS CMN-4 system for integration into the Air Force's F-22 fighter aircraft. This design will also provide TACAN, legacy Link 16, CMN-4, and Identification Friend or Foe/Selective Identification Feature transponder capabilities.

MISSION

U.S. military commanders and allied nations use MIDS terminal variants on aircraft, ships, and ground units to communicate with their forces by secure and jam-resistant Link 16 voice and datalinks, along with Internet-Protocol-based TTNT communications through the entire range of military operations.

MIDS JTRS-equipped units rapidly exchange information, including air and surface tracks, identification, platform fuel/weapons, cooperative integrated fire control, mission status, engagement orders, targeting data, and engagement results.

MIDS TACAN supports aircraft navigation, aircraft-to-aircraft station keeping, aircraft carrier recovery marshalling, and airfield approaches.

MIDS JTRS Identification Friend or Foe/Selective Identification Feature supports commercial airspace transit and safety, as well as secure, jam-resistant combat identification.

PROGRAM

The MIDS JTRS is an Acquisition Category IC program. DOT&E approved the MIDS JTRS TTNT Operational Assessment Plan (0357-07-OT-D4-1) on June 17, 2019. The Navy plans to continue platform integration testing of MIDS JTRS TTNT on E-2D and EA-18G in FY23. Development of an updated Test and Evaluation Master Plan for future increments of MIDS JTRS TTNT is expected in FY23.

» MAJOR CONTRACTORS

- Viasat, Inc. – Carlsbad, California
- Data Link Solutions – Wayne, New Jersey and Cedar Rapids, Iowa
- The Boeing Company – St. Louis, Missouri
- Northrop Grumman – Melbourne, Florida
- The MITRE Corporation – San Diego, California and McLean, Virginia

TEST ADEQUACY

MIDS JTRS TTNT component-level cyber testing, conducted in accordance with the DOT&E-approved Operational Assessment Plan (0357-07-OT-D4-1), occurred in September 2022. This event was observed by DOT&E. The adequacy of that testing will be evaluated after the test data are received by DOT&E.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E will evaluate any impacts to effectiveness, suitability, and cyber survivability from the results of the component-level cybersecurity testing scheduled for 4QFY22.

RECOMMENDATIONS

The Navy should:

1. Ensure adequate component-level cybersecurity testing is completed before the beginning of platform-level MIDS JTRS TTNT cybersecurity testing.
2. Coordinate with DOT&E on an updated Test and Evaluation Master Plan for the next increment of MIDS JTRS.

Next Generation Jammer Mid-Band (NGJ-MB)

The Next Generation Jammer Mid-Band (NGJ-MB) is currently undergoing integrated testing and is scheduled to begin dedicated operational testing during IOT&E in May 2023. The program is focusing on resolving deficiencies that were identified prior to Milestone C while demonstrating the system has matured enough to conduct operationally relevant test flights. The lack of verified, validated and accredited (VV&A) digital models required to supplement NGJ-MB operational flight test data will reduce the confidence of the effectiveness evaluation during IOT&E.

SYSTEM DESCRIPTION

The NGJ-MB is an airborne electronic attack system. It consists of two pods, mounted under each EA-18G aircraft wing, which integrate with the AN/ALQ-218 electronic warfare system and function as a radio frequency (RF) receiver and jammer. Each pod contains two active electronically scanned arrays that radiate over a wide frequency band and an internal ram-air turbine that generates electrical power. The NGJ-MB is the first of three programs comprising the planned Next Generation Jammer upgrade that is intended to replace the legacy AN/ALQ-99 Tactical Jammer System family of pods currently fielded on the EA-18G. The NGJ-MB is designed to engage multiple advanced threats at greater standoff ranges than the AN/ALQ-99 Tactical Jammer System.

MISSION

Combatant Commanders will employ the NGJ-MB equipped EA-18Gs as an embedded component of carrier air wings and expeditionary forces to provide EA capabilities against a wide variety of RF targets. The NGJ is designed to improve EA-18G capability against modern, advanced RF threats, communications, datalinks, and non-traditional RF targets.

The NGJ-MB has four electronic attack mission profiles: standoff, modified escort, penetrating escort, and stand-in jamming. Navy aircrew will primarily fly the standoff and modified escort profiles. The Navy will use the NGJ to deny, degrade, or deceive the enemy's use of the electromagnetic spectrum, employing both reactive and preemptive jamming techniques while enhancing the friendly force's use of the electromagnetic spectrum.

PROGRAM

The NGJ-MB is an Acquisition Category IC program. In May 2021, the Secretary of the Navy approved the NGJ-MB program to move past Milestone C, thereby authorizing procurement of low-rate initial production (LRIP) pods. Redesigned production-representative System Demonstration Test Article (SDTA) pods are currently undergoing integrated testing and are scheduled to begin operational test in May 2023. NGJ will replace the ALQ-99 Tactical Jammer System pods which were developed and fielded in 1971.

Per the DOT&E approved TEMP, NGJ-MB was originally slated to integrate as part of Software Configuration Set (SCS) H16 block upgrade. SCS block upgrades, labeled in numeric order, are a separate but parallel flight test for the EA-18 Growler program, and the current operational software is SCS H14. Delays in the NGJ program have deferred SCS integration to the H18 block upgrade.

The lack of validated or accredited digital models needed to supplement NGJ-MB operational flight testing will reduce the data available to evaluate effectiveness during NGJ-MB IOT&E. In addition, test data classification has prevented all required modeling and simulation (M&S) personnel from analyzing available data. To address this risk, the Navy implemented a series of flights in an operationally representative environment to ensure sufficient modeling data will be available to supplement operational test flights and generate data necessary for verification, validation, and accreditation of M&S. The simulated operational environment includes large-force exercises in a threat-representative environment. These flights also serve as risk-reduction for planned EA-18G H18 SCS test flights with NGJ-MB. The EA-18G H18 SCS requires significant maturation to support NGJ-MB operational test. The Navy still needs to address problems with data classification and personnel access to support M&S validation.

» MAJOR CONTRACTORS

- Raytheon Space and Airborne Systems – El Segundo, California
- The Boeing Company, Integrated Defense Systems – St. Louis, Missouri
- Northrop Grumman Mission Systems – Linthicum, Maryland

TEST ADEQUACY

The Navy did not conduct dedicated operational tests on the NGJ-MB system during FY22. However, the Navy is conducting a combination of laboratory, anechoic chamber, and integrated flight testing to address concerns identified at Milestone C and to mature the system to conduct operationally relevant test flights to support IOT&E.

PERFORMANCE

» EFFECTIVENESS

The Navy conducted integrated testing with Capabilities-Based Test and Evaluation events during 4QFY22. Raytheon and the Navy made progress using NGJ-MB software updates to improve system performance in several areas to address deficiencies present at Milestone C. However, the program still does not meet all Milestone C requirements and the NGJ-MB SDTA pods have not proven mature enough to conduct operational test flights. As a result, the operational test flights originally planned for the Capabilities-Based Test and Evaluation period will now be conducted during IOT&E.

» SUITABILITY

The Navy continues to develop corrective actions to mitigate reliability failures, but no additional data have been provided by the Navy to update pod reliability since Milestone C. These deficiencies in reliability and performance resulted in a decision to delay the NGJ-MB Operational Test Readiness Review until April 2023, further delaying the decision to enter the operational test phase.

» SURVIVABILITY

Cyber testing was conducted in October 2021, March 2022, and July 2022 to collect data and identify vulnerabilities in a cyber-contested environment. Results of developmental cyber testing will be reported prior to January 2023. The program is working with Raytheon to resolve identified vulnerabilities.

RECOMMENDATIONS

The Navy should:

1. Prepare to extend IOT&E past the currently scheduled end date of 4QFY23 given the uncertainty around the availability and reliability of operational test-ready LRIP pods and the maturity of SCS H18.
2. Continue to develop digital models and assesses operationally representative flights to ensure necessary data are available for verification, validation and accreditation of digital models for evaluation.
3. Obtain required security clearances for M&S personnel so they can access test facilities and data needed to support accreditation of M&S in order to evaluate operational effectiveness.

Offensive Anti-Surface Warfare (OASuW) Increment 1

The Offensive Anti-Surface Warfare (OASuW) Increment 1 program continues the development of missile hardware and software to increase targeting capabilities as an incremental upgrade to the currently fielded air-to-ground missile (AGM)-158C Long Range Anti-Ship Missile (LRASM). In October 2021, the program began flight test bed events with the goal of testing improved hardware and software resident in LRASM 1.1. Integrated captive carry events were conducted in July 2022 to provide risk reduction data prior to missile free-flight integrated test events (ITEs) completed on August 15 and September 23, 2022. The goal of ITE was to capture telemetry data to be used for modeling and simulation (M&S) verification, validation and accreditation (VV&A) for future IOT&E of LRASM 1.1 and support the FY22 Quick Reaction Assessment (QRA) report and planned declaration of early operational capability (EOC) in 1QFY23.

SYSTEM DESCRIPTION

The OASuW Increment 1 program 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. OASuW Increment 1 began as an accelerated acquisition program to procure a limited number of air-launched missiles leveraging the near-term Defense Advanced Research Projects Agency's LRASM initiative. LRASM is a long-range, conventional, air-to-surface, precision standoff weapon that can be launched from the Navy's F/A-18E/F and the Air Force's B-1B aircraft. LRASM, designated as the AGM-158C, is derived from the Joint Air-to-Surface Standoff Missile – Extended Range (JASSM-ER). Once launched, LRASM guides to an initial point using a GPS guidance system and employs onboard sensors to locate, identify, and provide terminal guidance to the target.

To date, there are three LRASM variants which comprise the OASuW Increment 1 program, designated LRASM 1.0, LRASM 1.1, and LRASM C-3. In FY21, the Navy introduced LRASM C-3, a version adding land strike capabilities while removing components to reduce unit cost. The Navy is working on the details required to plan and execute test events in order to meet the LRASM C-3 EOC planned for 4QFY24. LRASM 1.0 is currently fielded to the fleet while LRASM 1.1 entered ITEs in FY22.

OASuW Increment 2, the follow-on program to OASuW Increment 1, will deliver long-term anti-surface warfare capabilities to counter future threats. The DOD continues to plan for OASuW Increment 2 to be developed via full and open competition, and initial operational capability is anticipated in FY28-30. Due to congressional budget reductions for OASuW Increment 2, the Navy funded LRASM 1.1 to bridge the gap until an OASuW Increment 2 program of record is established. This upgrade incorporates missile hardware and software improvements to address component obsolescence and increase targeting capabilities. LRASM 1.1 is currently in the integrated test phase.

MISSION

Combatant Commanders will use units equipped with LRASM to destroy adversary ships from standoff ranges.

PROGRAM

DOT&E approved the LRASM 1.1 Master Test Strategy in January 2020. Developmental flight testing of LRASM 1.1 components on a Sabreliner flight test bed started in March 2021 and completed in January 2022. The Navy conducted a captive carry flight test in July 2022 as risk-mitigation for free-flight evaluation missiles (FFEM) prior to entering the free-flight integrated test phase.

Integrated testing occurred in August and September 2022 at Point Mugu Sea Range with three inert warhead shots at unmanned mobile maritime targets employed from F/A-18E/F aircraft. The Navy will use telemetry and impact data collected from ITEs to validate M&S and support accreditation for use in operational testing. Operational testing is composed of FFEM shots, including one with a live warhead in 2024, M&S-based test events, and cyber operational test events.

The Navy planned to complete verification and validation of the LRASM M&S suite by the end of FY22 before LRASM 1.1 EOC; however, M&S accreditation was not possible during FY22 due to insufficient open-air test flight data. As ITEs began in August 2022, validation and verification data will become available, but not until 1QFY23. Therefore, the decision was made to remove M&S from the QRA. DOT&E will write an operational test report in 2025 after operational flight, cyber, and M&S tests are complete.

The Navy plans to conduct an integrated test shot for LRASM C-3 in 1QFY24 and reach EOC in 4QFY24. The C-3 will compete for limited M&S resources already reserved for LRASM 1.1 operational testing.

» MAJOR CONTRACTOR

- Lockheed Martin Missiles and Fire Control – Orlando, Florida

TEST ADEQUACY

The LRASM 1.1 Master Test Strategy (MTS) was approved on January 30, 2020. The Navy is proceeding in accordance with the MTS, but LRASM 1.1 dedicated operational test activity did not occur in 2022. However, integrated test phase-1 began in August 2022, which can be used as operational test data. Data collected during integrated test phase-1 will produce open-air test data required to support the Operational Test and Evaluation Force's QRA required for the Navy to make a LRASM 1.1 EOC decision.

LRASM 1.0 integrated testing in FY17-19 was in accordance with the DOT&E-approved test plan but had limited operational realism. The Navy plans to increase operational realism in LRASM 1.1 IOT&E through replication of an operationally representative environment during M&S events. LRASM 1.1 will also undergo cyber operational testing using a signal processor-in-the-loop lab environment. The Navy is developing the LRASM 1.1 operational test plan.

No LRASM C-3 operational test activity occurred in 2022. The Navy needs to complete development of the LRASM C-3 concept of operations and system requirements, and work with DOT&E to plan and execute an adequate operational test to support full-rate production and EOC in 4QFY24. LRASM C-3 will require M&S resources to develop and test the new land strike capability. M&S resources are already limited for LRASM testing, so the Navy needs to ensure adequate resources remain for LRASM 1.1 when including C-3 test needs.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Operational effectiveness, suitability, and survivability assessments will be addressed in the FY25 IOT&E report, once testing and analysis are complete.

RECOMMENDATIONS

The Navy should:

1. Plan and execute operational testing before full-rate production of LRASM Increment 1 weapons.
2. Complete development and validation of the M&S environment to facilitate the operational effectiveness evaluation of LRASM 1.1.
3. Ensure adequate M&S resources remain for LRASM 1.1 operational testing when adding LRASM C-3 operational requirements.

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

In May 2022, the Navy conducted an evaluation of the cyber survivability of the Over-The-Horizon Weapons System (OTH-WS). The Navy delayed completion of IOT&E flight-testing in FY22 due to test asset reallocation in support of U.S. Marine Corps anti-ship missile testing.

SYSTEM DESCRIPTION

The OTH-WS is a long-range, surface-to-surface missile employed by the Navy on either the Littoral Combat Ship or the future guided-missile frigate. The Navy intends OTH-WS to defeat maritime targets both inside and beyond the firing unit's radar horizon. The OTH-WS is a stand-alone system requiring minimal integration with the host platform. It consists of an operator interface console, naval strike missile, 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 naval strike missiles from the Joint Light Tactical Vehicle-based mobile launch platform as a component of a Navy/Marine Expeditionary Ship Interdiction System (NMESIS).

PROGRAM

OTH-WS is an Acquisition Category II, Non-Developmental Item program. In FY18, the Navy awarded a firm-fixed-price contract to Raytheon Missile and Defense to integrate the OTH-WS onto Navy platforms. The Navy commenced operational test in March 2021 in accordance with DOT&E-approved test plans, and DOT&E observed the test. The Navy expects to deliver the Test and Evaluation Master Plan (TEMP) for OTH-WS to DOT&E for approval in 1QFY23. The Navy intended to make a Full-Rate Production decision in FY22; however, the Navy now expects this decision in FY25 due to test asset reallocation to support the Marine Corps NMESIS project.

» MAJOR CONTRACTOR

- Raytheon Missile and Defense – Tucson, Arizona

TEST ADEQUACY

The Navy commenced operational test of the OTH-WS in FY21, but delayed FY22 test events due to reallocation of test resources to support the Marine Corps NMESIS project. In May 2022, the Marine Corps conducted integration testing of the naval strike missile from a JLTV-based mobile launch platform. The Navy and DOT&E are evaluating the ability to use suitability data from this event to support the assessment of the OTH-WS. The Navy expects to conduct remaining IOT&E OTH-WS flight tests in FY24.

In May 2022, the Navy completed cyber survivability testing, specifically an adversarial assessment (AA) and cooperative vulnerability and penetration assessment (CVPA), of OTH-WS on a Littoral Combat Ship. Testing was adequate to assess the resilience of the OTH-WS to cyberattack.

In FY22, the Navy completed the first of seven requisite arena tests to characterize the OTH-WS warhead lethality against representative targets. The Navy expects to complete live fire testing to assess system lethality and survivability within a contested environment in FY24.

PERFORMANCE

» EFFECTIVENESS

Insufficient data are available to determine operational effectiveness of the OTH-WS. The three live firings in FY21 demonstrated that the OTH-WS has potential to provide the Navy with an over-the-horizon capability to defeat surface vessels; however, the Navy has not characterized this capability due to test remaining in progress. DOT&E will report OTH-WS operational effectiveness, including lethality, after the completion of remaining operational and lethality test events.

» SUITABILITY

Insufficient data are available to determine operational suitability of the OTH-WS due to the test remaining in progress. DOT&E will report OTH-WS operational suitability after the completion of remaining operational and lethality test events.

» SURVIVABILITY

Assessment from the Navy's cyber survivability evaluation in May 2022 is classified. DOT&E will report on the cyber survivability of the OTH-WS at the completion of IOT&E.

RECOMMENDATIONS

The Navy should:

1. Provide the OTH-WS TEMP for DOT&E approval.
2. Complete the remaining operational and lethality test events to support an adequate determination of operational effectiveness and suitability of the OTH-WS and inform Navy fielding decisions.

Ship Self-Defense System (SSDS) Mk 2 Integrated Combat Systems

In July 2022, the Navy conducted an operational test of the Ship Self-Defense System (SSDS) Mk 2 Baseline 10 of the Mod 6 variant for USS *Gerald R. Ford* (CVN 78), assessing SSDS's tracking capability against fast inshore attack craft and unmanned aerial vehicles (UAVs). In FY22, the Navy conducted no testing of the SSDS Mk 2 Mod 6 self-defense capability against anti-ship cruise missiles (ASCMs), and no operational test on SSDS Mk 2 Mod 1 through Mod 5.

SYSTEM DESCRIPTION

SSDS is the command and control system aboard amphibious ships and aircraft carriers. It comprises a local area network with processors that host tactical programs, and interfaces to external systems. SSDS integrates the following systems: horizon search radars (i.e., SPQ-9B and SPY-3), volume search radars (i.e., SPS-48, SPS-49, and SPY-4), close-in weapon system, MK 9 tracker illuminator system, SLQ-32 electronic warfare system, cooperative engagement capability, Evolved Sea Sparrow Missiles, and Rolling Airframe Missiles. SSDS includes operator workstations that display real-time tactical information.

SSDS Mk 2 has six variants referred to as mods. Each mod represents the integration of a unique set of sensors and self-defense weapon systems for a specific ship class. Individual ships in a class may have different SSDS baselines, but will be the same mod.

- Mod 1 on *Nimitz*-class aircraft carriers (CVN 68-class)
- Mod 2 on *San Antonio*-class amphibious transport dock ships (LPD 17-class)
- Mod 3 on *Wasp*-class landing helicopter dock ships (LHD 1-class)
- Mod 4 on *America*-class landing helicopter assault ships (LHA 6-class)
- Mod 5 on *Whidbey Island*-class and *Harpers Ferry*-class landing dock ships (LSD 41/49-classes)
- Mod 6 on *Gerald R. Ford*-class aircraft carriers (CVN 78-class)

SSDS Mk 2 capability improvements derive from software baselines that are integrated within the mod. On commissioned ships, there are different SSDS baselines, up to Baseline 10. The Navy is developing Baseline 12 that integrates new sensors and weapons, and includes major changes to engagement doctrine and weapon scheduling algorithms that the Navy intends to improve ship survivability.

MISSION

Navy commanders depend on SSDS to effectively integrate their ship's sensors and weapon systems and enable timely engagement of the diverse spectrum of air threats to the ship. The integrated SSDS combat system provides the ship self-defense capability against ASCMs and threat aircraft. Further, SSDS contributes to the commander's tactical picture during air, surface, amphibious, and undersea warfare missions.

PROGRAM

SSDS Mk 1 achieved Milestone C in 1998. In 2005, the Navy transitioned to SSDS Mk 2 and was designated as an Acquisition Category IC program. In May 2018, DOT&E approved Revision C of the SSDS Mk 2 Test and Evaluation Master Plan (TEMP), which included operational test of SSDS Mk 2 Mod 4 with Baseline 9 on LHA 6-class, Mod 5 with Baseline 9 on LSD 41/49, and SSDS Mk 2 Mod 6 with Baseline 10 on CVN 78. The Navy plans to conduct FOT&E of each SSDS Mk 2 Mod and baseline combination.

The Navy completed operational test on SSDS Mk 2 Mod 4 in 2017 during the IOT&E of USS *America* (LHA 6). The Navy has been in test on SSDS Mk 2 Mod 5 since 2016 and SSDS Mk 2 Mod 6 since 2019.

The Navy is developing an Air Warfare (AW) Ship Self-Defense Enterprise TEMP that includes follow-on testing of SSDS Mk 2. Testing will assess performance of updates to SSDS Mk 2 Mods to address significant changes to the ship class systems and will include SSDS Mk 2 Mod 4 with Baseline 12 on USS *Bougainville* (LHA 8), SSDS Mk 2 Mod 2 with Baseline 12 on USS *Harrisburg* (LPD 30), and SSDS Mk 2 Mod 6 with Baseline 12 on USS *John F. Kennedy* (CVN 79). Testing will also address the back-fit of Baseline 12 on existing ships.

» MAJOR CONTRACTOR

- Lockheed Martin, Rotary and Mission Systems – Moorestown, New Jersey

TEST ADEQUACY

In July 2022, the Navy continued evaluation of SSDS Mk 2 Mod 6 with test events on USS *Gerald R. Ford* (CVN 78), that evaluated performance to track surface targets and UAVs. DOT&E observed the tests and they were conducted with some deviation from the DOT&E-approved test plan due to surface target failures.

In FY22, the Navy conducted no additional testing of the SSDS Mk 2 Mod 6 self-defense capability against ASCMs. DOT&E submitted a classified report in April 2022 that detailed system performance from completed test events, specifically three live operational firing test events against the Self Defense Test Ship (SDTS) configured with a representation of SSDS Mk 2 Mod 6. The Navy has funded and plans to conduct OT firing and tracking ASCM events on USS *Gerald R. Ford* (CVN 78) in FY24.

There may not be enough data available to determine the operational effectiveness and suitability of the SSDS Mk 2 Mod 6 self-defense capability against ASCMs at the completion of IOT&E. The Navy will not complete the remaining planned firing events against the SDTS configured with a representation of SSDS Mk 2 Mod 6 due to there being no AN/SPY-3 radar set available to install on the SDTS. Additionally, the Navy planned to use data from live operational firing events from the USS *Zumwalt* (DDG 1000) IOT&E, but modifications to the DDG 1000 AN/SPY-3 radar no longer support the use of the DDG 1000 test data for validation of the Probability of Raid Annihilation (PRA) test bed. The PRA test bed is the high fidelity model and simulation the Navy intends to provide the remainder of the SSDS Mk 2 Mod 6 performance data.

The Navy has yet to schedule the planned cooperative vulnerability and penetration assessment and adversarial assessment to determine survivability of SSDS Mk 2 Mod 6 against cyber threats.

In FY22, the Navy conducted no tests on SSDS Mk 2 Mod 1 (*Nimitz*-class) or Mk 2 Mod 5 (*Whidbey Island*-class and *Harpers Ferry*-class), as a result of funding shortfalls, prioritization of remaining funding to conduct CVN 78 operational test on the SDTS, and Strike Group availability. The Navy has yet to execute any of the SSDS Mk 2 Mod 1 testing or eight of the nine test events for SSDS Mk 2 Mod 5 that are planned in Revision C of the May 2018 DOT&E-approved TEMP.

SSDS Mk 2 Mod 1 test data are insufficient to determine operational effectiveness with respect to force level interoperability, command and control, and weapons control functionality, when integrated into a Strike Group environment. The Navy intends to capture interoperability, command and control and weapons control functionality operational test requirements for SSDS Mk 2 Mod 1 in Enterprise TEMP 1910 for SSDS Baseline 12.

SSDS Mk 2 Mod 5 test data are inadequate to determine effectiveness and suitability. The Navy has deployed these ships since 2016.

PERFORMANCE

» EFFECTIVENESS

SSDS Mods 1 and 3 with Baseline 10 exhibit deficiencies related to the integration of an upgraded Mk 9 tracker illuminator system. The Navy deploys these ships with mitigations applied against these deficiencies, but the mitigations are not validated with operational testing.

No data were collected in FY22 that would change previously provided assessment of effectiveness for SSDS Mk 2 Mod 4 and SSDS Mk 2 Mod 5.

Insufficient data are available to determine operational effectiveness of SSDS Mk 2 Mod 6. Classified observations of self-defense capability against ASCM surrogates using the SDTS are provided in the USS *Gerald R. Ford* (CVN 78) – AW Self-Defense Interim Assessment report submitted in April 2022. No preliminary assessment of the SSDS Mk 2 Mod 6 tracking capability of small boats and UAVs from the July 2022 event is available; analysis is in progress.

» SUITABILITY AND SURVIVABILITY

No data were collected in FY22 that would change previously provided assessment of suitability and survivability for SSDS Mk 2 Mod 1 through SSDS Mk 2 Mod 5.

Insufficient data are available to determine the operational suitability of SSDS Mk 2 Mod 6.

RECOMMENDATIONS

The Navy should:

1. Fund and execute all planned testing of the SSDS Mk 2 Mod 6 capability to provide CVN 78 with self-defense against ASCMs.
2. Develop, validate, and accredit the PRA M&S test bed to support its intended use during operational assessment of SSDS Mk 2 Mod 6 in FY24.
3. Address all recommendations in the April 2022 classified report for CVN 78 on ship self-defense against ASCMs.
4. Validate with operational testing the correction of SSDS Mk 2 Mod 1 and 3 with Baseline 10 integration issues with upgraded Mk 9 tracker illuminator system.
5. Submit the AW Ship Self-Defense Enterprise TEMP for DOT&E approval in FY23.
6. Complete SSDS Mk 2 Mod 5 testing to characterize ship self-defense performance of LSD 41/49 ship classes.

Ship to Shore Connector (SSC)

In FY22, the Navy conducted phases of IOT&E and LFT&E to support assessments of Ship to Shore Connector (SSC) vulnerability to cyber-attack, sea worthiness, and susceptibility to threat mines. The Navy scheduled the phase of IOT&E intended to assess operational effectiveness and suitability of the SSC to commence in December 2022.

SYSTEM DESCRIPTION

The SSC is a fully amphibious air cushion vehicle similar to the Landing Craft, Air Cushion (LCAC). Compared to the LCAC, the SSC is intended to have increased payload, range, availability, and the ability to operate in a greater range of environmental conditions.

MISSION

Navy Commanders will use the SSC to provide ship-to-shore transport of forces conducting Ship-To-Objective Maneuver. The SSC system is expected to bridge the gap of brigade-sized maneuver and operations capability after the retirement of the LCAC at the end of its service life.

PROGRAM

The SSC is an Acquisition Category IC Major Defense Acquisition Program. The Navy approved Milestone C in July 2015. The Navy took delivery of the first test and training craft in February 2020. The SSC program Test and Evaluation Master Plan (TEMP) was approved in November 2021.

» MAJOR CONTRACTOR

- Textron Systems – New Orleans, Louisiana

TEST ADEQUACY

In July 2022, the Navy conducted a phase of IOT&E to evaluate the cyber survivability of the SSC. The testing, consisting of a cooperative vulnerability and penetration assessment and an adversarial assessment, was conducted in accordance with a DOT&E-approved test plan, and tests were observed by DOT&E.

The Navy completed three tests to assess SSC LFT&E survivability in FY22. All were conducted in accordance with DOT&E-approved test plans, and observed by DOT&E. Testing builds off of a series of previously conducted component and surrogate tests, including destructive testing of SSC-specific shafts and seats and full-hull weapon effects tests against decommissioned LCACs as SSC surrogates.

- In December 2021, the Navy conducted controlled damage tests using the second SSC hull at Naval Surface Warfare Center Panama City Detachment. Testing provided data on the ability of the craft to recover from representative threat-weapon damage.
- In April 2022, the Navy conducted seaworthiness testing of the SSC in the Gulf of Mexico. The Navy will use this data to validate the results from scale model testing; specifically, that the stresses in the hull while off cushion in extreme seas would not result in loss of the craft.
- In June 2022, then Navy conducted underwater signature evaluation in Norfolk, Virginia. Testing provided data to validate that the bare-hull signatures of the legacy LCAC are a suitable surrogate for the SSC. Testing included deviations in the planned number of runs and speeds, but was sufficient to identify the differences between the LCAC and SSC bare-hull signatures.

The Navy scheduled the phase of IOT&E intended to assess operational effectiveness and suitability of the SSC to commence in December 2022. The Navy expects to declare readiness for operational test in 1QFY23.

PERFORMANCE

» EFFECTIVENESS

No data are available to assess operational effectiveness of the SCC.

» SUITABILITY

No data are available to assess operational suitability of the SSC.

» SURVIVABILITY

The SSC cyber survivability assessment is classified. DOT&E expects to publish a final IOT&E report assessing operational effectiveness and suitability, and cyber survivability of the SSC in 3QFY23.

Remaining testing to assess survivability against threat weapons and mine susceptibility testing of the loaded craft are planned in FY23. However, DOT&E has yet to receive the full set of acoustic and magnetic data necessary to support test planning for this assessment of mine susceptibility.

The Navy is behind in the planned completion of verification, validation and accreditation (VV&A) of the supporting vulnerability assessment models. The Navy intends to complete VV&A in parallel with a final survivability assessment report in FY23.

SSC with USS Carter Hall *(LSD 50), February 2022*

RECOMMENDATIONS

The Navy should:

1. Provide DOT&E with the magnetic and acoustic data from the mine susceptibility tests as soon as feasible.
2. Complete VV&A of SSC vulnerability assessment models as soon as feasible to support the final survivability assessment report.

Standard Missile 2 (SM-2) Block IIIC

The Standard Missile 2 (SM-2) Block IIIC is a Middle Tier of Acquisition (MTA) program intended to provide medium-range air defense to Aegis cruisers and destroyers. The Navy is conducting a limited operational test known as a Quick Reaction Assessment (QRA) to support an initial capability deployment. DOT&E will issue an Early Fielding Report (EFR) upon completion of the QRA.

SYSTEM DESCRIPTION

The SM-2 Block IIIC is a medium-range, surface-to-air missile with an active radio frequency seeker. It is a modification to existing SM-2 Block III and IIIA missiles. This modification includes replacing the semi-active seeker with one based on Standard Missile 6 active seeker technology. The missile features a new dorsal fin design and a thrust vectoring jet tab assembly to control trajectory as the missile egresses the launcher.

MISSION

The Joint Force commander will utilize the SM-2 Block IIIC from Aegis cruisers and destroyers to provide the medium-range component of naval battle force's area and self-defense capability against anti-ship missiles and tactical aircraft.

PROGRAM

The SM-2 Block IIIC is an MTA program that the Navy intends to transition to an Acquisition Category II program upon its completion of an operational demonstration QRA, and approval of its acquisition program baseline capabilities. The Navy intends to field an SM-2 Block IIIC interim capability to the fleet at the completion of QRA.

» MAJOR CONTRACTOR

- Raytheon Missiles & Defense – Tucson, Arizona

TEST ADEQUACY

In July 2022, the Navy flew three SM-2 Block IIIC missiles against four targets during the QRA flight test event on USS *Frank E. Petersen, Jr.* (DDG 121). All testing was conducted in accordance with the DOT&E approved test plan and observed by DOT&E. The Navy has yet to schedule the planned QRA cyber survivability and model and simulation events. Once all events are complete, the QRA will be adequate to demonstrate a limited SM-2 Block IIIC capability but not to determine operational effectiveness, suitability, and cyber survivability.

PERFORMANCE

» EFFECTIVENESS

Preliminary assessment of QRA testing is that the SM-2 Block IIIC is progressing towards a successful demonstration of capability against subsonic anti-ship cruise missile surrogates in a stream raid scenario.

The July 2022 test did identify an anomaly that the Navy intends to address through engineering changes and evaluate in developmental and operational test when SM-2 Block IIIC transitions to a program of record. A detailed assessment of the anomaly and corrective actions will be provided in a DOT&E EFR after completion of QRA.

» SUITABILITY

Insufficient data are available to determine operational suitability. Early estimates for suitability metrics, reliability and availability, will be reported in a DOT&E EFR upon completion of QRA.

» SURVIVABILITY

Insufficient data are available to determine cyber survivability. DOT&E will report cyber survivability after transition of SM-2 Block IIIC to a program of record and completion of IOT&E.

RECOMMENDATION

The Navy should:

1. Complete the QRA testing to inform the final decision to transition to the Acquisition Category II SM-2 Block IIICU program.

Standard Missile-6 (SM-6) Family of Missiles

In December 2021, DOT&E published an Early Fielding Report that details demonstrated performance of the Standard Missile-6 (SM-6) Block I/IA missiles with modifications provided from the Navy's future capability demonstration (FCD) mission set expansion. The Navy demonstrated additional capability in the anti-surface missions, but did not conduct operational test to determine operational effectiveness, suitability, or survivability in a contested environment. Additionally, the latest variant of the family of SM-6 missiles, the SM-6 Block IB, transitioned from a Middle Tier of Acquisition program to an Acquisition Category (ACAT) IC Major Capability Acquisition program in FY22.

SYSTEM DESCRIPTION

SM-6 is a shipborne missile that can defeat a range of targets from supersonic anti-ship cruise missiles to threat surface ships, among others. The SM-6 seeker and terminal guidance electronics derive from technology developed in the Advanced Medium-Range Air-to-Air Missile program. SM-6 receives midcourse flight control from the Aegis Weapon System (AWS) via the ship's radar. Terminal flight control is autonomous via the missile's active seeker or is supported by the AWS via the ship's illuminator.

SM-6 consists of three primary variants: Block I, Block IA, and Block IB. Block I and Block IA were developed as a fleet area air defense weapon intended to engage anti-ship cruise missile and manned aircraft threats. The Navy upgraded the Block I and Block IA missiles to provide additional anti-surface capability through the Navy's FCD mission set expansion effort. Block IB is a modification of the Block IA missile that the Navy intends to extend engagement range through development of a new second stage rocket motor.

MISSION

The Joint Force Commander/Strike Group Commander employs naval units equipped with the SM-6 to conduct defensive and offensive operations. Missions include: 1) fleet air defense against fixed-/rotary-winged aircraft and anti-ship missiles operating at altitudes ranging from very high to sea-skimming, 2) extended range, over-the-horizon anti-surface capability, 3) overland air-defense as a component of the Navy Integrated Fire Control – Counter Air From the Sea operational concept, and 4) provide Sea-Based Terminal capability against short- and medium-range ballistic missiles in their terminal phase of flight.

PROGRAM

SM-6 is an ACAT IC program. SM-6 Block I and Block IA are beyond Milestone C. The Navy transitioned Block IB from a Middle Tier of Acquisition Program to the SM-6 ACAT IC program in November 2021. The Navy expects to deliver the Block IB missile to the fleet in FY27. The Navy is also developing an upgrade to computing components of the SM-6 family of missiles to mitigate obsolescence issues.

The SM-6 Test and Evaluation Master Plan requires an update to document the test strategy and resources to evaluate the Block IB missile. The Navy expects to provide the Test and Evaluation Master Plan update for DOT&E approval in FY23.

» MAJOR CONTRACTOR

- Raytheon Missiles & Defense – Tucson, Arizona

TEST ADEQUACY

In FY21, the Navy completed a series of land-based and at-sea developmental tests and tactical demonstrations of the additional capabilities provided the SM-6 Block I/IA missiles through the FCD effort. Data were sufficient to demonstrate additional capability within a limited set of operational conditions. Demonstrations were not intended to support a determination of operational effectiveness, suitability, or survivability in a contested environment. The Navy did not conduct operational test and did not submit operational test plans for DOT&E approval; however, the Navy included DOT&E and the Navy's Operational Test Force during test planning and test observation.

Large/full size aerial targets and representative surface targets are required to adequately test operational effectiveness, suitability, and lethality of the SM-6 Block IB. Neither are currently available nor planned for acquisition.

PERFORMANCE

» EFFECTIVENESS

The SM-6 Block I/IA missiles with FCD modifications demonstrated additional capability in anti-surface missions. In December 2021, DOT&E published an Early Fielding Report that details this performance.

SM-6 Block I/IA effectiveness in the air defense mission is unchanged from previous DOT&E assessments. SM-6 Block IB effectiveness will be reported upon completion of operational test.

» SUITABILITY

Insufficient data are available to determine operational suitability of the SM-6 Block I/IA missiles with FCD modifications. SM-6 Block IB suitability will be reported upon completion of operational test.

» SURVIVABILITY

Insufficient data are available to determine cyber survivability. Insufficient data are available to determine survivability of SM-6 with FCD modifications in a contested and congested electromagnetic environment. SM-6 Block IB survivability will be reported upon completion of operational test.

RECOMMENDATIONS

The Navy should:

1. Develop and acquire sufficient quantities of large/full size aerial targets and representative surface targets to support operational test of the SM-6 Block IB missile.
2. Conduct operational and lethality testing of the SM-6 Block I/IA with FCD modifications.

Trident II (D-5) Sea-Launched Ballistic Missile – Life Extension Program Variant

The Navy completed IOT&E for the Trident-II (D-5) Life Extension Program (LEP) in June 2022, flying a total of 23 missiles. Preliminary assessments indicate that the Trident-II (D-5) life extension variant remains operationally effective and suitable. DOT&E will submit the IOT&E report in FY23.

SYSTEM DESCRIPTION

The Trident II (D-5) delivers nuclear warheads using a three-stage, solid propellant rocket and inertial guidance aided by a stellar sighting. The Navy plans for the Trident II (D-5) to be available through at least 2042, and developed the LEP modifications to provide missile component refresh, including an updated guidance system and flight control electronics.

MISSION

The submarine-launched Trident II (D-5) supports the sea-based leg of the U.S. nuclear triad. The Navy deploys the Trident II (D-5) from nuclear ballistic submarines, ensuring the weapon's survivability and availability. The Trident II (D-5) is a primary means of deterring nuclear attacks on the United States and its allies. In the event deterrence fails, the Trident II (D-5) is able to attack the entire range of enemy targets and help terminate the conflict on terms favorable to the United States.

PROGRAM

The Trident II (D-5) is an Acquisition Category IC program. The Navy initially deployed the D-5 life extension missiles in 2017 and expects to complete deployment in 2024. DOT&E approved a Trident II (D-5) LEP Test and Evaluation Plan and Strategy in 2015 as an update to the Test and Evaluation Master Plan.

» MAJOR CONTRACTORS

- Lockheed Martin Space – Titusville, Florida
- Charles Stark Draper Laboratory – Cambridge, Massachusetts

TEST ADEQUACY

In June 2022, the Navy completed the IOT&E flight test program for the LEP variant of the Trident II (D-5) missile. DOT&E observed these tests, and they were conducted per the DOT&E approved test plan. The Navy conducted 23 flights of the LEP variant between 2018 and 2022 in accordance with DOT&E-approved flight test support plans. Tests were adequate to determine operational effectiveness and suitability.

PERFORMANCE

» EFFECTIVENESS

Analysis of the final six flight tests is in progress. Completed analysis of the previous 17 flights and the preliminary assessment of the final 6 flights suggest that the LEP variant of the Trident II (D-5) missile remains operationally effective. DOT&E will provide a final determination of operational effectiveness in an IOT&E report in FY23.

» SUITABILITY

As previously identified, analysis of the final flight tests remains in progress, and the completed analysis of the previous 17 flights and preliminary assessment of the final 6 flights suggest that the LEP variant of the Trident II (D-5) missile remains operationally suitable. DOT&E will provide a final determination of operational suitability in the FY23 IOT&E report.

» SURVIVABILITY

DOT&E monitors the cyber survivability of Trident II (D-5) through annual reviews of the system's cyber postures and understanding current threats and the program's processes to proactively manage cyber improvements. DOT&E will detail the program's cyber survivability posture in the FY23 IOT&E report.

RECOMMENDATIONS

Once analysis is completed, DOT&E will provide recommendations in the FY23 IOT&E report.

Unmanned Influence Sweep System (UISS)

In July 2022, the Navy declared initial operational capability of the Unmanned Influence Sweep System (UISS) based on their assessment of operational effectiveness, suitability, and survivability. DOT&E submitted a classified IOT&E report in June 2022. UISS is not operationally suitable due to low reliability and availability. In August 2022, the Navy tested the integration of UISS within the Littoral Combat Ship (LCS) Mine Countermeasures (MCM) Mission Package (MP) during the LCS MCM MP IOT&E.

SYSTEM DESCRIPTION

UISS is an acoustic and influence mine clearance system designed to detonate moored and bottom mines. UISS consists of an Unmanned Surface Vehicle (USV) that powers and tows the Unmanned Surface Sweep System. The USV operates along pre-planned tracks and uses a radar and camera surveillance suite to provide the remote operator with situational awareness and the ability to avoid obstacles or other watercraft. The Unmanned

Surface Sweep System consists of a magnetic towed cable that is energized to create a magnetic field and a towed acoustic generator that emanates acoustic signatures to detonate mines. UISS is a baseline capability of the LCS MCM MP and is designed to be deployed from the LCS, but can also operate from ashore. The UISS USV is the same vehicle used to support the LCS MCM MP Minehunt capability with the AQS-20C towed multi-function sonar.

MISSION

UISS is the Navy's intended replacement for the aging *Avenger*-class MCMs. Upon decommissioning of the *Avenger*-class, UISS will be the Navy's only maritime minesweeping capability. Commanders will deploy UISS from the LCS to perform minesweeping operations against moored and bottom mines in sea lanes, straits, choke points, fleet operating areas, and amphibious objective areas.

PROGRAM

The UISS is an Acquisition Category III program. In July 2022, the Navy declared initial operational capability of the UISS. In August 2022, the Navy conducted testing of the UISS within the LCS MCM MP IOT&E to assess the interoperability of UISS and other baseline capabilities within the MP. The Navy expects to make a UISS Full-Rate Production decision in the first half of FY23.

» MAJOR CONTRACTOR

- Textron Systems Corporation – Hunt Valley, Maryland

TEST ADEQUACY

In October 2021, the Navy completed classified survivability testing of the UISS. All testing was conducted in accordance with a DOT&E-approved test plan, and observed by DOT&E. Data were sufficient to assess specific attributes of UISS survivability to near mine explosion, but the Navy has not tested magnetic sweep cable survivability.

The Navy did not complete all planned test events during the FY21 IOT&E of UISS. However, testing remained adequate to assess UISS effectiveness, suitability, and survivability.

In August 2022, the Navy conducted an operational test event of the LCS MCM MP that included the integration of UISS. Analysis of this event is in progress and will be reported within an LCS MCM MP IOT&E report in FY23.

PERFORMANCE

» EFFECTIVENESS

UISS demonstrated its designed capability against a limited set of the surrogates used to represent threat mines in representative scenarios. UISS performance metrics against moored and bottom mines are classified. DOT&E submitted a classified IOT&E report in June 2022.

» SUITABILITY

UISS is not operationally suitable. UISS reliability and availability do not support sustained mine sweeping operations. Operational availability demonstrated when employing UISS from an LCS was 0.29, well below the Navy-defined minimum threshold.

» SURVIVABILITY

UISS survivability is classified and detailed in the June 2022 report.

RECOMMENDATIONS

The Navy should:

1. Improve the reliability and availability of UISS as employed from LCS and meet fleet operational requirements.
2. Complete underwater explosion testing on the magnetic sweep cable.
3. Address all recommendations in the June 2022 report.
4. Conduct testing of UISS capability of exploited mine threats that were not evaluated in UISS IOT&E.

USSOCOM Dry Combat Submersible (DCS) Now

The Navy's Operational Test and Evaluation Force (OPTEVFOR) completed an evaluation of the cyber survivability of the Dry Combat Submersible Now (DCS Now) in FY22. However, U.S. Special Operations Command (USSOCOM) delayed the at-sea portion of operational test until FY23 due to COVID-19, weather, and materiel issues on DCS Now Boat #1. DOT&E will report on DCS Now operational effectiveness and suitability in FY23 upon completion of IOT&E.

SYSTEM DESCRIPTION

The DCS Now is a 39.4-foot long, submersible vessel with lock-in/lock-out capability for up to eight Special Operations Forces (SOF) occupants. The DCS Now is battery-powered and operated by two pilots. The DCS Now maintains a one-atmosphere dry environment within the personnel compartments.

MISSION

USSOCOM is developing DCS Now for covert insertion and recovery of SOF from denied areas. By reducing operator exposure to the underwater environment, the dry environment of DCS Now improves mission endurance and range over existing small submersibles. The DCS Now further enhances SOF mission capability with additional payload capacity.

PROGRAM

DCS Now is an Acquisition Category III program managed by USSOCOM. In 2018, the program achieved Milestone C and DOT&E approved a Test and Evaluation Master Plan update. Initial Operational Capability, originally planned for FY19, is now projected in FY23 following the completion of IOT&E. In 2021, DOT&E approved IOT&E test plans for at-sea testing and shore-based cyber survivability testing.

» MAJOR CONTRACTOR

- Lockheed Martin Rotary Mission Systems – Riviera Beach, Florida

TEST ADEQUACY

In December 2021, DOT&E approved a test plan for OPTEVFOR to conduct at-sea evaluation of DCS Now for IOT&E. However, developmental test continued through the remainder of FY22 due to delays from COVID-19, non-supportive weather, and materiel issues on DCS Now Boat #1. OPTEVFOR expects to commence operational test in 1QFY23.

In February 2022, OPTEVFOR completed cyber survivability tests consisting of a cooperative vulnerability and penetration assessment and an adversarial assessment of DCS Now. DOT&E observed these tests, and they were conducted in accordance with the DOT&E-approved test plan.

PERFORMANCE

» EFFECTIVENESS

Operational test of the DCS Now is delayed until FY23 and data are not available to provide a preliminary assessment of operational effectiveness. DOT&E will report operational effectiveness of DCS Now upon completion of IOT&E in FY23.

» SUITABILITY

Operational test of the DCS Now delayed until FY23 and data are not available to provide a preliminary assessment of operational suitability. DOT&E will report operational suitability of DCS Now upon completion of IOT&E in FY23.

» SURVIVABILITY

Analysis of the cyber survivability test remains in progress and assessment is classified. DOT&E will report the cyber survivability of DCS Now upon completion of IOT&E in FY23.

RECOMMENDATION

USSOCOM should:

1. Work with OPTEVFOR to complete operational testing as soon as practical.

VH-92A® Patriot™ Presidential Helicopter

The United States Marine Corps declared initial operational capability in December 2021 based upon the service's assessment of the VH-92A's operational effectiveness, suitability, and survivability demonstrated in IOT&E. Since the FY21 IOT&E, the program has made system improvements based on DOT&E recommendations from IOT&E and feedback from the White House Military Office (WHMO). Marine Helicopter Squadron One (HMX-1) conducted an FOT&E period from July 12 to September 16, 2022 under the auspices of the Navy's Operational Test and Evaluation Force (OPTEVFOR). VH-92A® is a registered trademark of the Department of the Navy.

SYSTEM DESCRIPTION

The VH-92A is a four-bladed, dual-piloted, twin-engine helicopter based on the Sikorsky S-92 medium lift helicopter, equipped with a Mission Communication System (MCS) to enable simultaneous short- and long range, secure and non-secure, voice and data communications. HMX-1 will use the VH-92A aircraft to conduct administrative lift and contingency operations intended to provide safe and timely, pre-planned or unscheduled, transport of the President of the United States and other parties as directed by the WHMO. The VH-92A is air transportable to remote locations via a single Air Force C-17 cargo aircraft. The VH-92A will replace the legacy fleet of VH-3D and VH-60N aircraft.

MISSION

HMX-1 will use the VH-92A aircraft to provide safe and timely transport of the President of the United States and other parties as directed by the WHMO. The MCS provides the passengers with reliable voice and data communications to carry out senior leader duties.

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 that does not include a Full-Rate Production decision. DOT&E approved: (1) the VH-92A Test and Evaluation Master Plan in 2015, (2) the IOT&E plan in 2020 in support of the United States Marine Corps declaration of initial operational capability and the WHMO's VH-92A Commissioning Program, and (3) the FOT&E plan in 2022 in support of verification of correction of deficiencies. The Department of the Navy procured 23 VH-92A aircraft.

» MAJOR CONTRACTOR

- Sikorsky Aircraft Corporation, a Lockheed Martin Company – Stratford, Connecticut

TEST ADEQUACY

Integrated, operational, and cybersecurity testing were conducted in accordance with DOT&E-approved test plans, observed by DOT&E, and were adequate to evaluate effectiveness, suitability, and cyber survivability of the VH-92A as operated by HMX-1.

HMX-1 conducted FOT&E using operational aircraft from July 12 to September 16, 2022 under the auspices of OPTEVFOR. The majority of operations took place in the National Capitol Region using facilities and landing zones routinely employed by HMX-1. Representatives from the WHMO and other operational units participated to the maximum extent possible. Additional data was gathered during familiarization and training events and initial operational commissioning plan events led by WHMO. In accordance with agreements made between OPTEVFOR and DOT&E, data gathered during the events were scored and included in FOT&E results when appropriate.

To address cybersecurity findings discovered during IOT&E, the Navy conducted cybersecurity testing as part of FOT&E. Results are included in the classified annex of the FOT&E report that will be published in FY23.

PERFORMANCE

» EFFECTIVENESS

The White House intends to place the VH-92A into service supporting the Presidential Lift mission in 2022 based on operational effectiveness demonstrated in FOT&E and the White House Commissioning Program. DOT&E's assessment of the VH-92A's effectiveness is described in detail in the FOT&E report that will be published in FY23.

» SUITABILITY

The White House intends to place the VH-92A into service supporting the Presidential Lift mission in 2022 based on operational suitability demonstrated in FOT&E and the White House Commissioning Program. DOT&E's assessment of the VH-92A's operational suitability is described in detail in the FOT&E report that will be published in FY23.

» SURVIVABILITY

The White House intends to place the VH-92A into service supporting the Presidential Lift mission in 2022 based on survivability demonstrated in FOT&E and the White House Commissioning Program. DOT&E's assessment of the VH-92A's survivability is described in detail in the FOT&E report that will be published in FY23.

RECOMMENDATION

The Navy should:

1. Address recommendations found in DOT&E's FOT&E report and classified annex that will be published in FY23.

DEPARTMENT OF THE AIR FORCE PROGRAMS

Advanced Pilot Training (APT)

The Advanced Pilot Training (APT) program is re-baselining its schedule with IOT&E to support a Full-Rate Production decision anticipated in FY26. The top critical issues for the Air Force to address are the T-7A emergency escape system (including the bird strike capability of the canopy), the lack of an Automatic Ground Collision Avoidance System (AGCAS), the On-Board Oxygen Generation System (OBOGS), and cyber survivability.

SYSTEM DESCRIPTION

The APT Family of Systems (FoS) includes the T-7A Red Hawk aircraft and associated ground based training systems (GBTS) to replace the aging fleet of 429 T-38C aircraft and associated ground training systems. The T-7A is a two seat trainer powered by a single afterburning-turbofan engine, with digital avionics and fly-by-wire flight controls. GBTS devices include the aircrew ground-egress trainer, part-task trainer, weapons-system trainer, ejection-seat trainer, and operational-flight trainer. The weapons-system trainer and operational-flight trainer are two types of simulators that incorporate a dynamic-motion seat and g-suit inflation to provide a physical sensation of high g force flight maneuvers.

MISSION

Air Education and Training Command (AETC) instructor pilots will use the APT FoS to train student pilots to be prepared to fly 4th- and 5th-generation fighter and bomber aircraft after graduating from pilot training. 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 on September 27, 2018. The contract is a fixed price incentive firm contract for Engineering and Manufacturing Development, and a fixed price incentive firm target with a transition to a firm fixed price contract for production. AETC plans to procure 351 T-7A aircraft, 46 simulators, and other associated GBTS for deployment to the five pilot training bases: Joint Base San Antonio-Randolph, Texas; Columbus AFB, Mississippi; Laughlin AFB, Texas; Vance AFB, Oklahoma; and Sheppard AFB, Texas.

DOT&E approved the Milestone B Test and Evaluation Master Plan in January 2018. The program is re-baselining the schedule and expects the Milestone C to occur in FY24. IOT&E will support the Full-Rate Production decision anticipated in FY26.

» MAJOR CONTRACTORS

- The Boeing Company, Defense, Space & Security – St. Louis, Missouri
- SAAB AB – Linköping, Sweden and Lafayette, Indiana

TEST ADEQUACY

Phase one of testing, currently underway, consists of flying qualities and envelope expansion using the Boeing-owned T1 and T2 aircraft with the Federal Aviation Administration experimental certification. Testing is conducted at the contractor's facilities in St. Louis, Missouri. Air Force test personnel established distributed test operations (DTO) to permit real-time observation at Edwards AFB, California.

Since May 2019, the Air Force Operational Test and Evaluation Center (AFOTEC) Detachment 5 test team maximized early involvement by incorporating operational perspective into the contractor-led developmental testing of the two Boeing prototype aircraft, along with design reviews and simulator test events. On February 7, 2022, AFOTEC published a fourth APT Periodic Report to inform stakeholders of their assessment of developmental test planning, APT FoS design considerations, and IOT&E readiness. APT Periodic Report-4 added 6 new unclassified recommendations to the 22 open recommendations from previous reports. A classified annex, published on April 20, 2022, added three classified recommendations.

DOT&E concurs with the AFOTEC assessments and recommendations. AFOTEC's early involvement enables them to provide an operational perspective, assessments, and continuous feedback on program development, which have the potential to reduce costs by identifying and resolving issues at the earliest opportunity rather than waiting until the end of the IOT&E.

PERFORMANCE

» EFFECTIVENESS

Early tests demonstrated the T-7A can sustain high-g maneuvering capability, which is necessary to teach student pilots the fundamental concepts required for transition to 5th-generation aircraft. Fighter aircraft employ AGCAS to prevent loss of life during high-g maneuvers when sustained high g-forces can cause the pilot to lose consciousness. Although the formal requirements for APT did not include a requirement for AGCAS, AETC has requested funding in FY24 to plan and implement AGCAS.

To support the Milestone C decision in FY24, DOT&E will assess the progress of operational effectiveness of the APT FoS to enable AETC instructor pilots to train student pilots.

» SUITABILITY

The designs of the emergency escape system and canopy bird strike capability of the Engineering and Manufacturing Development aircraft have failed to meet minimum safety requirements during subsystem qualification tests. Both systems require design changes prior to low-rate initial production and IOT&E to ensure the safety of instructor and student pilots. The Air Force should work with Boeing to correct these design issues.

Initial qualification testing of the OBOGS system consisted of unmanned altitude chamber tests. The OBOGS system met MIL-STD-3050 and the latest draft of MIL-STD-3050A requirements related to mask pressure and oxygen concentration. Results from this unmanned testing support entry into the next phase of qualification tests that includes human altitude chamber and centrifuge testing. The T-7A program needs technically adequate OBOGS flight test data as well, to include operationally representative flight profiles. These data should be consistent with the FY22 NDAA Section 224 mandate to assess and correct deficiencies in pilot breathing systems, even though the T-7A is not a fielded fighter aircraft and not included in the FY22 Section 224 mandate.

» SURVIVABILITY

The APT cybersecurity integrated test team used the Mission-based Risk Assessment Process for Cyber Report, signed August 2021, to focus resources on the most critical areas of concern for the cyber threat to confidentiality, integrity, and availability. AFOTEC highlighted three areas of concern in their classified annex to Periodic Report-4 based on the current system design and potential cyber threats. The next step is to develop the Milestone C Test and Evaluation Master Plan and IOT&E plans using details from the Mission-based Risk Assessment Process for Cyber Report.

DOT&E will assess cyber survivability of the APT FoS to support the Milestone C and Full-Rate Production decisions.

RECOMMENDATIONS

The Air Force should:

1. Address the AFOTEC Periodic Report recommendations and make necessary design changes prior to the start of IOT&E; the program should not wait until the end of the firm fixed price production contract.
2. Resolve the emergency escape system design issues (including the bird strike capability of the canopy) with Boeing to prevent further program delays and resolve safety concerns.
3. Support AETC's request to add an AGCAS capability to the T-7A before production begins to reduce safety risks and loss of life.
4. Procure OBOGS flight-test instrumentation to collect breathing pressures, air delivery response timing and flow, and g-forces during operationally representative flight profiles.
5. Incorporate on-aircraft cybersecurity assessments during integrated testing and IOT&E.

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

Despite being under DOT&E oversight for over four years, the AGM-183A Air-Launched Rapid Response Weapon (ARRW) Program Office does not have a DOT&E-approved Integrated Master Test Plan nor has the Office submitted an Operational Demonstration Plan, but is proceeding to test the ARRW. The ARRW program has not yet demonstrated the required warfighting capability. The program conducted two successful flight tests demonstrating proper function of the solid rocket motor, shroud separation, and simulated glider separation. Hardware and software problems have delayed planned operational demonstration flights.

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

Units utilize ARRW to provide an offensive, high-speed strike capability to destroy fixed, high-value, time-sensitive, land-based targets in anti-access/area-denial environments. Launched from a B-52H aircraft, ARRW provides standoff capability to prosecute targets in a timely fashion.

PROGRAM

ARRW is a Section 804 Rapid Prototyping Middle Tier of Acquisition program leveraging lessons learned from the Defense Advanced Research Projects Agency's Tactical Boost Glide vehicle program. The ARRW program is currently developing an Integrated Master Test Plan and an Operational Demonstration Plan for DOT&E approval. Having concluded a series of booster rocket flight tests in FY21 and FY22, the program plans to proceed into all-up round (AUR) testing with live warheads in FY23. All ARRW AUR tests will involve land impacts. The Air Force currently is producing a limited number ARRWs, with four intended for AUR T&E. The Air Force will utilize the AUR test results to inform their production decision.

The program flight test schedule could be delayed due to the limited number and availability of hypersonic flight corridors, target areas, and test support assets. The program will be competing for these limited resources with other hypersonic programs, including those being developed by the Navy, Army, and Missile Defense Agency.

» MAJOR CONTRACTOR

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

TEST ADEQUACY

The draft ARRW Integrated Master Test Plan consists mostly of developmental ground and flight testing, and some live-fire lethality testing. The Air Force plans to execute an operational demonstration to assess the operational capabilities and limitations of the system, yet DOT&E has yet to see a completed Operational Demonstration Plan. The limited number of planned test assets and test targets will not allow an assessment of operational effectiveness (including lethality), suitability, and survivability with high confidence.

In May and July 2022, the program completed the second and third of three planned booster test flights with simulated gliders. DOT&E observed the May test. The booster test flights demonstrated final weapon-aircraft integration with the production-representative missile, the capability to launch the weapon inside the flight envelope, and proper performance of the booster rocket. The program also completed the last of six warhead characterization arena tests in early FY22. Four AUR tests are scheduled, beginning in FY23.

The Air Force plans to use engagement-level and mission-level modeling and simulation (M&S) to assess ARRW survivability against surface-to-air missile systems and anti-aircraft-artillery batteries.

PERFORMANCE

» EFFECTIVENESS

Hardware and software problems have delayed planned ARRW operational demonstration flights, precluding an initial assessment of risks to demonstrating the ARRW's intended operational effectiveness requirements. The ARRW program executed two successful booster test flights in FY22.

During the first attempted booster test flight of FY22 (the second booster test flight for the program), the Air Force aborted the launch before release. A low voltage caused a built-in-test fault upon application of power, causing the weapon to prevent launch. The Air Force implemented software fixes to correct the issue and the second attempt of this booster test flight was successful. This test flight demonstrated safe separation and deconfliction of the ARRW away from the B-52H bomber, achieved successful ignition of the solid rocket motor, and attained operational hypersonic speeds, culminating in a successful booster-glider separation event.

The second booster test flight of FY22 (third booster test flight for the program) was successful. The Air Force demonstrated the safe separation and deconfliction of the ARRW away from the B-52H bomber at a tactical deconfliction distance. It was launched in a different region of the launch envelope than the previous booster test flight. The second booster test flight also demonstrated maneuver of the ARRW toward a target.

Lethality testing is ongoing, precluding an initial assessment of ARRW warhead performance. Given the limited number of planned test events, there is risk to demonstrating the ARRW lethal effects against the required tactical and strategic targets.

» SUITABILITY

The limited number of planned flight hours and test assets (booster and AUR) will preclude an adequate assessment of all operational suitability metrics for the ARRW system during this phase of testing.

» SURVIVABILITY

The engagement-level or mission-level simulations have not yet been completed to assess ARRW survivability in a contested environment. Pending the verification, validation, and accreditation of the M&S tools, the final survivability assessment should estimate the probability that a single ARRW will complete its mission, given the capabilities of various early warning radars, surface-to-air missile systems, and anti-aircraft-artillery batteries to detect and engage ARRW in various one-on-one scenarios. The final survivability assessment should also estimate such probabilities in the presence of multiple threat systems connected by threat-representative integrated air-defense systems capable of detecting, tracking, and engaging multiple airborne targets, including hypersonic weapons like the ARRW. Finally, ARRW only has an Authority to Operate; an assessment of ARRW's survivability within a cyber-contested environment is not currently scheduled, but should be completed before acquisition production decision.

RECOMMENDATIONS

The Air Force should:

1. Deliver an adjudicated Integrated Master Test Plan and Operational Demonstration Plan for DOT&E approval.
2. Verify, validate, and accredit all M&S tools intended for use to enable an adequate assessment of ARRW performance.
3. Conduct an adequate survivability assessment of ARRW in a cyber-contested environment.

AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM)

The Advanced Medium-Range Air-to-Air Missile (AMRAAM) Air Intercept Missile (AIM)-120D System Improvement Program (SIP)-3 completed operational testing in FY22. DOT&E assessed the system as effective, suitable, and survivable, with one issue and several recommendations identified in the DOT&E classified test report, dated November 2022. In June 2022, the Air Force and Navy commenced integrated testing of the new AIM-120D3 missile configuration with SIP-3F software and expect completion in FY23.

SYSTEM DESCRIPTION

The AMRAAM is a radar-guided, air-to-air missile with capability in both the beyond-visual-range and within-visual-range arenas. F-35A/B/C, F-22A, EA-18G, F/A-18C/D/E/F, F-16C/D, and F-15C/D/E aircraft can all employ AMRAAM, including multiple-target engagements with multiple missiles simultaneously. The AIM-120D is the newest variant in the AMRAAM family of missiles and includes both hardware and software improvements over the AIM-120C3-C7. Multiple planned follow-on SIPs will provide updates to the AIM-120D to enhance missile performance and resolve previous deficiencies. The AIM-120D3 missile configuration incorporates a form-fit-function hardware refresh to replace obsolete components and re-hosts the SIP-3 operational flight software as SIP-3F.

MISSION

The Air Force, Navy, and several foreign military forces employ various versions of the AIM-120 AMRAAM to conduct air-to-air combat missions. All U.S. fighter aircraft use the AMRAAM as the primary beyond-visual-range air-to-air weapon.

PROGRAM

The AMRAAM SIP-3 upgrade is a project under the Acquisition Category IC AMRAAM program. DOT&E approved the SIP-3 revision of the Test and Evaluation Master Plan in 2019. The Air Force and Navy completed SIP-3 operational testing in FY22; the Air Force fielded the software in January 2022, and the Navy fielded the software in March 2022. SIP-3F integrated testing began in June 2022 and expects completion in FY23.

» MAJOR CONTRACTOR

- Raytheon Missiles and Defense – Tucson, Arizona

TEST ADEQUACY

In FY22, the Air Force completed SIP-3 integrated and operational testing in accordance with the DOT&E-approved test plan, and DOT&E personnel observed the testing. Based on the test results, DOT&E made several recommendations for future test environments and scenarios to enhance test adequacy. DOT&E approved the SIP-3F test plan in June 2022; integrated testing is ongoing, with two of five planned missile flight tests complete thus far.

The Air Force completed a cooperative vulnerability and penetration assessment and an adversarial cyber survivability assessment in FY22.

PERFORMANCE

» EFFECTIVENESS

SIP-3 software is effective, with one platform integration issue identified. Details are available in the November 2022 classified DOT&E test report.

» SUITABILITY

SIP-3 software is suitable, with significantly better overall reliability than specification. Details are available in the November 2022 classified DOT&E test report.

» SURVIVABILITY

SIP-3 is survivable, with one issue and several recommendations for improvement and future testing. Details are available in the November 2022 classified DOT&E test report.

RECOMMENDATIONS

DOT&E recommends that the Air Force and Navy, in coordination with DOD, develop a full-scale target with 5th-generation signatures to enable adequate operational testing of planned future capabilities. While the hardware improvements in the AIM-120D3 missile configuration are meant only to replace obsolete components, the extent of the refresh will likely yield improved capabilities against modern threats. A full-scale target with fifth-generation signatures would provide a holistic surrogate for modern, operationally representative threats with adequate power and cooling for associated, modern on-board defensive systems. Sub-scale targets have significant limitations representing modern threat aircraft.

Air Operations Center – Weapon System (AOC-WS)

The Air Force continues to develop and deploy Air Operations Center – Weapon System (AOC-WS) software. Two capability modernization upgrades were delivered in FY22 to sustain the fielded AOC-WS 10.1 increment. The AOC-WS 10.1 Agile Release Event (ARE) 21.10 is operationally effective, and ARE 22-02 is currently in operational test. The Air Force is also developing and deploying AOC-WS Block 20 software, although a required test strategy has not yet been approved. Also, the Block 20 software released to date lacks sufficient capabilities to support major combat scenarios and the sustainment, maintenance, and training processes would not adequately support a meaningful operational evaluation. The Service submitted a Block 20 test strategy, but critical comments have not been resolved and it is still in coordination. The Air Force conducted a cooperative vulnerability and penetration assessment at a functional AOC-WS 10.1 site and submitted a revision of the outdated 10.1 Test and Evaluation Master Plan (TEMP), which DOT&E approved in 2011. However, there is still no DOT&E-approved TEMP or test strategy for AOC-WS Block 20.

SYSTEM DESCRIPTION

The AOC-WS is a system of systems that incorporates numerous third party, commercial off-the-shelf, and agilely developed software applications. The AOC-WS consists of two instantiations. The AOC-WS 10.1 (AN/USQ-163 Falconer) is the currently fielded backbone system for the AOC. The AOC-WS Block 20 consists of software-based upgrades that are delivered incrementally to enhance warfighter capability. The Air Force continues to provide upgrades to sustain the fielded AOC-WS 10.1 increment, while developing and fielding software capabilities through the AOC-WS Block 20. As more Block 20 capabilities are developed, the AOC-WS will transition from the fielded 10.1 increment to a hybrid configuration of the two instantiations. Ultimately, the Air Force intends to replace AOC-WS 10.1 with Block 20 as the delivered software capabilities mature.

MISSION

The AOC-WS provides the Commander, Air Force Forces or the Joint/Combined Forces Air Component Commander the capability to exercise C2 of joint (or combined) air forces, including planning, directing, and assessing air, space, and cyberspace operations; air defense; airspace control, and coordination of space and mission support operations not resident within the theater of operations.

PROGRAM

The AOC-WS 10.1 began as an Acquisition Category III program when it entered into sustainment over a decade ago. Block 20 began as a Defense Innovation Unit Experimental Pathfinder effort in 2017 and transitioned to six Middle Tier of Acquisition Section 804 programs in FY19. In October 2021, the Assistant Secretary of the Air Force for Acquisition, Technology and Logistics designated both AOC-WS 10.1 and Block 20 as Software Acquisition Pathway (SWP) programs and authorized them to enter the execution phase of development.

The Program Office continues to deliver incremental capability updates and maintenance software revisions to AOC-WS 10.1 via periodic Agile Release Events (ARE). The Air Force delivered ARE 21-10 and ARE 22-02 during FY22, and decided to field them based on results from operational testing at the Ryan Center, Joint Base Langley-Eustis, Virginia, and at the 612th AOC, Davis-Monthan AFB, Arizona.

Block 20 capabilities are developed and fielded following agile software development and continuous integration and continuous deployment principles. The SWP requires Block 20 to deploy a Minimum Viable Capability Release (MVCR) to an operational environment and conduct required operational testing within one year after initial funding obligation. This MVCR occurred on September 17-18, 2022 and delivered initial warfighting capabilities to enhance mission outcomes for the single AOC supporting U.S. Central Command, with delivery of a mature capability to fully support the missions of the remaining eight AOCs expected in late FY24. The program's acquisition strategy had previously identified future capability delivery points by defining multiple MVCRs, but the Program Office altered its approach in late FY22 and has not yet redefined the capability delivery milestones.

The Air Force submitted an initial draft of the Block 20 test strategy for DOT&E review in November 2021, which DOT&E returned with critical comments. The Air Force has not yet submitted a revised test strategy. In accordance with DOD Instruction 5000.87, the program requires a DOT&E-approved test strategy prior to entry into the execution phase of development. However, there is still no DOT&E-approved TEMP or test strategy for AOC-WS Block 20.

» MAJOR CONTRACTORS

- Raytheon Intelligence, Information and Services – Dulles, Virginia
- Science Applications International Corp. – Reston, Virginia

TEST ADEQUACY

The Air Force adequately assessed both AOC-WS 10.1 software upgrades, ARE 21-10 and ARE 22-02, in accordance with the

DOT&E-approved test plan, and DOT&E observed testing of both upgrades. ARE 21-10 underwent integrated testing at the Ryan Center in October 2021 and was subsequently deployed to the field. ARE 22-02 included a major update of the Global Command and Control System – Joint, along with upgrades to other critical targeting and planning systems as well. Based on results from previous operational testing of these upgrades, DOT&E requested the Air Force conduct an operational test of ARE 22-02 functionality and its ability to be installed by typical users. Testing uncovered critical deficiencies, resulting in a fix period and subsequent regression testing prior to fielding to a single site. Operational testing of ARE 22-02 at the first fielded site revealed a recurrence of the deficiencies, so the Air Force paused the test for two months to implement additional fix actions, resuming test once the site's operational schedule allowed.

The Air Force conducted a cooperative vulnerability and penetration assessment at a functional AOC-WS 10.1 site. Deviations from the DOT&E-approved 10.1 test plan due to unforeseen constraints at the site, as well as test resource limitations, precluded a full investigation of the entire system. Although some AOC-WS sites currently use both 10.1 and Block 20 capabilities, the Air Force still needs to conduct operational cybersecurity testing of this hybrid configuration, and of Block 20 capabilities at a fielded site. Additionally, the Air Force has not conducted an adequate cybersecurity assessment of the Block 20 software supply chain.

The Air Force conducted an operational assessment of the Block 20 MVCR on September 17-18, 2022 at a fielded site to inform the user community. This event characterized the ability of the MVCR to meet the performance standards for operations in the U.S. Central Command Theater. In particular, the assessment focused on the production of error-free air tasking orders and airspace control orders for the current mission set. However, the scheduled duration of the test was not sufficient to characterize the system's ability to operate at near-peak system loading. Block 20 capabilities are being deployed incrementally through an agile release capabilities model. Capabilities are released to the field, then feedback is obtained from the users, and the capability is refined to fit warfighter needs. However, capabilities released to date are not sufficient to support meaningful operational testing of major combat scenarios or an evaluation of sustainment, maintenance, and training processes.

The Air Force has not yet met the long-standing requirement to collect and report reliability, availability, and maintainability data for the AOC-WS. The required data capture capability does not exist in AOC-WS 10.1, so the Air Force has deferred this requirement to Block 20.

PERFORMANCE

» EFFECTIVENESS

AOC-WS 10.1 ARE 21-10 is operationally effective. ARE 22-02 is operationally effective with limitations that prevent mission accomplishment in certain circumstances. Currently, Block 20 capabilities cannot support all major combat scenarios. During the MVCR assessment, Block 20 produced an error-free air tasking order for daily operations in the U.S. Central Command Theater.

» SUITABILITY

AOC-WS 10.1 ARE 21-10 is operationally suitable. ARE 22-02 is operationally suitable. Block 20 sustainment, maintenance, and training processes require more development to support meaningful operational testing.

» SURVIVABILITY

The survivability of the AOC-WS, increment 10.1, Block 20, or the hybrid configuration in a cyber-contested environment is currently unknown due to the lack of adequate cybersecurity testing. This includes the cyber supply chain, where, if adequate cybersecurity testing is not accomplished, then potential risks may not be identified and resolved.

RECOMMENDATIONS

The Air Force should:

1. Provide an updated Block 20 acquisition strategy with

product roadmaps that identify when capabilities under development are expected to be sufficiently mature for operational testing; sufficient lead time is necessary for test planning and to comply with DOD policy for SWP programs.

2. Submit an approach to testing the hybrid AOC-WS, inclusive of the continued evolution of 10.1 and Block 20, in their respective TEMPs and test strategies, or ideally in a single, consolidated TEMP or test strategy covering both programs.
3. Conduct cybersecurity operational testing at a fielded AOC that uses both AOC-WS 10.1 and Block 20 in the hybrid configuration to characterize the mission survivability of the system in a realistic, cyber-contested environment.
4. Conduct a cybersecurity assessment of the software supply chain to characterize the effectiveness of the controls and defensive capabilities against expected supply chain threats.
5. Implement a solution to meet the long-standing requirement to collect and report reliability, availability, and maintainability data for the AOC-WS.

B-52 Radar Modernization Program (RMP)

The B-52 Radar Modernization Program (RMP) completed the Critical Design Review milestone in February 2022. Modification of two test aircraft and development of initial system flight software will begin in FY23. Developmental and integrated flight test will begin in FY24 leading to IOT&E, full-rate production and operational fielding in FY27.

SYSTEM DESCRIPTION

The B-52H RMP will replace the legacy APQ 166 radar with the modified APG-79 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 capabilities to track moving surface and air targets.

MISSION

Theater Commanders use units equipped with the B-52H 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-52H 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-52H RMP is an Acquisition Category IB Major Defense Acquisition Program. DOT&E approved the B-52H RMP Test and Evaluation Master Plan (TEMP) in April 2021. In June 2021, the Air Force completed the Milestone B decision and awarded a five-year Engineering, Manufacturing, and Development contract to Boeing. A two-part Milestone C decision is planned in FY24 and FY25 to modify 28 low rate initial production aircraft. A Full-Rate Production decision for the remaining 46 aircraft will follow IOT&E in FY27.

The program completed Critical Design Review in February 2022. Modification of two test aircraft and development of initial system flight software will begin in FY23. Developmental and integrated flight testing is planned to begin in FY24 leading to IOT&E in early FY27. Installation of the Tactical Data Link communication system upgrade necessary to complete RMP operational test requirements is behind schedule, which may reduce early operational test opportunities.

The February 2021 USD(R&E) developmental test assessment concluded that the program test schedule was high risk, with significant similarities to previous aircraft radar development programs that encountered developmental delays. Emerging system integration issues include potential electromagnetic interference between radar and electronic attack systems and regulation of radar operating temperatures in extreme low-temperature environments. Both issues are being assessed by Air Force and Boeing engineering teams.

The Air Force plans to submit a B-52H enterprise cybersecurity test strategy for DOT&E approval in 1QFY23. This strategy defines a comprehensive, integrated cybersecurity test approach across all planned modernization programs, including B-52H Commercial Engine Replacement Program, the B-52H RMP, and multiple communication system upgrade programs.

» MAJOR CONTRACTORS

- The Boeing Company – Oklahoma City, Oklahoma
- Raytheon Technologies – Waltham, Massachusetts

TEST ADEQUACY

DOT&E approved the B-52H RMP TEMP in April 2021. The TEMP defines an adequate operational test strategy and necessary test resources for integrated testing and IOT&E. The B-52H enterprise cybersecurity test strategy defines an adequate cybersecurity test approach across all modernization programs.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Modification of two test aircraft and development of initial system flight software will begin in FY23. Developmental and integrated flight test will begin in FY24. IOT&E will assess operational effectiveness, suitability, and survivability in early FY27.

RECOMMENDATION

The Air Force should:

1. Evaluate opportunities for accelerated Tactical Data Link integration to allow early evaluation of key communication system interoperability requirements.

B-52H Commercial Engine Replacement Program (CERP)

The B-52H Commercial Engine Replacement Program (CERP) is a Middle Tier of Acquisition (MTA) rapid prototyping development program that will transition to a Major Capability Acquisition (MCA) program in FY23. The Air Force is currently using the MTA-developed Virtual System Prototype (VSP) digital design tool to support initial performance analysis, production process planning, system support analysis, and early training activities. The program test strategy and schedules are currently in revision to support the planned FY23 Milestone B acquisition program decision.

SYSTEM DESCRIPTION

The B-52H CERP is the final phase of a multi-program, Air Force B-52H modernization effort. B-52H 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, electrical power generation capacity, and provide modern digital engine controls and displays.

MISSION

Theater Commanders use units equipped with the B-52H 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-52H 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-52H CERP is an MTA rapid prototyping development program that will conclude at the end of the Rapid VSP phase in FY23. In March 2022, the Air Force Acquisition Executive directed program transition to the MCA pathway with a Milestone B entry decision in FY23.

Boeing delivered an initial VSP digital design in September 2021. The Air Force is currently using this digital design tool to support initial performance analysis, production process planning, system support analysis, and early training activities. The final VSP product is planned to be completed in FY23. This digital design product and other supporting system models developed during the MTA phase will require extensive ground and flight test validation to enable their use as primary program data sources.

DOT&E approved the initial B-52H CERP MTA Test and Evaluation Master Plan (TEMP) in March 2020. This TEMP is in revision to support an FY23 B-52H CERP MCA Milestone B decision. The new program acquisition strategy is currently in development and engineering, manufacturing, and development schedules are not yet defined. The Air Force is initiating actions to modify B-52H CERP developmental and operational test aircraft with all preceding modernization upgrades to include the B-52H Bomber Modernized Radar System and communication system upgrades. B-52H CERP developmental and operational testing will be conducted on the final modernized B-52H fielding configuration.

The Air Force plans to submit a B-52H enterprise cybersecurity test strategy for DOT&E approval in 1QFY23. This strategy defines a comprehensive, integrated cybersecurity test approach across all planned modernization programs, including B-52H CERP, the B-52H Radar Modernization Program, and multiple communication system upgrade programs.

» MAJOR CONTRACTORS

- The Boeing Co., – Oklahoma City, Oklahoma
- Rolls Royce Corp., – Indianapolis, Indiana

TEST ADEQUACY

The previously approved B-52H CERP MTA TEMP defines an adequate operational test strategy for the rapid prototyping design phase. This TEMP is currently in revision to support the planned FY23 B-52H CERP MCA Milestone B decision.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

B-52H CERP is in the system design phase. A revised test strategy to support a new MCA acquisition strategy is currently in development to support a planned Milestone B entry decision in FY23. This strategy will include an IOT&E to determine operational effectiveness, suitability, and survivability in both the conventional and nuclear environments.

RECOMMENDATION

The Air Force should:

1. Develop comprehensive verification and validation plans for the VSP and other digital models to enable their use as high-fidelity data sources during system development, production, and deployment.

Defense Enterprise Accounting and Management System (DEAMS)

The Defense Enterprise Accounting and Management System (DEAMS) program has developed an operationally representative integrated test environment, addressing a long-standing DOT&E recommendation. The Air Force Operational Test and Evaluation Center should perform a DEAMS verification and validation (V&V) of its integrated test environment to determine its level of operational representativeness. The results should be used to develop a more operationally representative test strategy to support agile development of new capabilities.

SYSTEM DESCRIPTION

DEAMS is a Defense Business System that uses commercial off-the-shelf (COTS) enterprise resource planning software to provide accounting and financial management services.

The DEAMS Program Management Office (PMO) is following an agile acquisition strategy that adds additional capabilities and users incrementally. DEAMS serves an estimated 16,600 end-users at approximately 170 locations worldwide.

MISSION

DEAMS is intended to deliver accurate, reliable, timely, and auditable financial management information compliant with governing laws, regulations, and policies. DEAMS performs the following core accounting functions:

- Financial System Management
- General Ledger Management
- Funds Management
- Payment Management
- Receivable Management
- Cost Management
- Reporting

Air Force financial managers and tenant organizations use DEAMS to do the following across the Department of the Air Force, the U.S. Space Force, and their supported Combatant and Field Commands:

- Compile and share accurate, up-to-the-minute financial management data and information
- Satisfy congressional and DOD requirements for auditing of funds, standardizing of financial ledgers, timely reporting, and reduction of costly rework

PROGRAM

DEAMS was designated as an Agile Software Development (ASD) pilot program in the FY 2019 National Defense Authorization Act. DEAMS adopted the Scaled Agile Framework (SAFe)® to facilitate agile software development. During FY22, DEAMS completed 4 agile program increments of approximately 15 weeks each, which resulted in deployments of updates to already fielded capabilities.

» MAJOR CONTRACTOR

- CACI – Dayton, Ohio

TEST ADEQUACY

The DEAMS program recently developed a more operationally representative integrated test environment to support shortened development and deployment cycles enabled by agile software development methods. Following FOT&E in FY24, the DEAMS program intends to deploy new capabilities to new user sets in major acquisition commands in FY24. Due to the implementation of the SAFe® agile software development:

1. The approved TEMP for DEAMS is out of date and requires an update.
2. A V&V of the operational representativeness of the DEAMS integrated test environment is needed.
3. An Agile Operational Master Test Plan (AOMTP) with sufficient detail to conduct adequate operational tests of the upcoming DEAMS capability deployments is needed.

PERFORMANCE

» EFFECTIVENESS

In FY20, DOT&E reported that the DEAMS program deployed a software upgrade. The software upgrade introduced a significant number of major software deficiencies that has compromised the operational effectiveness of DEAMS. A significant factor precluding discovery of major software deficiencies prior to deployment was due to limitations in the integrated test environment. In previous DEAMS deployments, operational testing has been conducted after deployment of capabilities.

DEAMS implementation of the SAFe® development is facilitating a software development environment that can focus on faster resolution of critical software deficiencies. However, the DEAMS program has limited resources and cannot rapidly fix some of the software deficiencies. Areas impacting operational effectiveness of the DEAMS program from previous operational testing include:

- Lack of timeliness of displayed information to users
- Problems resulting from software obsolescence and a major system software upgrade
- The need to modernize existing payment processes

» SUITABILITY

In FY20, DOT&E recommended that site-specific workflows are needed to improve the usability of DEAMS. The DEAMS AOMTP should contain a test strategy that will evaluate site-specific operational needs for existing users and future user deployments.

» SURVIVABILITY

DEAMS remains not operationally survivable based upon previous operational tests. In the FY20 DOT&E Annual Report, DOT&E recommended that the DEAMS PMO address cybersecurity vulnerabilities that present a high risk to DEAMS missions.

RECOMMENDATIONS

The Air Force should:

1. Perform a V&V of the operational representativeness and realism of the DEAMS integrated test environment. The Air Force Operational Test and Evaluation Center should provide a report that details any deficiencies in the integrated test environment that would preclude use of the integrated test environment for adequate operational testing prior to FOT&E in FY24 and deployment of new capabilities.
2. Submit an AOMTP and a TEMP update to DOT&E for approval to support the next planned capability deployment to new users in FY24.
3. Conduct a cooperative vulnerability and penetration assessment in FY24 to evaluate cyber survivability of DEAMS missions.

F-15 Eagle Passive Active Warning and Survivability System (EPAWSS)

The Air Force continues to integrate software, firmware, and hardware fixes to improve performance of the F-15 Eagle Passive Active Warning and Survivability System (EPAWSS) and address deficiencies uncovered in ground and flight testing. In June 2022, the program successfully completed a Milestone C Decision Point (DP) 2 authorizing the start of operational aircraft retrofits, and DOT&E approved an update to the Test and Evaluation Master Plan in preparation for dedicated IOT&E in FY23.

SYSTEM DESCRIPTION

The AN/ALQ-250(V)1 EPAWSS is a self-protection system intended to enable the F-15 aircrew to detect, identify, locate, deny, degrade, disrupt, and defeat air and surface-to-air threats during operations within highly contested environments. EPAWSS replaces three functionally obsolete F-15 legacy Tactical Electronic Warfare System components: the AN/ALR-56C Radar Warning Receiver, the AN/ALQ-135 Internal Countermeasures Set, and the AN/ALE-45 Countermeasures Dispenser Set. The EPAWSS radar warning function scans the radio frequency environment and provides the aircrew with identification and location information of potential threat signals. When necessary, the system can respond with countermeasures (jamming or expendables) to defeat a threat radar or missile. EPAWSS integrates with the F-15 AN/APG-82(V)1 radar and mission computer.

MISSION

The Air Force employs the F-15E Strike Eagle as a dual-role fighter, designed to perform air-to-air and air-to-ground missions. EPAWSS provides the primary defensive suite to protect the F-15E during the conduct of both offensive and defensive missions.

The Air Force plans to employ the F-15EX in an air-to-air role similar to the F-15C aircraft it will replace. The expectation is to be an air superiority fighter, flown by active duty and Air National Guard units, to perform both offensive and defensive air-to-air missions. EPAWSS will provide the defensive suite to protect the F-15EX during counter-air missions.

PROGRAM

F-15 EPAWSS is an Acquisition Category IC program that tailored Milestone C into two Decision Points (DPs) to take long-lead hardware procurement off the critical path and deliver the capability as soon as possible. The Air Force Service Acquisition Executive approved Milestone C DP 1 (Production Decision) on December 1, 2020, authorizing the procurement of low-rate initial production aircraft retrofit kits and installation hardware, and DP 2 (Installation Decision) on June 23, 2022, authorizing the start of fleet aircraft modifications. DOT&E approved the Milestone B Test and Evaluation Master Plan in 1QFY18 and an Air Force update on June 16, 2022. The Air Force started modification of the first 2 of a planned 217 F-15Es. Additionally, EPAWSS will field on production deliveries of F-15EX aircraft.

» MAJOR CONTRACTORS

- The Boeing Company – St. Louis, Missouri
- BAE Systems – Nashua, New Hampshire

TEST ADEQUACY

During FY22, the Air Force completed a series of ground and flight test events as part of EPAWSS T&E. All developmental testing was conducted in accordance with the DOT&E approved Test and Evaluation Master Plan, and observed by DOT&E. Ground testing of an uninstalled system at the Integrated Demonstrations and Applications Laboratory (IDAL), Wright-Patterson AFB, Ohio, provided data to evaluate the radar warning function against most radio frequency emitters the system is required to engage in the presence of background emitters. The Air Force tested the jamming effectiveness against a sample of required threats at two government hardware-in-the-loop test facilities: The Electronic Combat Simulation and Evaluation Laboratory, Point Mugu, California, and a test facility at Wright-Patterson AFB, Ohio. The Air Force conducted installed-system testing in the Benefield Anechoic Facility at Edwards AFB, California, to assess integration with F-15E avionics and weapons, as well as installed radar warning performance. The Air Force plans to conduct operationally oriented Integrated Demonstrations and Applications Laboratory and Electronic Combat Simulation and Evaluation Laboratory testing as part of the IOT&E.

The Air Force's 96th Test Wing conducted flight testing of the incremental EPAWSS software releases, each integrating new capabilities with the hardware/

firmware and correcting deficiencies. Operational testers participated in these developmental flights and the aforementioned ground tests. Test data available in early-FY22 were adequate to support DP 2. Dedicated IOT&E ground and flight test events will be conducted in FY23.

In June 2022, the Air Force conducted the final of the three planned developmental cybersecurity assessments in the Boeing Electronic Systems Integration Lab. The Air Force plans to conduct on-aircraft operational cybersecurity testing as part of the IOT&E.

PERFORMANCE

» EFFECTIVENESS

The data collected indicate a low risk to EPAWSS demonstrating operational effectiveness as it proceeds to IOT&E. During FY22, the Air Force continued to mature the software and hardware to address the deficiencies identified during developmental testing, and the additional effectiveness data collected indicate further progress. DOT&E published an interim assessment on September 13, 2022 and will continue to monitor the EPAWSS program as the program conducts an IOT&E in FY23.

» SUITABILITY

The available data indicate risk that EPAWSS will not demonstrate operational suitability as it proceeds to IOT&E. Hardware failure data during flight operations to date indicate the system potentially can meet the requirement for mean time between unscheduled maintenance; however, the very high incidence of built-in test (BIT) failure indications is a significant concern. Correction of the BIT performance and indications prior to entry into IOT&E could ameliorate this risk assessment. Failure to address the BIT performance may drive unscheduled flight line and depot-level maintenance actions. In addition, the aircrew may not have confidence in EPAWSS or may not be aware of an actual failure due to the lack of accurate system status. This may have a negative impact on operations of F-15 units equipped with EPAWSS.

Currently, Air Force aircrews and maintainers (with substantial Boeing assistance) operate and support EPAWSS during flight test using the following contractor-provided elements: training, preliminary technical orders, and support equipment. Technical order changes are being incorporated and should be available for use during the IOT&E. Additionally, Air Force maintainers completed the second of two planned maintenance demonstrations that confirmed their ability to remove and replace each EPAWSS line-replaceable unit and line-replaceable module, and reprogram the EPAWSS software. The Air Force plans to conduct an operationally oriented maintenance demonstration as part of the IOT&E.

» SURVIVABILITY

The available data from cybersecurity testing indicate a low risk to EPAWSS proceeding into operational survivability testing. The Air Force completed planned developmental cybersecurity assessments, and the EPAWSS program continues to improve the EPAWSS cybersecurity posture by implementing and validating corrective actions, based on the susceptibilities and vulnerabilities found during the developmental cybersecurity assessments. The Air Force plans to conduct on-aircraft operational cybersecurity testing as part of the IOT&E.

RECOMMENDATION

The Air Force should:

1. Correct BIT performance and indications prior to entry into IOT&E.

F-15EX Eagle II

The F-15EX Eagle II entered integrated developmental and operational test in FY22, completing 8 of 17 planned two-ship missions. Five four-ship missions are planned for FY23 when the Lot 1B aircraft are delivered. Testing was paused due to restrictions on the use of Link 16. Initial effectiveness data from the missions flown show the F-15EX performed as well as, or better than, the F-15C it is intended to replace.

SYSTEM DESCRIPTION

The F-15EX is a two-seat, twin-engine, multi-role fighter aircraft. It is a derivative of the Qatari F-15QA, which is a derivative of the U.S. 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 Eagle Passive/Active Warning Survivability System for electronic warfare.

MISSION

Although the aircraft is multi-role capable, the U.S. Air Force intends to use the F-15EX with a single pilot, primarily in an air superiority role, for the near-term. 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 is capable of employing a full complement of air-to-air weapons and has two additional weapons stations compared to the F-15E. In addition, the F-15EX will have a very limited capability to employ precision-guided, air-to-surface munitions due to lack of conformal fuel tanks.

PROGRAM

The F-15EX is an Acquisition Category IC program that transitioned from a Rapid Fielding Middle Tier of Acquisition (MTA) program to a Major Defense Acquisition Program on September 6, 2022. The MTA process allowed the Air Force to rapidly obtain two test aircraft within months of program initiation, and begin testing the aircraft within the program’s first year. The Air Force intends to procure 78 F-15EX aircraft, trainers, and support equipment over five procurement lots in five years. As part of the MTA approval process, DOT&E approved the Operational Test and Evaluation section of the Program Strategy Document (i.e., Section 4) in July 2020.

» MAJOR CONTRACTOR

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

TEST ADEQUACY

In May 2021, prior to beginning formal IOT&E, the Air Force flew the first two F-15EX aircraft for early operational assessment within two months of initial delivery. The F-15EX, along with F-15C and F-15E aircraft, deployed to Joint Base Elmendorf–Richardson, Alaska, to participate in the Northern Edge large-force exercise. This exercise provided significant feedback on initial aircraft systems and software, and early discovery of mission planning hardware deficiencies, which have since been corrected.

The Air Force started integrated testing in October 2021, in accordance with the DOT&E-approved test plan, and DOT&E observed the testing. The Air Force collected data to evaluate the F-15EX performing the missions of the F-15C it is replacing. A portion of the missions were flown alongside the F-15C, and other missions were executed by the F-15EX without any F-15C. While it is not a true comparative test, the use of the F-15C was required due to the rapid fielding and having only two Lot 1A F-15EX aircraft delivered for Phase 1 of the operational test and evaluation. With the addition of six Lot 1B F-15EX aircraft expected in FY23, Phase 2 of the test will only use F-15EX aircraft for the effectiveness evaluation.

The Air Force completed eight of 17 planned Phase 1 test missions before the Air Force Operational Test and Evaluation Center declared a pause to testing due to a Federal Aviation Administration imposed restriction on the use of Link 16. At the time of writing, the F-15EX has Federal Aviation Administration approval to transmit Link 16. Testing is expected to resume in 1QFY23.

Following the initial portion of Phase 1 testing, the Air Force’s Air Combat Command clarified that the aircraft configuration for the first operational F-15EX units will not include conformal fuel tanks (CFT). The lack of CFTs will limit the number of external pods and air-to-ground weapons the F-15EX will be able to employ. While the initial Phase 1 testing was done with CFTs, it is likely that the test data produced will still be representative of the production aircraft equipped with two external tanks, as now planned. Until CFTs are procured and provisioned, F-15EX's air-to-ground capabilities will be very limited.

F-15EX operational testing requires a real-time, high-fidelity kill-removal system, known as Open Air Battle Shaping (OABS). The current OABS system is transitioning to the Common Range Integrated Instrumentation System architecture as the DOD continues to incorporate OABS into multiple CONUS ranges and fighter aircraft. Efforts are underway to complete the integration, along with updates to OABS in F-15 operational flight program Suite 9.2 and all F-15 operational flight program releases, to support future operational test requirements. Utilization of OABS enhances the realism of testing against current and future high-fidelity active electronically scanned array threat radar emulators, while providing critical data from open-air, mission-level testing for use in verification, validation, and accreditation of modeling and simulation solutions.

In FY22, the Air Force completed low-level lightning, external radio frequency, electromagnetic environmental, and high-altitude electromagnetic pulse testing at Naval Air Station Patuxent River, Maryland. The Air Force and Boeing are completing vulnerability assessments for ballistic, low-power lasers, and chemical and biological weapons as part of the F-15EX Alternate LFT&E strategy approved by DOT&E in January 2021. Additional susceptibility studies assessing vulnerability to enemy air and surface-to-air defenses, taking into account F-15EX performance and countermeasures, are planned and on track to be completed before the end of operational testing.

PERFORMANCE

» EFFECTIVENESS

Results from the first eight test missions provided compelling data that show the F-15EX was effective, although the limited number of missions did not cover all the planned mission conditions. In particular, threat levels were limited to fourth-generation adversaries with commensurate electronic warfare capabilities. Subsequent testing will assess the system against higher threat levels in more complex mission scenarios. An F-15EX successfully guided a long-range AIM-120 Advanced Medium-Range Air-to-Air Missile in June 2022 as part of a series of integrated (developmental and operational) weapons tests. The final assessment of F-15EX operational effectiveness will be published in the F-15EX IOT&E report in FY24, after the completion of operational testing.

» SUITABILITY

Due to the preliminary, limited data collected to date, DOT&E is unable to make a suitability assessment. However, the data indicate the F-15EX meets (or is close to meeting) its reliability, availability, and maintainability (RAM) requirements and is on track to demonstrate operational suitability. Initial survey data assessing human-systems interactions show the aircrew had positive opinions of F-15EX cockpit usability. While training for both aircrew and maintainers on new systems is lacking, the Air Force plans to have all training available in time for initial operational capability. The program has not yet finalized a charter nor established the Joint Reliability and Maintainability Evaluation Team to review and categorize discrepancies.

» SURVIVABILITY

The Air Force conducted a Mission-based Risk Assessment Process for Cyber that concluded in May 2022. Vignettes developed during the event will form the basis of an integrated cybersecurity test plan for the new F-15EX hardware. The Air Force intends to conduct a cooperative vulnerability and penetration assessment of the Lot 1B F-15EX in 2QFY23, followed by an adversarial assessment. Data from these two assessments should provide insight into the capabilities and limitations of the new F-15EX hardware in a cyber-contested environment.

The Air Force plans to complete Alternate LFT&E assessments and analyses in February 2023. DOT&E will submit a report in 4QFY23 to support the Full-Rate Production decision.

RECOMMENDATIONS

The Air Force should:

1. Ensure the F-15EX test fleet, in particular the Lot

1A aircraft, is modified to include any configuration or equipment changes that occur in later deliveries, so they are representative of the fielding configuration.

2. Complete the Joint Reliability and Maintainability Evaluation Team charter and establish quarterly failure scoring boards to adjudicate reliability data to ensure the F-15EX remains on track to demonstrate operational suitability.
3. Incorporate OABS and high fidelity, active electronically-scanned array, threat radar emulators into future test events, to include any F-15EX FOT&E.

F-15EX integrated test and evaluation at Nellis AFB, October 2021

F-16 Radar Modernization Program (RMP)

The APG-83 F-16 Radar Modernization Program (RMP) is currently on track, with some schedule risk, for a planned Full-Rate Production decision in mid-FY23. The IOT&E to support the decision began in September 2022 under a DOT&E-approved test plan and is expected to complete in March 2023.

SYSTEM DESCRIPTION

The APG-83 Scalable Agile Beam Radar (SABR) is a multifunction, active electronically scanned array radar intended to replace the legacy APG-68 radar. It provides F-16 pilots with air-to-air and air-to-ground situational awareness, high-resolution synthetic aperture radar mapping, fire control, and datalink support to air-to-air missiles.

MISSION

F-16 pilots use the APG-83, along with onboard weapons, to accomplish the full kill chain against air, ground, and surface targets, from beyond visual range and in all weather conditions. As a specific improvement over the legacy system, the APG-83 allows for targeting and engagement from farther ranges with enhanced accuracy and combat identification.

PROGRAM

The APG-83 F-16 RMP is an Acquisition Category II program. DOT&E concurs with the program's test approach as it is being executed; however, the Test and Evaluation Master Plan (TEMP) has not been formally submitted to DOT&E for approval. The Air Force is conducting final coordination on the draft TEMP for planned submission in November 2022.

The F-16 RMP acquisition approach initially included two phases and was not under DOT&E oversight. In Phase 1, the Air National Guard tested, fielded, and acquired 24 radars to meet a U.S. Northern Command Joint Emergent Operational Need Statement (JEONS) requirement for homeland defense. Phase 1 completed in FY20, then the Air National Guard acquired an additional 48 radars under RMP Phase 2, which completed in FY22.

In March 2021, the Air Force approved F-16 RMP Phase 3 with a Milestone C decision. Phase 3, which is under DOT&E oversight, develops full APG-83 capability and equips up to 450 active component F-16s. The Program Office plans to make a Full-Rate Production decision in mid-FY23.

» MAJOR CONTRACTOR

- Northrop Grumman Mission Systems – Linthicum, Maryland

TEST ADEQUACY

F-16 RMP IOT&E is being conducted in accordance with a DOT&E-approved test plan and observed by DOT&E. The testing is adequate to assess the radar capabilities currently being delivered for the F-16. However, inconsistent program funding and unexpected engineering challenges have delayed other components of the overall F-16 system, which has prevented full realization of APG-83 capability. When those components are available, the Air Force should assess any remaining untested expanded radar capabilities in FOT&E.

Cyber survivability testing is being conducted in accordance with a DOT&E-approved test plan and observed by DOT&E. The Program Office conducted a cooperative vulnerability investigation of the radar installed in an F-16 aircraft in April 2022 at Eglin AFB, Florida. Portions that could not be tested on the aircraft are scheduled for laboratory testing at Hill AFB, Utah, in February 2023, along with an adversarial assessment that will close out IOT&E.

PERFORMANCE

» EFFECTIVENESS

APG-83 operational testing conducted to date, including the IOT&E Force Development Evaluation in September 2022, provided compelling evidence that the APG-83 is a significant improvement over the legacy APG-68, even though it cannot yet provide all required capabilities. The radar is limited by the aging F-16 mission computers, obsolete data system, and insufficient network architecture. Upgrades to these aircraft systems have been delayed or have failed to meet mission requirements. The most significant such upgrade would be the transition from MIL-STD-1553 data buses to Ethernet, which is part of the high-speed data network project.

» SUITABILITY

Early data suggest that the APG-83 will be suitable. Although the Air Force has identified some maintenance challenges due to tight clearances between the radome and air data system, the radar has shown vast improvements in overall maintainability over the legacy APG-68. Pilots are generally satisfied with the human-systems interface, although some limitations and tradeoffs were required to integrate it with existing F-16 systems. The tradeoffs result in increased pilot workload for some tasks, such as switching between different displays based on radar mode and function in use.

» SURVIVABILITY

The APG-83's survivability in a cyber-contested environment cannot yet be assessed. Data from the cooperative vulnerability investigation and upcoming adversarial assessment will provide insights into the capabilities and limitations of the new equipment in a cyber-contested environment. The cooperative vulnerability investigation also provided useful system stability information to the program independent of threat cyber effects.

RECOMMENDATIONS

The Air Force should:

1. Submit the TEMP for DOT&E approval.
2. Complete IOT&E and correct any deficiencies.
3. Ensure any remaining expanded radar capabilities are tested via FOT&E after associated aircraft systems, such as the mission computer and data architecture, are modernized.

F-22A – Raptor Advanced Tactical Fighter Aircraft

In FY22, the F-22 program completed FOT&E on the first of several planned annual Capability Releases. DOT&E assessed the Release 1 (R1) operational flight program and its associated capabilities as effective but identified one suitability concern and one cyber survivability issue, with details available in the November 2022 classified test report. The program is currently executing FOT&E on the Release 2 (R2) operational flight program, but Federal Aviation Administration (FAA) restrictions are prohibiting Link 16 transmission – a major impediment to both testing and utilizing a combat capability already installed in the aircraft.

SYSTEM DESCRIPTION

The F-22A Raptor is a fifth-generation, air-superiority fighter aircraft that delivers low observability to threat radars, high maneuverability, sustained supersonic speed, and advanced integrated avionics. The capability release program adds to the F-22's already significant combat capability on an incremental, annual basis. The specific capabilities delivered in each release are available in the November 2022 classified test report.

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 dominance to enable the range of coalition air operations.

PROGRAM

The F-22A Raptor started as a Major Defense Acquisition Program, with the first production aircraft fielding in 2003. Since 2019, the Air Force has been implementing hardware and software modernization efforts as Capability Releases using Section 804, Middle Tier of Acquisition, rapid prototyping and fielding acquisition authorities. The Tactical Link 16 and Tactical Mandates Test and Evaluation Master Plans, approved by DOT&E in 2018, provide the capstone test strategy and concepts for the capability release pipeline. The Air Force completed the R1 Force Development Evaluation (FDE) in March 2022, and DOT&E approved the R2 FDE test plan in September 2022. The Air Force tasked the U.S. Air Force Warfare Center's 53d Wing to execute the R2 FDE, which is planned for October and November 2022.

» MAJOR CONTRACTOR

- Lockheed Martin Aeronautics Company – Fort Worth, Texas

TEST ADEQUACY

The Air Force conducted the R1 FDE in accordance with the DOT&E-approved test plan, and DOT&E observed the events. The FDE adequately assessed the effectiveness and suitability of new software and hardware systems, but fell short of adequately assessing overall mission effectiveness with the new capabilities incorporated. The adequacy shortfall stemmed from delays in fielding the Common Range Integrated Instrumentation System (CRIIS), the most current flight test instrumentation system, which was a known limitation prior to test plan approval. The FDE completed in March 2022 and included the following events: 286 test sorties totaling 332 flight hours; successful employment of Joint Direct Attack Munitions, Air Intercept Missile (AIM)-120 Advanced Medium Range Air-to-Air Missiles, and AIM-9X Sidewinder missiles; and five large-force employment mission trials covering both defensive and offensive counter-air mission tasks. Cyber survivability testing adequately assessed the Integrated Maintenance Information System and other mission systems in FY22. However, for F-22 and other Agile software development programs, limited test capacity often results in operational flight programs and other mission software packages fielding prior to completion of a full software effectiveness and cybersecurity assessment.

The DOT&E-approved R2 FDE test plan includes five large-force employment mission trials, similar to those executed in the R1 FDE, with initial incorporation of the CRIIS. This will enable high-fidelity mission evaluation under the Open Air Battle Shaping construct, once fully implemented.

PERFORMANCE

» EFFECTIVENESS

The F-22 with R1 capabilities demonstrated effectiveness in tasked missions; however, the FAA restrictions on Link 16 transmissions continue to prevent testing and fielding of one of the core enhancements delivered with R1. Final evaluation of Link 16 capability will occur as soon as the FAA lifts the restrictions.

» SUITABILITY

The F-22 hardware and software systems with R1 enhancements are mostly suitable, except for one identified issue detailed in the November 2022 classified DOT&E test report.

» SURVIVABILITY

DOT&E assessed the F-22 as survivable, with one identified issue and final results pending completion of the Integrated Maintenance Information System cyber adversarial assessment in September 2022.

RECOMMENDATIONS

The DOD should:

1. Solidify a plan to accomplish Link 16 testing that demonstrates mission effectiveness and cyber survivability while accommodating FAA protocols, restrictions, and test-specific operating procedures.
2. Conduct a holistic assessment of the T&E enterprise's ability to keep pace with Agile development processes. This assessment should cover program management, test infrastructure, test community workforce, cost effectiveness, and overall capacity, focusing particularly on cyber survivability test capacity.

The Air Force should:

3. Conduct all future FDEs with an accredited flight test instrumentation system, such as CRIIS, to enable high-fidelity, holistic mission evaluations with new capabilities in operationally representative environments.
4. Correct identified deficiencies affecting suitability and cyber survivability.

Global Positioning System (GPS) Enterprise

The U.S. Space Force's Operational Control System (OCS) Architecture Evolution Plan (AEP) commands and controls the current GPS satellite constellation, including GPS III satellites, and has the ability to provide Military Code (M-Code) to appropriately equipped users in the field. As was reported last year, full control of modernized civil and M-code signals and navigation warfare functions have continued to be delayed, due to ongoing development delays of the Next Generation Operational Control System (OCX), along with delays in the fielding of M-code capable receivers. These ongoing delays increase the risk that U.S. and allied warfighters will not be able to conduct operations with GPS-derived position, navigation, and time (PNT) information.

SYSTEM DESCRIPTION

The GPS Enterprise is a satellite-based global radio navigation system of systems that provides accurate and secure PNT information to users worldwide.

The GPS Enterprise consists of three operational segments: space, control, and military users. The space segment includes the GPS constellation of 31 operational satellites. The control segment (primary and alternate sites) operates the GPS constellation; supports launches, anomaly resolution, and disposal operations; and tasks navigation warfare effects in support of Combatant Commands. The user segment includes the Military GPS User Equipment (MGUE) intended to modernize military GPS receivers, including the ability to receive M-code.

MISSION

GPS provides PNT information to military and civilian users globally. Military commanders use the position, navigation, and timing signals provided by GPS for a wide variety of missions. Units equipped with GPS military receivers can navigate and maneuver forces in strategic, operational, and tactical theaters. Units with GPS-equipped munitions can employ them with precision, reducing both collateral damage and the number of expended munitions needed to accomplish a military objective. MGUE Increment 1 based receivers will allow military users to access the more secure M-Code signal. MGUE Increment 2 receivers will use Regional Military Protection, which concentrates higher M-code signal power broadcast by GPS IIIF satellites in a targeted region to ensure the warfighter has continued access to PNT data in contested environments.

PROGRAM

The GPS Enterprise consists of multiple programs pursuing different acquisition strategies to advance the space, control, and user segments.

- GPS III Satellite – Acquisition Category IC program which achieved Milestone C in January 2011. The U.S. Space Force has successfully launched five GPS III satellites since 2018 and plans to launch the sixth satellite in January 2023, with the last of the remaining four GPS III satellites being available to launch by early 2QFY23.
- GPS III Follow-On Production (GPS IIIF) Satellite – Acquisition Category IB program that will provide enhanced Regional Military Protection signals and support for search and rescue services. The Air Force made the GPS IIIF Milestone C decision in July 2020 based on the completion of a Critical Design Review. The first GPS IIIF will be available for launch in 2QFY26.
- OCS AEP – The Air Force fielded OCS AEP in 2007. It features two recent Acquisition Category III upgrades: M-code Early Use (MCEU) and the Contingency Operations (COps). The upgrades allow the system to command and control core M-code capability from the existing GPS constellation consisting of GPS IIR, GPS IIR-M, GPS IIF, and GPS III satellites.
- OCX – Acquisition Category ID program that achieved Milestone B in June 2017 (relieved of Milestone C requirements) and will provide full control of modernized civil and M-code signals and navigation warfare functions. OCX will replace OCS AEP following a successful IOT&E in October and November of 2023, a delay of 9 months from last year's IOT&E scheduled release of January 2023. Following successful OCX deployment, the subsequent OCX Block 3F upgrade will allow OCX to launch as well as command and control GPS IIIF satellites.
- MGUE Increment 1 – Acquisition Category IC program that achieved Milestone B in January 2017 (relieved of Milestone C requirements). The program will deliver M-code capability to the warfighter, improving GPS signal availability in degraded threat environments. Delays with final software and hardware builds by MGUE Increment 1 vendors continue to cause delays to the two remaining MGUE Increment 1 lead platforms (B-2 aircraft and the *Arleigh Burke*-class naval destroyer) test schedules for the Navy and the Air Force. The MGUE Increment 1 program delivered a fully functional aviation/maritime receiver card in September 2022. The Army and Marine Corps will not field their respective lead platforms (Joint Light Tactical Vehicle and Stryker) with the ground-based MGUE Increment 1 receiver cards. Due to Application-Specific Integrated Circuit (ASIC) obsolescence and limited production, the Services plan to use commercially available, MGUE-derived M-code receivers. Those receivers will undergo operational testing outside of the MGUE Increment 1 program of record.
- MGUE Increment 2 – The program is currently structured as two Middle Tier of Acquisition rapid prototyping efforts. The Miniaturized Serial Interface receiver with next-

generation ASIC will deliver improved jam resistance, address MGUE Increment 1 ASIC hardware obsolescence, support the enhanced regional military protection offered by the GPS IIIF program, and support low-power applications (e.g., guided munitions). The handheld receiver will incorporate the Miniaturized Serial Interface receiver with the prototype handheld unit planned to be available in late 2026.

DOT&E approved the GPS Enterprise Test and Evaluation Master Plan (E-TEMP) Revision C on August 25, 2021. Space Systems Command continues to revise the GPS E-TEMP to update threat requirements, address cyber testing, and define the test strategies for OCX, MGUE Increment 2, Nuclear Detonation Detection System control system upgrades, GPS IIIF satellites, and OCX Block 3F. To improve test development, future E-TEMPs will include tailored annexes for each program, including updates to MGUE Increment 1 and Increment 2 programs, GPS IIIF and OCX 3F programs, and civil testing requirements on OCX. The next annex for review and approval is the GPS IIIF and OCX 3F Enterprise and Operational Test annexes signed in November 2022.

The next GPS operational test is an OCX cyber assessment scheduled for August 2023. The GPS Enterprise IOT&E is scheduled to commence in 4QFY23.

The Air Force B-2 Spirit bomber program and the Navy *Arleigh Burke*-class destroyer program plan to operationally test the MGUE Increment 1 aviation/maritime cards in 1QFY23 and 3QFY24 respectively. The GPS Enterprise Multi-Service Operational Test and Evaluation (MOT&E), designed to assess all three third-generation segments together, is scheduled for early 2025.

» MAJOR CONTRACTORS

Space Segment

- Block IIR/IIR-M/III/IIIF satellites: Lockheed Martin Space Systems – Denver, Colorado
- Block IIF satellites: Boeing, Network and Space Systems – El Segundo, California

Control Segment

- OCS: Lockheed Martin Space Systems Division – Denver, Colorado
- OCX: Raytheon Technologies, Intelligence, Information, and Services – Aurora, Colorado
- OCX 3F: Raytheon Technologies, Intelligence, Information, and Services – Aurora, Colorado

User Segment (MGUE Increment 1 and 2)

- MGUE Increment 1 and 2:
  - L3Harris Technologies, Inc. – Anaheim, California
  - Raytheon Technologies, Space and Airborne Systems – El Segundo, California
  - BAE Systems – Cedar Rapids, Iowa
- MGUE Increment 2 Handheld Device:
  - Technology Advancement Group – Dulles, Virginia
  - Raytheon Technologies, Space and Airborne Systems – El Segundo, California
  - BAE Systems – Cedar Rapids, Iowa

TEST ADEQUACY

No operational testing was conducted in 2022 across the GPS Enterprise. While not an operational cyber test, the 4th Test and Evaluation Squadron (4 TES) conducted cyber-resiliency testing of the GPS III satellite simulator at a Lockheed contractor facility in accordance with the DOT&E-approved E-TEMP. DOT&E plans to observe OCX operational testing through late FY23.

The Department of Transportation and the Federal Aviation Administration (FAA) have responsibilities for testing PNT systems that control navigation and traffic control, per the 2019 Federal Radionavigation Plan. DOT&E is working with the FAA to incorporate their OCX test requirements into a GPS OCX civilian test annex to the DOT&E-approved E-TEMP.

PERFORMANCE

» EFFECTIVENESS

Based on previous operational testing, the current OCS AEP control segment is operationally effective, enabling the constellation to use both legacy signals and M-code signals. GPS operators can command and control legacy and 3rd generation GPS III satellites as part of the full GPS constellation, allowing OCS AEP to produce a global core M-code signal usable by M-code capable receivers. The lack of M-code capable receivers currently limits M-Code use by U.S. and allied warfighters.

The Marine Corps Field User Evaluation for the MGUE Increment 1 ground receiver card reported mixed effectiveness and suitability results, which the MGUE Increment 1 Program Office is working to address. The MGUE Increment 1 aviation/maritime receiver card is still under development, with the latest software update delivered in September 2022. MGUE Increment 1 program operational effectiveness will be assessed during operational testing of the B-2 and *Arleigh Burke*-class, currently scheduled for 1QFY23 and 3QFY24 respectively.

» SUITABILITY

Based on previous operational testing, GPS III satellites and OCS AEP are operationally suitable. Developmental testing has revealed maintenance and sustainment concerns with the OCX simulator, technical orders, and training materials that the Program Office is working to address. MGUE Increment 1 program suitability will be determined during operational testing of the B-2 and *Arleigh Burke*-class in 2QFY23 and 4QFY24 respectively.

» SURVIVABILITY

Since the 2016 independent assessment of the OCX program, the Air Force funded and implemented additional cyber security improvements to OCS AEP as well as provided for integrated cyber security reporting. The cyber survivability operational testing planned for late 2025 should assess whether the cyber survivability of OCX is at least as good as that of OCS AEP. To ensure cyber survivability, OCX will have to be integrated with Space Force cyber security reporting, and OCX cyber defenders must be integrated into space operations.

To ensure continuity of GPS operations, the U.S. Space Force needs to conduct a no-notice transfer of control from the primary OCX control station to the backup.

The Program Office continues to develop a space threat plan to adequately evaluate the survivability of the entire GPS Enterprise in a contested space environment that includes kinetic, cyber, electromagnetic spectrum, nuclear, and directed energy threats.

RECOMMENDATIONS

The U.S. Space Force should:

1. Work with DOT&E and the FAA to make sure that civilian GPS user equities are adequately tested.
2. Develop an operational cyber assessment plan to compare OCS AEP and OCX cyber survivability.
3. In coordination with 4 TES, plan to conduct an early end-to-end operational test event to assess the GPS Enterprise's ability to support the warfighter using M-code capabilities under OCX command and control.
4. Plan to conduct a no-notice transfer from the Master Control Station to the Alternate Master Control Station, during the GPS Enterprise IOT&E of the space segment and OCX run control segment, to verify system survivability.

HH-60W Jolly Green II

The Air Force Operational Test and Evaluation Center (AFOTEC) expects to complete IOT&E of the HH-60W in 1QFY23. DOT&E will publish a classified IOT&E report to inform a Full-Rate Production decision in 2QFY23. Developmental testing of capabilities deferred from IOT&E and other aircraft upgrades is proceeding in parallel with IOT&E.

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 an 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

HH-60W is an Acquisition Category IC program. DOT&E approved the LFT&E Strategy in April 2015 and the Milestone C Test and Evaluation Master Plan in January 2020. DOT&E approved the IOT&E plan, and AFOTEC started dedicated IOT&E in April 2022. AFOTEC expects to complete IOT&E in 1QFY23 after successful resolution of procedures for restricted visibility approaches and landings in degraded visual environments (DVE). The Air Force intends to conduct a Full-Rate Production decision in 2QFY23.

» MAJOR CONTRACTOR

- Sikorsky Aircraft Corporation, a Lockheed Martin Company – Stratford, Connecticut

TEST ADEQUACY

The program completed developmental test (DT) of the developmental aircraft software configuration in the first half of FY22 with regression testing of updates to the GAU-2 and GAU-21 weapon systems, aircraft defensive systems, the transponder, and navigation systems. The Air Force conducted open-air flight testing of the updated radar warning receiver and ALE-47 countermeasures dispensing system (CMDS) software to verify correction of deficiencies discovered in previous testing. This DT established a minimum operationally representative configuration to begin dedicated IOT&E. The next aircraft software configuration, including mission planning and GAU-18 weapon system updates, was deferred until after IOT&E. This configuration will be tested in the first of several future FOT&E periods. During DT, the Air Force continued data collection through participation and observation of 41st Rescue Squadron training exercises, collecting 40 percent of required data points prior to the start of dedicated IOT&E.

The Air Force conducted dedicated IOT&E starting in April 2022 in accordance with the DOT&E-approved test plan and observed by DOT&E. Testing focused on end-to-end mission accomplishment over 18 scenarios including open, confined, and mountain terrain; high and low altitude; water and shipboard operations; and a range of threats from small arms to radar-guided missiles. The Air Force was not able to conduct restricted visibility approaches and landings in DVE until September 2022 due to restrictions in the military flight release (MFR). The Air Force flew eight full-mission profiles to characterize aircraft performance in DVE when the MFR restrictions were removed. The Air Force conducted a successful demonstration of an operational CMDS sequence in August 2022 after the Air Force removed the MFR restriction.

The Air Force conducted several phases of cybersecurity assessment. The Program Office and 41st Rescue Squadron restricted some cyber testing on the aircraft due to insufficient hardware spares and software restoration capabilities, as mentioned in previous Annual Reports. Despite these restrictions, The Air Force's testing effort for this program represented a noteworthy advance in aircraft cybersecurity assessment.

The Air Force has completed all testing and analysis efforts described in the DOT&E-approved LFT&E Strategy. These tests and analyses evaluated aircraft system-level vulnerability, personnel force protection, and low-energy laser effects. The Air Force has conducted an integrated survivability assessment against kinetic threats, directed-energy weapons, and electromagnetic pulses as well as chemical, biological, radiological, and nuclear threats, as summarized in the LFT&E Consolidated Report.

PERFORMANCE

» EFFECTIVENESS

The FY23 DOT&E classified IOT&E report will describe how the HH-60W demonstrated most of the capabilities required to recapitalize the legacy HH-60G fleet and support the personnel recovery mission. However, the HH-60W does not provide identical air indications as were available in the HH-60G to support reduced visibility and low-altitude tactical maneuvers. The program plans for upgrades in the next aircraft software configuration to provide improved navigation displays. Otherwise, pilots favorably rate most aspects of the automatic flight control systems and flight director. Crews indicate the intercom system requires improvements to enable effective communications, both external and internal to the aircraft. Datalinks enhanced the crews' ability to locate and communicate with isolated personnel, but the full datalink operability was not tested due to Federal Aviation Administration restrictions, which should be resolved in FY26. The Air Force is replacing the current Situational Awareness Data Link.

» SUITABILITY

The DOT&E report will show that the HH-60W is meeting most reliability and maintainability requirements. Availability and mission capable rate are below threshold, but these measures may have been strongly influenced by unit stand-up issues and delayed updates to defensive systems. Weapon boresight procedures are a significant constraint for maintenance personnel to generate alert aircraft in a deployed location. Deficiencies with the aircraft's alert systems (including maintenance and threat advisories) degraded aircrew situational awareness, and crews reported frequent computer resets. The off-board computer systems for diagnostics, mission planning, and post-mission debrief require usability improvements and better technical manuals. The program is developing an update to the off-board mission planning environment. Cabin aircrew made recommendations to the cabin configuration to better support their missions. Crews also reported ergonomic and usability concerns with the weapons and primary aircrew cabin seats.

» SURVIVABILITY

The Air Force is tracking several deficiencies that result in degraded crew situational awareness from threat warnings and indications on navigation displays during engagements. The program expects to improve threat display integration and missile warning system performance with software updates planned over the next several years. The program also plans to upgrade to a directional infrared countermeasures system.

All the testing and analysis efforts described in the DOT&E-approved LFT&E Strategy were completed. The LFT&E reports provide a detailed analysis of aircraft survivability. While the armor meets survivability and force protection requirements against the specification threat, the program needs to overcome several shortfalls. In addition, the test results of the new fuel system and aerial refueling system should be addressed.

RECOMMENDATIONS

The Air Force should:

1. Update the Test and Evaluation Master Plan with a timeline and resources to address key deficiencies identified in developmental and operational testing, as well as follow-on operational testing of software, weapons, and defensive system upgrades.
2. Address the various recommendations in the LFT&E reports for the cabin and cockpit armor, the fuel system, and the aerial refueling system.

KC-46A Pegasus

The Air Force Operational Test and Evaluation Center (AFOTEC) continues to collect IOT&E data as Air Mobility Command certifies additional receiver aircraft for both test and operational aerial refueling (AR). The Air Force is working with Boeing to develop critical upgrades to the remote vision system (RVS), refueling boom, and defensive systems necessary for closure of IOT&E in FY24.

SYSTEM DESCRIPTION

The KC-46A tanker aircraft is a modified Boeing 767-200ER commercial airframe with military and technological upgrades. KC-46A tanker aircraft upgrades include a fly-by-wire refueling boom, centerline and wing aerial refueling pod (WARP) drogues, a dual remote Air Refueling Operator's Station, enabled by an exterior RVS, additional fuel tanks in the body, a boom refueling receiver receptacle, a 787 digital cockpit update, Large Aircraft Infrared Countermeasures, a modified ALR-69A radar warning receiver (RWR), and Tactical Situational Awareness System (TSAS). The KC-46A cargo bay is designed to accommodate palletized cargo, aeromedical evacuation equipment, and roll-on command, control, and communications gateway payloads.

MISSION

Commanders will use units equipped with the KC-46A to:

- Perform AR in support of six primary missions of nuclear operations support, global strike support, air bridge support, aircraft deployment support, theater support, and special operations support.
- Accomplish the secondary missions of airlift, aeromedical evacuation, emergency AR, air sampling, and support of combat search and rescue.

PROGRAM

The KC-46A Pegasus is an Acquisition Category IC program intended to be the first increment of 179 replacement tankers for the fleet of more than 400 KC-135 and KC-10 tankers. DOT&E approved the Milestone C Test and Evaluation Master Plan update in 2016 and the IOT&E test plan in April 2019. In a May 2020 memorandum, DOT&E communicated to the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics that DOT&E will not submit an IOT&E report on KC-46A until operational testing of a production-representative RVS is complete. The Air Force expects a corrected RVS version 2.0 to be ready for operational testing in mid-FY24. Air Mobility Command has issued seven interim capability releases for KC-46A to support 97 percent of joint force operational refueling taskings.

» MAJOR CONTRACTOR

- The Boeing Company, Commercial Aircraft, in conjunction with Defense, Space & Security – Seattle, Washington

TEST ADEQUACY

KC-46A IOT&E has been ongoing since May 2019. AFOTEC has continued to collect data, in accordance with the DOT&E-approved test plan, to support assessments for sortie generation, AR, airlift, aeromedical evacuation, survivability through threat-avoidance, and sustained operations under adversarial cybersecurity conditions. DOT&E has been periodically observing and continually monitoring all IOT&E testing. In FY22, AFOTEC data collection included WARP loading demonstrations and certification flight testing, RWR and TSAS update integrated testing, participation in the COPE NORTH and VALIANT SHIELD exercises, special fueling operations, and desert operations in Africa.

AFOTEC has executed over 160 IOT&E AR test events for B-1B, B-2, B-52H, C-5M, C-17A, CV-22, E-3G, F-15C/E, F-16C, F/A-18C/D, F/A-18E/F, F-22A, F-35A, F-35B, H/MC-130J, KC-10, and KC-46A receivers. During IOT&E, probe/drogue receivers such as the CV-22, F/A-18C/D, and F-35B have been refueling from the Centerline Drogue System (CDS). The Air Force completed F-15EX AR certification testing in September 2022. The WARP, used to refuel probe/drogue receivers, is under developmental and receiver certification testing. Once complete, it will begin AR operations as part of IOT&E (anticipated beginning 1QFY23).

The Air Force collected and adjudicated suitability data exceeding the minimum planned 1,250 flight hours for IOT&E while accumulating over 10 times the required flight hours for an adequate suitability assessment. The Program Office periodically reviews the entire KC-46A fleet's maintenance data, which currently exceeds 30 times the IOT&E flighthour requirement, to help guide future decisions on the program.

So far, during IOT&E, AFOTEC collected data from over 60 cargo and 18 passenger test events while executing airlift missions throughout the United States and locations in Australia, France, Germany, Guam, Japan, Korea, Morocco, and the United Kingdom.

Boeing and the Program Office completed a Critical Design Review for the RVS 2.0 in June 2022 and are continuing hardware and software laboratory testing for the boom actuator redesign to rectify the stiff boom deficiency. Flight testing of the new boom actuator is anticipated to begin 4QFY23.

AFOTEC is planning a second phase of cooperative and adversarial cybersecurity testing in FY23-24. Future KC-46A operational assessments will be focused on solutions to fleet-wide maintenance and supply issues, as well as already planned changes to the existing baseline (e.g., boom and RVS upgrades).

PERFORMANCE

» EFFECTIVENESS

Deficiencies with the fielded RVS in low sun angles and dynamic lighting conditions continue to degrade boom AR effectiveness. However, the test team recorded zero undetected contacts outside the receptacle during IOT&E AR events throughout FY22. This suggests the restrictions the Air Force put on the system using the RVS have been adequate to avoid additional occurrences of undetected contacts outside the receptacle. These restrictions come at a cost of interrupting boom AR operations if lighting conditions invoke the restrictions.

AFOTEC assessed that a combination of individual cargo-related deficiencies merited generation of a Category I emergency deficiency report against overall KC-46A cargo operations capability. Any of the following individual contributing deficiencies could result in an unsafe cargo configuration problem:

- Complex, unorganized cargo loading guidance.
- Non-standard cargo limitations, causing aircrew confusion and requirement of onboard cargo inspections.
- Restrictions regarding the cargo barrier net can prohibit loading sufficient, or any, cargo if the forward-most cargo does not meet requirements.
- Problems with the Automated Performance Tool software used to calculate aircraft weight and balance can increase loadmaster workload and require complex manual calculations, introducing potential human error.
- Aerial port operational restrictions caused by inadequate technical guidance increase workload for loading personnel and loading times, driving KC-46A incompatibilities within the Defense Transportation System.

AFOTEC attempted to evaluate performance of the Roll-On Beyond-line-of-sight Enhancement palletized data communications system during VALIANT SHIELD. However, problems with network and cryptographic setup, exacerbated by inadequate technical data, prohibited its successful demonstration.

» SUITABILITY

Operational availability (≥80 percent threshold) and mission capable rate (≥90 percent threshold) are currently well below their threshold requirements, as are several secondary suitability measures. The latest factors affecting these measures include scheduled inspections and reliability problems with two fuel system components. In particular, fuel manifold leaks have degraded receiver capability and caused mission delays or cancellations since FY20. The Program Office is aggressively attempting to address suitability problems and, based on the program's reliability growth plan, the program may still meet their suitability requirements by 50,000 fleet flight hours.

» SURVIVABILITY

The program continues work on software updates to the TSAS and RWR systems and mission data files in order to improve survivability, including integrated open-air range testing of recent updates in June 2022. Analysis of the data is ongoing to determine whether further improvements are necessary to ensure threat identification and avoidance capabilities are adequate before the closure of IOT&E on these systems.

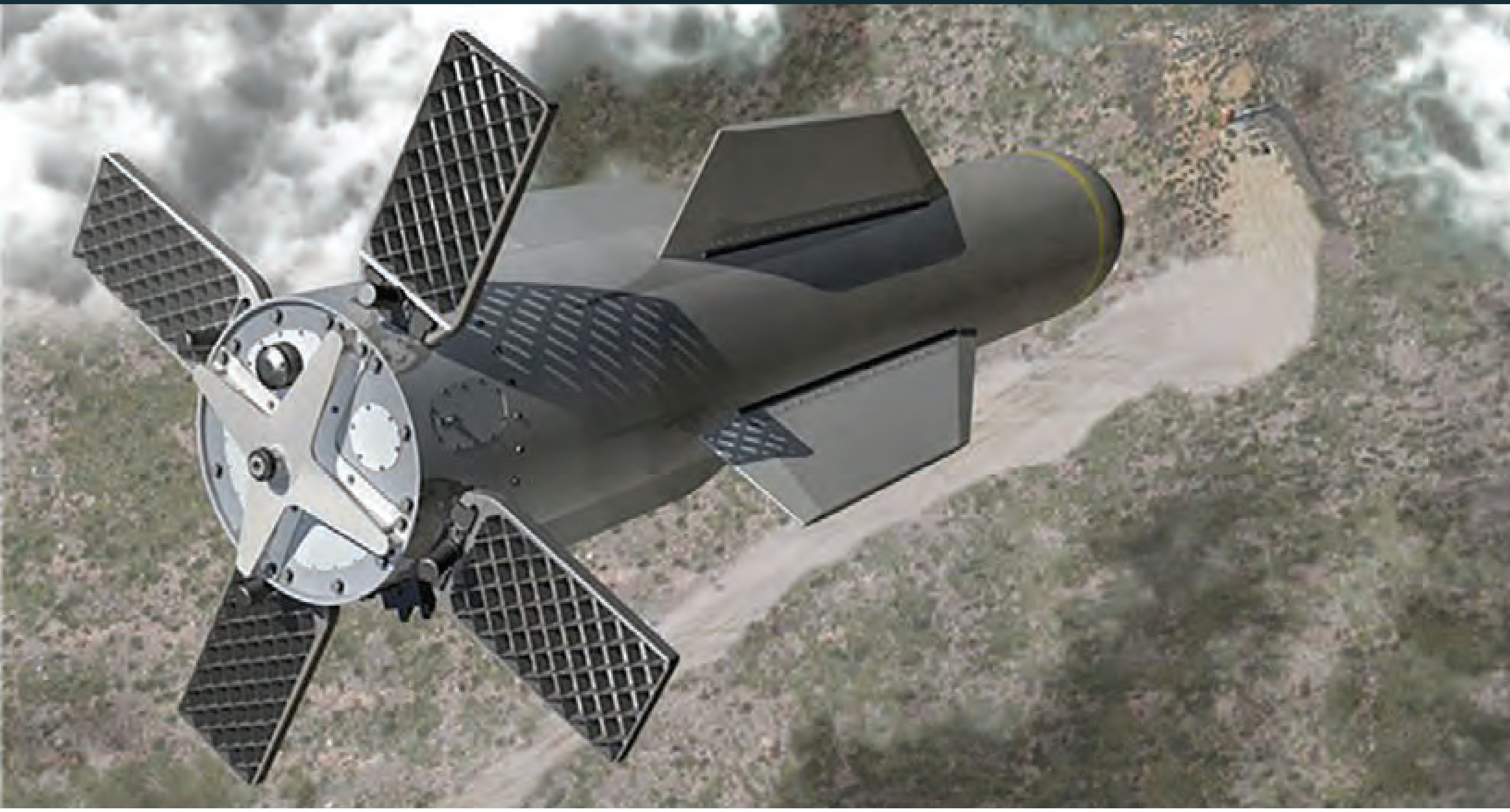
Active and passive system electromagnetic pulse testing in FY21 indicated that the KC-46A has basic survivability in a nuclear environment. The program will conduct electromagnetic pulse direct electric current testing in early FY23 to determine the extent of that survivability.

RECOMMENDATIONS

The Air Force should:

1. Continue to redesign the RVS and refueling boom to facilitate their readiness for operational testing, scheduled in FY24.
2. Address the collection of cargo-related deficiencies to improve cargo-carrying operations.
3. Continue to improve systems that support threat identification and avoidance to improve aircraft and aircrew survivability.

Massive Ordnance Penetrator (MOP) Modification



In FY22, the Air Force conducted three full-scale performance tests of the Large Penetrator Smart Fuze (LPSF) integrated into the Massive Ordnance Penetrator (MOP) and began subscale lethality testing. The Air Force has postponed fielding of the LPSF-enabled MOP from FY22 to at least FY25 due to delays in constructing the required target surrogates.

SYSTEM DESCRIPTION

The Guided Bomb Unit (GBU)-57 MOP is a large, GPS-guided, penetrating weapon designed to attack hard and deeply buried targets (HDBTs) such as bunkers and tunnels. The GBU-57 warhead is intended to be more lethal than its predecessors, the GBU-28 and GBU-37. The LPSF integrates 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 in the Air Force inventory programmed to employ the MOP.

MISSION

Provide Combatant Commanders with a low-observable platform-deliverable, conventional HDBT defeat capability to acheive national security objectives.

PROGRAM

The MOP was developed from an Air Force-led, Quick Reaction Capability (QRC), SECDEF special interest effort. MOP transitioned to an Acquisition Category IC program in August 2017. The Air Force established the LPSF QRC program in August 2018 to respond to an Urgent Operational Need, validated in July 2018, to integrate and qualify a smart fuze capability into the MOP. This upgrade provides the capability to hold additional high-value HDBTs with limited threat intelligence at risk.

In FY21, the Air Force Program Executive Officer for Weapons pulled funds from the full-scale LPSF MOP testing due to contract award delays and significant Defense Threat Reduction Agency (DTRA) target construction overruns. In FY22, target construction was further delayed by pandemic-induced supply and labor shortages, and the loss of scheduling priority status at the test range. Based on current funding options, the LPSF MOP fielding will begin in FY25 or later.

The next phase of the program intends to finalize smart fuze software, improve weaponeering tactics, and validate through demonstration lower-risk smart fuze capability against a full-scale, high-fidelity underground target.

» MAJOR CONTRACTOR

- The Boeing Company, Defense, Space & Security – St. Louis, Missouri

TEST ADEQUACY

In November 2021 and May 2022, the Air Force completed the second and third live weapon drops from B-2s to validate MOP performance. The events were in accordance with the DOT&E-approved Smart Fuzing Test Strategy and observed by DOT&E.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E will provide a classified assessment of MOP effectiveness and suitability at the conclusion of the LPSF effort. The survivability assessment of MOP in a contested environment is classified.

RECOMMENDATIONS

The Air Force should:

1. Revalidate the Urgent Operational Need requirement for the LPSF QRC against legacy and pacing threats.
2. Complete the LPSF testing to validate the ability of MOP to meet Combatant Command requirements.

DTRA should:

1. Evaluate and expedite the contracting and test plan review processes to minimize delays to target construction and test execution.

MH-139A Grey Wolf

After several delays, the contractor obtained the third Federal Aviation Administration supplemental type certification (STC) required to support an initial military flight release. Four MH-139A aircraft were then transferred to the Air Force in August 2022 to begin government-led developmental flight testing. The current program schedule provides only a few months to collect operationally relevant data before the Milestone C decision, currently scheduled in January 2023. The MH-139A program needs to address several additional challenges to mitigate the risk to meeting operational effectiveness, suitability, and survivability requirements.

SYSTEM DESCRIPTION

The MH-139A Grey Wolf is a dual-piloted, twin-engine helicopter based on the commercial AW139 with added military capabilities in communication, navigation, identification, and survivability.

MISSION

The Air Force intends for the MH-139A to replace the UH-1N to provide rapid transport capability for two primary commands:

- Air Force Global Strike Command (AFGSC) will use the MH-139A to support the nuclear security missions by providing emergency security response and convoy escort at Minot AFB, North Dakota; Malmstrom AFB, Montana; and Francis E. Warren AFB, Wyoming.
- Air Force District of Washington (AFDW) will use MH-139A to provide contingency response, continuity of operations, and executive transport for senior government officials in the National Capital Region.

In addition, MH-139A-equipped units will conduct secondary missions for multiple commands:

- Air Force Materiel Command will provide test range support to Eglin AFB, Florida, and developmental test aircraft from Duke and Hurlburt Fields, Florida.
- Air Force Reserve Command will provide formal flight training at Maxwell AFB, Alabama.
- Air Education and Training Command will provide medical evacuation and support operations to the Air Force Survival School at Fairchild AFB, Washington.

All commands will perform search and rescue via the National Search and Rescue Plan and Defense Support to Civil Authorities.

PROGRAM

MH-139A is an Acquisition Category IB program. DOT&E approved the Milestone B Test and Evaluation Master Plan in June 2018 and the Alternative LFT&E Strategy in May 2019. In April 2021, the program reported an Acquisition Program Baseline breach to the Service Acquisition Executive, with a delay of the Milestone C decision beyond the threshold date of September 2021.

The MH-139A acquisition strategy relies on contractor flight-testing to obtain a series of civil STC approvals before the military flight release required for government-led developmental flight test. Three of eight STCs were required for the initial military flight release. The contractor gained the third STC approval in July 2022, and four test aircraft were transferred to the Air Force in August 2022. As a result, only a limited portion of testing will likely be accomplished before the Milestone C decision, currently scheduled in January 2023. DOT&E and the Air Force Operational Test and Evaluation Center (AFOTEC) intend to provide reports to inform this decision. IOT&E is scheduled for late FY24 to support a Full-Rate Production decision in FY25.

» MAJOR CONTRACTOR

- Boeing Defense, Space & Security – Ridley Park, Pennsylvania

TEST ADEQUACY

The Air Force participated in contractor ground and flight testing at Duke Field, Florida, and at contractor facilities in Philadelphia, Pennsylvania. These tests supported the civil STC process, specification compliance, and airworthiness testing. The military utility of this phase of testing was limited.

Contractor testing focused on mitigating or removing contractor-imposed operating restrictions. Additional tests were conducted in September 2022 to evaluate performance at high density altitudes and high aircraft gross weights. These tests are necessary to validate the expanded operating envelope of the MH-139A. The crews using the MH-139A are expected to operate up to the edge of the allowed operating envelope, increasing the importance of the high-density-altitude tests for determining mission capability.

Government-led developmental flight testing began in August 2022, with planned demonstrations of military subsystems, including the fast-rope insertion/extraction system bar, military communications, crew-served weapons, and the countermeasures dispensing system. Due to the limited time between the start of government-led flight testing and the Milestone C decision, there are limited opportunities to collect operationally representative performance data to inform the decision.

The Air Force published its seventh periodic report in January 2022, which summarized their observations from contractor testing and additional site visits to foreign government and law enforcement operators of the AW139. The Air Force will produce an interim summary report on all testing accomplished to date in accordance with a DOT&E-approved test concept to support the Milestone C decision.

The Air Force is executing live fire testing of all the aircraft components and subsystems described in the DOT&E-approved Alternative LFT&E Strategy. The Air Force conducted all testing in accordance with the DOT&E-approved test plans, and observed by DOT&E. The Air Force expects to perform full-scale dynamic testing for flight-critical subsystems during the next six months. Most testing is proceeding close to plan; however, persistent problems in acquiring technical data and some aircraft components from the contractor are delaying execution of some portions of the live fire test program.

DOT&E approved the electromagnetic pulse (EMP) test plan and reviewed a Program Office-developed plan to perform infrared signature testing to collect aircraft survivability data. The EMP testing is not currently scheduled due to negotiations with the contractor.

PERFORMANCE

» EFFECTIVENESS

MH-139A deficiencies identified in ground and flight testing to date continue to represent a risk to MH-139A meeting operational effectiveness requirements. Newly identified concerns include the certified envelope of the automatic flight control system not matching the expanded envelope of the aircraft, sensor display availability to the crew in the cabin, and intercommunication system deficiencies.

Concerns persist from the previous Annual Reports regarding the capability of the cabin layout to support employment of armed tactical response forces, as well as flight manual restrictions on takeoffs in crosswinds or near obstacles. The program is pursuing options to modify the cabin layout to support the tactical response forces and their required equipment while also working with AFGSC to update their concept of operations. International users of the AW139 recommended changes including the type of hoist, the location of the fast-rope insertion/extraction system bar, and other cabin configuration changes.

» SUITABILITY

The Program Office needs to address several challenges for the MH-139A to be operationally suitable. As reported in previous reports, expansion of the MH-139A operating envelope relative to the commercial AW139 baseline may stress powertrain components and increase maintenance requirements. AFOTEC collected observations from international users of the AW139 recommending routine corrosion-prevention measures to minimize long-term airframe maintenance. They also noted potential reliability shortfalls of the installed hoist system that the Air Force should monitor in testing. The contractor-provided mission planning system is not compatible with the Joint Mission Planning System and may not support current AFGSC and AFDW mission planning procedures.

» SURVIVABILITY

The Program Office needs to address several challenges for the MH-139A to be survivable against kinetic and electromagnetic threats. Ballistic testing of various components and subsystems has provided valuable information on the damage tolerance of the aircraft and will inform planned subsequent aircraft system-level assessments. The Air Force is preparing final test reports for completed component testing, along with plans for survivability and vulnerability analyses. DOT&E and the Air Force are reviewing cabin and cockpit armor protection against the specification threat and other operationally representative small arms threats, at all relevant ranges.

The original contractor-proposed fuel cell design did not meet the required military standard for vendor qualification against a particular threat. The Program Office and AFGSC are evaluating a modified design to correct this deficiency.

RECOMMENDATIONS

The Air Force should:

1. Provide sufficient time for adequate government-led flight-testing before the Milestone C decision.
2. Execute the approved EMP test plan to assess aircraft survivability in expected missions at the AFGSC and AFDW operating areas.
3. Address the performance of the armor and fuel system against ballistic threats.
4. Develop corrective action plans for deficiencies that affect operational requirements, including mission planning and cabin configuration.

Small Diameter Bomb Increment II (SDB II)

The Small Diameter Bomb Increment II (SDB II) program continued integration efforts on the F-35 and limited supplemental testing on the F/A-18E/F before resumption of the Navy F/A-18E/F Quick Reaction Assessment planned for 1QFY23. In FY22, the Navy conducted 8 out of 10 planned SDB II releases required for declaration of an Early Operational Capability (EOC) for F-35B with software blocks 30R07 and 30R08: 5 successful releases of the SDB II from F-35B 30R07 test aircraft and 3 successful releases from F-35B 30R08 test aircraft. In September 2022, the Air Force declared Initial Operational Capability (IOC) for F-15E.

SYSTEM DESCRIPTION

The SDB II, also known as the GBU-53/B StormBreaker, is an air-to-ground glide weapon capable of destroying moving targets in adverse weather by using a multi-mode seeker. SDB II is a 250-pound weapon that uses deployable wings to increase standoff range. It is the first Air Force network-enabled weapon to use weapon datalink (WDL), allowing post-launch tracking and control of the weapon via in-flight target updates. The seeker uses multiple sensors to operate in adverse weather. Once launched, SDB II guides to a designated target cue which is updated inflight via the WDL until the seeker provides terminal guidance to the target. SDB II is fielded on the F-15E, and integration efforts continue on the F/A-18E/F and F-35B/C.

MISSION

Combatant Commanders will use units equipped with the SDB II to attack stationary and moving ground and littoral targets in adverse weather conditions at standoff ranges.

PROGRAM

SDB II is a joint Air Force and Navy Acquisition Category IC program intended to deliver capabilities deferred from SDB I. DOT&E approved the SDB II Milestone C Test and Evaluation Master Plan (TEMP) in April 2015. The TEMP update, including a cybersecurity strategy for Multiservice Operational Test and Evaluation (MOT&E) Phase II, was originally planned for FY22 but now is expected in FY23.

The Air Force fielded SDB II on the F-15E following completion of MOT&E Phase I with an early fielding report in July 2020 and declared IOC in September 2022.

The Navy is integrating the SDB II on the F/A-18E/F as part of a Quick Reaction Assessment approved by the Commander, Operational Test and Evaluation in June 2020. Integration is expected to be completed as early as 1QFY23.

Completion of MOT&E Phase II on the F-35 is expected in FY25. The F-35B 30R07 is progressing towards a limited envelope EOC declaration 1QFY23. In parallel, testing of the SDB II on the F-35B/C 30R08 started in FY22 with developmental environmental and loads testing, and is expected to complete in FY23 for the F-35B, leading to a second full envelope EOC declaration by the Marine Corps. Testing on the F-35C 30R08 is expected to complete in FY24 leading to an EOC declaration by the Navy. Testing on the F-35B/C 41R01 is scheduled for FY23 to FY25 supporting an IOC declaration by the Navy and informing the Full-Rate Production decision for the SDB II in FY25.

» MAJOR CONTRACTOR

- Raytheon Missiles & Defense – Tucson, Arizona

TEST ADEQUACY

The Navy conducted MOT&E testing in accordance with the DOT&E-approved Milestone C TEMP. Certain test limitations including cryptographic modernization delays, F-35B operational flight program limitations, and range safety restrictions have limited the findings. However, in the eight releases from the F-35B, the aircraft showed the capability to condition the weapon for laser, coordinate, and normal attack modes. Additionally, current range safety restrictions do not allow for operationally relevant employment of all-up-round SDB IIs, resulting in missed training and testing opportunities while putting a strain on a limited supply of costly guided test vehicles.

MOT&E Phase I cybersecurity testing conducted by the Air Force was inadequate to support an independent evaluation. The test shortfalls from Phase I need to be addressed during MOT&E Phase II testing.

PERFORMANCE

» EFFECTIVENESS

F-35B limited envelope integration and F/A-18E/F integration issues will need to be resolved for the SDB II to be operationally effective in all mission contexts. The F-35B EOC configuration, allowing only a single weapon release and no WDL post-launch control (consistent with the release conditions observed during the seven SDB II releases in FY22), will heavily restrict tactical employment of the bomb when initially fielded on the F-35B.

F/A-18E/F integration testing in early FY22 showed multiple integration issues stemming from various software faults found in the aircraft, weapon, and mission planning systems, as well as a bomb rack hardware issue related to SDB II employment. These issues, combined with the expiration of legacy encryption keys, resulted in a broad effort to upgrade all major software types (i.e., aircraft, weapon, WDL, and mission planning) in a well-coordinated and integrated manner. The Navy is implementing cryptographic modernization of the encryption keys to allow resumption of the testing. Additionally, the Navy is addressing the bomb rack hardware issue to lessen the likelihood of it inducing a failure or degrading weapon performance when ejecting the SDB II.

The Navy flew two F/A-18E/F envelope expansion missions with one successful and the other suffering a release abort. The software issue causing the abort was quickly identified and a fix incorporated in the next weapon software release.

The SDB II continues to be operationally effective as employed by the F-15E. The range safety restrictions mentioned above and real-world contingencies have delayed SDB II Operational Test and Weapon System Evaluation Program drops during FY22. Despite these delays, the Air Force declared IOC in September 2022.

» SUITABILITY

Ongoing MOT&E testing is required to inform a suitability assessment, but the SDB II appears to be on track to be operationally suitable when employed from the F-35B and the F/A-18E/F. The complexity of cryptographic information delivery, loading, and mission planning (e.g., the exclusion zone creation processes), continues to be a problem with only modest mission planning improvements incorporated into the Joint Mission Planning System to date.

The SDB II continues to be operationally suitable as employed by the F-15E.

» SURVIVABILITY

The survivability of the SDB II in a cyber-contested environment is currently unknown due to the lack of adequate test assets provided by the vendor, which resulted in inadequate cybersecurity testing during MOT&E Phase I.

RECOMMENDATIONS

The DOD should:

1. Work with the candidate open-air-ranges for SDB II integration trials on the F-35 to address and mitigate self-lasing restrictions. Additionally, the DOD should work with the ranges to reassess restrictions on all-up-rounds and release profiles, to allow operationally representative employment by all platforms.
2. Continue to advocate for operationally suitable initiatives to streamline the cryptographic information delivery, loading, and verification process.

The Navy should:

1. Develop and fund an adequate MOT&E Phase II cybersecurity T&E strategy to support an evaluation of SDB II survivability in a cyber-contested environment. The SDB II Program Office should also update the Milestone C TEMP to reflect this commitment.

The SDB II Program Office should:

1. Continue efforts to streamline the mission planning process to decrease the time required and increase reliability, particularly with regard to cryptographic data entry.

Space Command and Control System (Space C2)

The Space Command and Control (Space C2) system did not undergo any DOT&E-approved operational testing activities in FY22, primarily due to delayed product delivery, understaffed development teams, unclear test team constructs and responsibilities, and development focus on non-critical capabilities. To address those concerns, the program changed key leadership personnel, restructured development teams, more clearly defined their integrated testing construct, and refocused capability development to only the most crucial capabilities. Despite the lack of operational testing, one Data-as-a-Service capability, Warp Core, was conditionally accepted for operations by the U.S. Space Force (USSF) in FY22, pending completion of cyber survivability testing. Two other data environments (known as tenants) within Warp Core were operationally fielded by the Air Force and North American Aerospace Defense Command (NORAD)/U.S. Northern Command (USNORTHCOM).

SYSTEM DESCRIPTION

The Space C2 system uses a common commercially supported platform to access data and services for user applications that enable command and control operations. System capabilities fall into three general categories: Battle Management Command and Control, Space Domain Awareness, and Space Defense. Space C2 enables multi-domain operations that are integrated with classified mission partner capabilities.

Space C2 uses a hybrid cloud, as well as hardware at operations centers for resiliency and accessibility.

The system has its own continuous integration/continuous deployment (CI/CD) pipeline for capability and application development.

MISSION

USSF Guardians will use Space C2 to provide a wide range of battle management command and control, space domain awareness, space defense, and cross-mission data capabilities to facilitate timely, quality battlespace decisions by DOD and mission partners at multiple classification levels. Those capabilities include infrastructure, data and enterprise services, and mission applications to enable responsive, resilient operational-level command and control capabilities for the National Space Defense Center, the Combined Space Operations Center, and 18th and 19th Space Defense Squadrons.

PROGRAM

The Space C2 program was initiated as a Development, Security, and Operations (DevSecOps) pathfinder in 2019. The program is currently seeking designation as a software acquisition pathway (Execution Phase) program. USD(A&S) has placed conditions on that declaration, including the development of a DOT&E-approved Test and Evaluation Strategy (TES) for the program. The formal designation is anticipated in December 2022. The TES has been in-work for 3 years but has not yet been formally submitted to DOT&E for approval. The TES is expected to enter into formal approval coordination in early FY23.

In FY22 the program restructured its capability development efforts to focus on the near-term challenge of retiring outdated Space Defense Operations Center infrastructure. The restructure was done to accelerate delivery of Advanced Tracking and Launch Analysis System (ATLAS) capabilities to allow for the decommissioning of the Space Defense Operations Center, while deemphasizing the delivery of non-critical applications. The restructure included a realignment of existing development teams and associated priorities as well as a change of program leadership personnel.

The program will use an integrated testing construct and has made significant efforts to define how that testing will be accomplished within USSF's new Integrated Test Force model.

Despite the lack of operational testing, one of the program's major capabilities – Warp Core, the program's current Data-as-a-Service capability that provides data distribution, manipulation, analysis, and visualization capabilities to its users – was fielded to the Air Force and NORAD/USNORTHCOM to support readiness data analytics and Operation Allies Refuge activities respectively.

» MAJOR CONTRACTORS

- General Dynamics Mission Systems – Fairfax, Virginia
- L3Harris Technologies, Inc. – Colorado Springs, Colorado
- Leidos Inc. – Reston, Virginia
- Lockheed Martin – Littleton, Colorado
- ManTech – Herndon, Virginia
- Omitron – Colorado Springs, Colorado
- Palantir Technologies, Inc. – Denver, Colorado
- Parsons Corporation – Centreville, Virginia

TEST ADEQUACY

The Space C2 program did not conduct any operational testing in FY22. USSF's Space Training and Readiness Command submitted two operational test plans to DOT&E for approval. The first test plan is a cyber survivability adversarial assessment plan for Warp Core, Space C2's Data-as-a-Service capability. The second test plan is the overarching plan covering multiple test events for the phased-delivery of ATLAS. The first ATLAS operational test is planned for early FY23 and will focus on foundational capability deliveries that are the key underpinnings of future ATLAS capabilities.

One system capability (Warp Core) was operationally accepted by USSF's Space Operations Command in October 2021. That operational acceptance was granted with a condition to complete DOT&E-mandated cyber survivability testing. That testing is scheduled to occur in early FY23.

Warp Core has undergone developmental cybersecurity testing, both by the developer and external non-governmental organizations. Those test results did not identify significant findings or vulnerabilities with Warp Core. Government-led cooperative vulnerability identification and cooperative vulnerability and penetration assessment (CVPA) activities were conducted on Warp Core in FY21, but those tests were limited in scope and the system was not in an operationally-representative configuration. DOT&E personnel observed the CVPA and the testing was accomplished in accordance with the DOT&E-approved test plan.

Two other tenants that share Warp Core's virtual space were fielded without operational testing. The Air Force and NORAD/USNORTHCOM fielded Envision and NorthStar, respectively, to support readiness data analytics and Operation Allies Rescue and Operational Allies Welcome activities, respectively.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

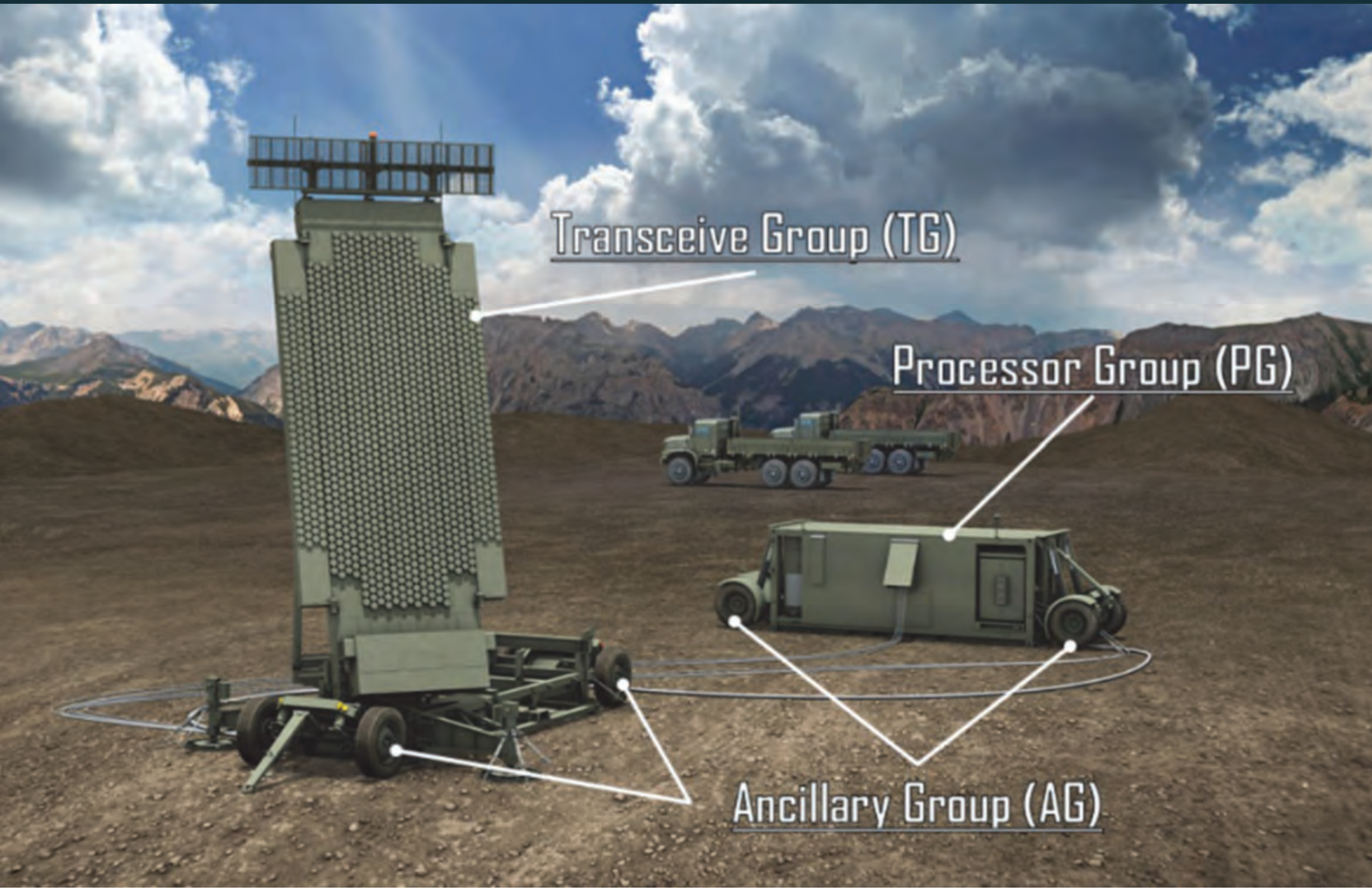
Because no operational testing has been performed on Space C2, DOT&E cannot assess its effectiveness, suitability, or survivability. In addition, DOT&E is concerned that the lack of cyber defenders currently assigned to Space C2 poses a significant risk to its cyber survivability.

RECOMMENDATIONS

The USSF should:

1. Continue to define their Integrated Test Force construct, in order to conduct operational testing earlier in program timelines to realize the benefits of agile program development.
2. Synchronize across product deliveries within Space C2 to enable efficient testing of related capabilities.
3. Perform government-led operational cyber testing (i.e. CVPA and adversarial assessment) on Space C2's software factory to ensure CI/CD pipeline survivability.
4. Assign cyber defenders for Space C2-related capabilities.

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



In February 2022, the Air Force selected Lockheed Martin as the Three-Dimensional Expeditionary Long-Range Radar (3DELRR) TPY-4 production contractor to replace the aging AN/TPS-75 passive electronically scanned array, three-dimensional radar. In April 2022, Program Executive Office Digital executed the Lot 1 initial production option for Lockheed Martin to produce two units, designated IP1 and IP2. The Air Force plans to start government developmental testing on IP1 in 2QFY24 and IP2 in 3QFY24. The Air Force plans for dedicated IOT&E in 3QFY24 to support an initial operational capability of six fielded TPY-4s in FY25.

SYSTEM DESCRIPTION

3DELRR TPY-4 is designed to serve as the organic radar for the U.S. Air Force Control and Reporting Center (CRC) Weapon System (WS) providing the capability to perform long-range detection of both air-breathing threats and theater ballistic missiles. The 3DELRR employs a single-face, rotating, active electronically scanned array with a highly distributed and scalable digital beam forming architecture. The active electronically scanned array incorporates power-efficient, reliable, and commercially sourced Gallium Nitride transmitters, low-noise digital receivers, and efficient power conversion.

MISSION

The U.S. Air Force employs 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 defensive operations. The 3DELRR will 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 (including 5th-generation fighter aircraft) 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 Rapid Fielding Middle Tier of Acquisition program, which the Air Force is planning to transition to a Major Capability Acquisition program by December 2023.

» MAJOR CONTRACTOR

- Lockheed Martin Corporation – Syracuse, New York

TEST ADEQUACY

There was no 3DELRR government test activity in FY22. The Air Force plans to conduct an early operational assessment on Lockheed Martin's Production Representative Unit radar at Eglin AFB in 4QFY23. The Air Force plans to utilize integrated testing at every opportunity after developmental testing starts in 2QFY24 and plans to start dedicated IOT&E in 3QFY24.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

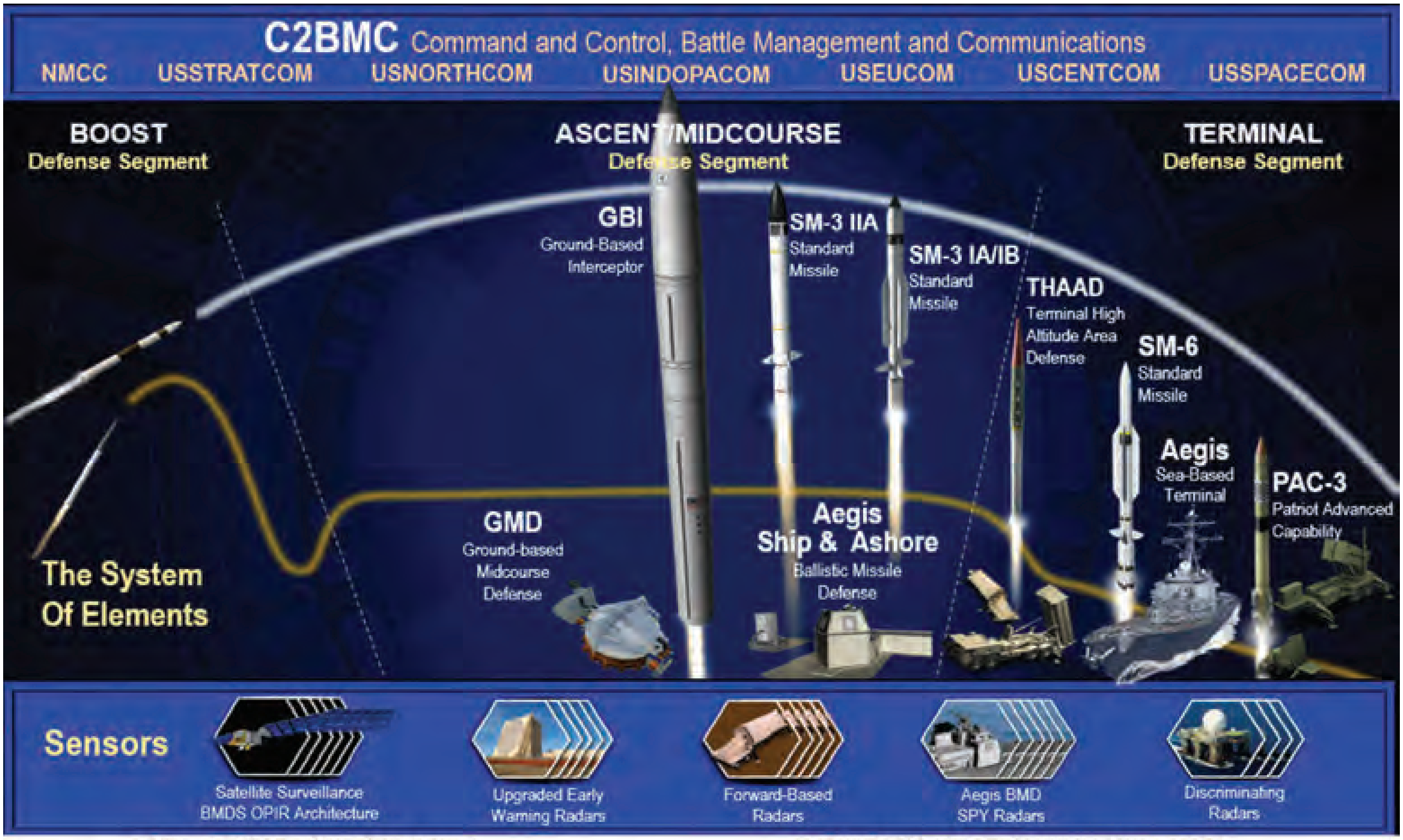
DOT&E will assess operational effectiveness, suitability and survivability in the FY24 DOT&E report, if testing is initiated as planned in 4QFY23.

RECOMMENDATION

The Air Force should:

1. Plan and resource for appropriate, threat-representative targets and electronic attack threats.

MISSILE DEFENSE SYSTEM



BMD - Ballistic Missile Defense
BMDS - Ballistic Missile Defense System
NMCC - National Military Comand Center
OPIR - Overhead Persistent Infrared
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
USSTRATCOM - U.S. Strategic Command

> **The MDS has demonstrated a measured capability to defend the United States, deployed forces, and allies from a rogue nation's missile attack.**

Missile Defense System (MDS)

The Ground-based Midcourse Defense (GMD) weapon system has demonstrated the capability to defend the United States Homeland from a small number of ballistic missile threats with ranges greater than 3,000 kilometers and employing simple countermeasures, when supported by the full architecture of Missile Defense System (MDS) sensors. Similarly, the Regional/Theater MDS has demonstrated the capability to defend the U.S. Indo-Pacific Command (USINDOPACOM), U.S. European Command (USEUCOM), and U.S. Central Command (USCENTCOM) areas of responsibility from a small number of medium- or intermediate-range ballistic missile threats with ranges less than 4,000 kilometers, and from representative raids against short-range ballistic missile (SRBM) threats. DOT&E assesses that the top five challenges for the MDS are: 1) the need for realistic and emerging threat representations in flight and ground testing; 2) the need for accredited modeling and simulation (M&S) to assess MDS effectiveness; 3) susceptibility of the MDS to cyberattack; 4) system reliability and sustainment; and 5) interoperability and maturation of engagement coordination.

In FY22, the Missile Defense Agency (MDA) tested three significant new MDS capabilities:

- Terminal High Altitude Area Defense (THAAD) integration with Patriot Missile Segment Enhancement (MSE) interceptors and launchers, designed to improve THAAD self-defense without requiring a dedicated Patriot battery.
- Initial Long Range Discrimination Radar (LRDR) performance in support of U.S. Homeland Defense.
- An Aegis Ballistic Missile Defense (BMD) capability to detect, track, and report on resident space objects based on Space Domain Awareness (SDA) when tasked by Command and Control, Battle Management, and Communications (C2BMC).

DOT&E will provide additional information and recommendations in the classified DOT&E FY22 Assessment of the MDS report to be published in February 2023.

SYSTEM DESCRIPTION

The MDA's MDS is a geographically distributed system of systems that relies on element interoperability and warfighter integration for combat capability and efficient use of guided missile/interceptor inventory. As shown in Table 1, the MDS consists of six weapon systems, a sensor architecture (i.e., terrestrial, maritime, and global sensors), and a command and control element.

MISSION

The Commanders of U.S. Northern Command (USNORTHCOM), USINDOPACOM, USEUCOM, and USCENTCOM employ the assets of the BMDS to defend the United States, deployed forces, and allies against ballistic missile threats at all ranges.

Table 1. Elements of MDA's Missile Defense System

Type	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. MDA is developing a Next Generation Interceptor to supplement the current GBI fleet.	**Aegis BMD[a]:** Both sea- and land-based variants defend U.S. deployed forces and allies from SRBM, MRBM, and IRBM threats. Aegis BMD uses the SM-3 family of guided missiles against exoatmospheric ballistic missile threats alongside SM-6 guided missiles that Aegis SBT (Inc 2) uses for endo-atmospheric engagements. **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 from Aegis BMD or other sensors via C2BMC. THAAD complements the upper-tier Aegis BMD and the lower-tier PAC-3 weapon systems. **PAC-3[b]:** Defends U.S. deployed forces and critical assets from SRBM 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.	**Aegis SBT (Inc 3)[a]:** Aegis SBT provides critical asset protection at sea and for joint forces ashore against ballistic, maneuverable, and hypersonic glide threats in the terminal phase. **GPI[a]:** Provides an additional layer of Hypersonic Defense augmenting Aegis SBT (Inc 3) to increase depth of fire against hypersonic threats. The program is currently in development of prototype interceptors.
Terrestrial and Maritime Sensors	**Cobra Dane Upgrade[d]:** L band fixed site phased array radar. **UEWRs[d]:** Ultrahigh frequency fixed site phased array radars. **SBX[a]:** X-band mobile phased array radar located aboard a self-propelled, ocean-going platform. **LRDR[a]:** 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]:** Being developed for installation on new construction Aegis DDG 51 Flight III destroyers, this S-band four-face radar will extend Aegis threat detection ranges and provide simultaneous ballistic missile and air defense support. **AN/TPY-2 FBM Radar[a]:** X-band single-face transportable phased array radar. **LTAMDS[b]:** C-band three-face multi-function, multi-mission radar interfacing with IBCS and supporting interoperability with PAC-3.	Leverages Homeland Defense, Regional/Theater Defense, and Global sensors.
Global Sensors	**SBIRS[d]:** Satellite constellation of infrared sensors. **BOA[a]:** Element that combines OPIR observations to provide missile event and track reports to C2BMC. **SKA[a]:** Network of space sensors providing interceptor hit assessments. **HBTSS[a]:** Network of space sensors to detect and track both ballistic and hypersonic threats, and provide fire-control quality data to MDS sensors and weapon systems.		
Command and Control	**C2BMC[a]:** Integrating element within the MDS providing deliberate and dynamic planning, situational awareness, sensor track management, engagement support and monitoring, data exchange between elements, and network management. C2BMC also directs sensor tasking for the AN/TPY-2 FBM radars and BOA systems.		

Notes:
[a] Under MDA development/sustainment. [b] Under Army development/sustainment. [c] Under Navy development/sustainment. [d] Under Space Force development/sustainment.

Acronyms: BMD – Ballistic Missile Defense; BMDS – Ballistic Missile Defense System; BOA – BMDS Overhead Persistent Infrared Architecture; C2BMC – Command and Control, Battle Management, and Communications; FBM – Forward-Based Mode; GMD – Ground-based Midcourse Defense; GBI – Ground Based Interceptors; GPI – Glide Phase Interceptor; HBTSS – Hypersonic and Ballistic Tracking Space Sensor; IAMD – Integrated Air and Missile Defense; IBCS – IAMD Battle Command System; ICBM – Intercontinental Ballistic Missile; Inc – Increment; IRBM – Intermediate-Range Ballistic Missile; LRDR – Long Range Discrimination Radar; LTAMDS – Lower Tier Air and Missile Defense Sensor; MDA – Missile Defense Agency; MDS – Missile Defense System (formerly BMDS); MRBM – Medium-Range Ballistic Missile; OPIR – Overhead Persistent Infrared; PAC – Patriot Advanced Capability; SBIRS – Space-Based Infrared System; SBT – Sea-Based Terminal; SBX – Sea-Based X-band; SKA – Space-Based Kill Assessment; SM – Standard Missile; SRBM – Short-Range Ballistic Missile; THAAD – Terminal High Altitude Area Defense; UEWR – Upgraded Early Warning Radar

PROGRAM

The MDS is a single Acquisition Category (ACAT) ID program that encompasses five of its six weapon systems, most of its sensor architecture, and its command and control element. In 2002, the Secretary of Defense granted the MDA special acquisition authorities for the MDS, which allowed it to use tailored processes and milestones to deploy new capability as soon as technologically possible to defend the United States and its allies against limited ballistic missile attack. The MDA manages the MDS through a series of six program baselines – Schedule, Test, Technical, Resource, Contract, and Operational Capability and maintains responsibility for integrating all elements into the MDS whether or not the MDA developed the element. The MDA publishes the Test Baseline twice a year in an Integrated Master Test Plan (IMTP) that corresponds to the MDA Program Objective Memorandum submission to the Department and the President's Budget release to Congress. DOT&E approves each version of the IMTP, the latest of which was dated March 2022 (version 23.1).

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 Test and Evaluation Master Plan (TEMP) in FY20. LTAMDS is a Middle Tier of Acquisition program, for rapid prototyping, and is expected to be designated as an ACAT IC program at its Materiel Development Decision scheduled for December 2023. DOT&E approved its initial TEMP in 2019. A Test and Evaluation Strategy is under development to replace the TEMP, with DOT&E approval expected in FY23.

The Navy manages the AN/SPY-6(V)1 radar program, an ACAT IC program. DOT&E approved its TEMP in September 2022.

The Space Force operates and sustains three sensor types integrated into the MDS: Cobra Dane Upgrade, five Upgraded Early Warning Radars (UEWRs), LRDR, and the Space-Based Infrared System (SBIRS) constellation. The Air Force completed development and initial operational testing for these sensors prior to them becoming Space Force assets.

» MAJOR CONTRACTORS

- The Boeing Company
  - GMD Integration: Huntsville, Alabama
- Lockheed Martin Corporation
  - Aegis BMD, AAMDS, Aegis SBT, AN/SPY-1 radar, LRDR, and GPI: Moorestown, New Jersey
  - C2BMC: Huntsville, Alabama, and Colorado Springs, Colorado
  - NGI AUR through Critical Design Review: Huntsville, Alabama
  - SBIRS: Sunnyvale, California
  - THAAD Weapon System, PAC-3 Command and Launch System, and PAC-3 interceptor variants: Dallas, Texas
  - THAAD Interceptors: Troy, Alabama
- Northrop Grumman Corporation
  - GMD Weapon Systems Development; Chandler, Arizona
  - GBI Booster Vehicles: Chandler, Arizona
  - GCN, LMS, and GFC: Huntsville, Alabama
  - NGI AUR and GPI through Critical Design Review: Chandler, Arizona
  - BOA: Boulder, Colorado; Colorado Springs, Colorado; and Azusa, California
  - HBTSS through Prototype Demonstration Phase: Redondo Beach, California, and Azusa, California
- Raytheon Technologies Corporation
  - GMD EKV, SM-3/6 Interceptors, LTAMDS, and GPI: Tucson, Arizona
  - Patriot Ground System and PAC-2 interceptor variants, AN/SPY-6(V)1 radar, AN/TPY-2 radar, SBX radar, and UEWRs: Tewksbury, Massachusetts
  - Cobra Dane Radar: Dulles, Virginia
- L3 Harris Technologies
  - GMD IDT: Melbourne, Florida

- HBTSS through Prototype Demonstration Phase: Fort Wayne, Indiana
- Johns Hopkins University, Applied Physics Laboratory
  - SKA: Laurel, Maryland

TEST ADEQUACY

The MDA IMTP focuses on collecting the flight, ground, and cybersecurity test data needed for contract compliance and operational capability declarations, as well as for the verification, validation, and accreditation of associated M&S. The MDA conducted testing in accordance with the DOT&E-approved IMTP although there were technical and programmatic delays to some events. Table 2 outlines the 24 flight, ground, high-fidelity M&S, and cybersecurity test events that the MDA performed or participated in during FY22. Testing was conducted in accordance with a DOT&E approved the test plan and DOT&E observed the testing as shown in Table 2 below.

Table 2. FY22 Body of Testing

Date	Test	Mission Area	Description
October 2021	At Sea Demonstration-2[b,c]	Regional/Theater Defense	The MDA conducted an Aegis AN/SPY 1 radar SDA mission providing sensor tracking of resident space objects. This test informed radar performance and C2BMC/Space C2 interfaces for mission tasking.
October 2021	Flight Test Other-43[b,d]	Regional/Theater Defense	The MDA conducted a developmental test of the MDS to assess its ability to detect, track, and report on an advanced vehicle.
October 2021	THAAD 4.0 CVPA-08a[a,c]	Regional/Theater Defense	The MDA, MDS OTA, and the Army's DEVCOM conducted a CVPA to characterize cybersecurity elements of THAAD and unit operators, and provide reconnaissance in support of the adversarial assessment.
November 2021	Patriot PDB 8.1 DT-1a[b,d]	Regional/Theater Defense	The Army demonstrated the capability of the Patriot PDB-8.1 system to detect, track, engage, intercept, and kill a low radar cross section cruise missile target at low altitude with a GEM-T Ballistic Missile interceptor.
December 2021	THAAD 4.0 AA-08a[a,c]	Regional/Theater Defense	The MDA, MDS OTA, and the Army's TSMO conducted an AA to determine an adversary's ability to achieve mission effects and assess THAAD's operational resilience to insider, nearsider, and outsider cyber threats.
February 2022	THAAD Controlled Test Vehicle-01a[b,c]	Regional/Theater Defense	The MDA conducted this non-intercept flight test to demonstrate the capability of THAAD to fire and direct a PAC-3 MSE interceptor against a simulated SRBM target. The successful outcome of the test verified that THAAD could compute a firing solution, communicate with the M903 launcher, and control the MSE interceptor in flight to the target.
March 2022	Flight Test THAAD Weapon System-21[b,c]	Regional/Theater Defense	The MDA and the MDS OTA conducted this test to support the THAAD/PAC-3 MSE integration capability. The AN/TPY-2 Terminal Mode radar tracked the SRBM target. Per the test design, there were no THAAD interceptors available, thus ensuring an MSE engagement. A salvo of 2 MSE interceptors were launched using THAAD fire control data and successfully intercepted the target.

Table 2. FY22 Body of Testing

Date	Test	Mission Area	Description
April 2022	Flight Test Experiment Aegis Weapon System-01[b,c]	Regional/Theater Defense	The MDA conducted a developmental test of Aegis BMD, firing a Standard Missile-3 Block IIA guided missile against an MRBM target. Operational assets included overhead sensors, BOA, C2BMC, and the Enterprise Sensor Processing Network at Buckley Space Force Base, Colorado.
March 2022	Hypersonic Air-breathing Weapon Concept-7[b,d]	Hypersonic Defense	The MDA participated in this DARPA event to collect hypersonic missile phenomenology and tracking data to inform future capability development.
April 2022	Ground Test Integrated-08a (USNORTHCOM/ USINDOPACOM)[b,c]	Homeland Defense and Regional/Theater Defense	The MDA and the MDS OTA conducted this developmental/operational HWIL laboratory test to support assessment of MDS capabilities in the USNORTHCOM/USINDOPACOM geographic regions, examining new functions of LRDR, C2BMC, GMD, SBX, BOA, Aegis BMD, and AN/TPY-2 FBM.
May to July 2022	SM-3 Block IIA M&S Runs for Record, Phase 1C[a,c]	Regional/Theater Defense	The MDA executed and delivered a set of high-fidelity M&S runs to assess Aegis BMD performance against raids of threats in scenarios relevant to European Phased Adaptive Approach Phase 3.
June 2022	C2BMC/BOA Cyber Event[b,c]	Homeland Defense	The MDA, MDS OTA, and the Army's DEVCOM performed a DT cyber event on the C2BMC and BOA using a HWIL laboratory representation to assess insider and nearsider threat postures.
June 2022	UEWR CVPA[b,c]	Homeland Defense	The Space Force performed a CVPA on the UEWR at Beale AFB that explored insider and nearsider threat postures.
June 2022	LRDR Cyber Event[b,c]	Homeland Defense	The MDA, MDS OTA, and the Army's DEVCOM performed a DT cyber event on LRDR using a HWIL laboratory representation to assess insider and nearsider threat postures.
June 2022	Joint Flight Campaign-1[b,d]	Hypersonic Defense	The MDA participated in this Army/Navy event to collect hypersonic missile phenomenology and tracking data to inform future capability development. However, an anomaly occurred during the flight, and data collection was sub-optimal.
July 2022	HAWC-9[b,d]	Hypersonic Defense	The MDA participated in this DARPA event to collect hypersonic missile phenomenology and tracking data to inform future capability development. HAWC-9 provided a unique opportunity to support MDA's need for realistic and emerging threat representations in flight and ground tests.
June 2022 to August 2023	Patriot PDB-8.1 Limited User Test[a,c]	Regional/Theater Defense	During this operational test, the Army is assessing the effectiveness, suitability, and survivability of the Patriot PDB-8.1 system through flight tests, accredited HWIL scenarios, interoperability testing in an MDA ground test, and cybersecurity testing (a CVPA and an AA).
July 2022	Ground Test Integrated-09 Sprint 1[b,d]	Regional/Theater Defense	The MDA conducted this developmental HWIL laboratory test to support assessment of MDS capabilities in the USEUCOM/USCENTCOM geographic regions, examining new functions of C2BMC, BOA, Aegis BMD, THAAD, and AN/TPY-2 FBM.

Table 2. FY22 Body of Testing

Date	Test	Mission Area	Description
July 2022	Air Force National Nuclear Security Agency Demonstrator Initiative[b,d]	Homeland Defense	The MDA participated in this NNSA event as a target of opportunity to exercise sensors, communication links, and emerging technologies to help assess the system-level capabilities and performance of the integrated MDS.
August 2022	Glory Trip-243[b,d]	Homeland Defense	The MDA participated in this Air Force Global Strike Command event to collect data, exercise MDS communication links, perform future capability assessments, and provide confidence to participating MDS elements and component.
August 2022	Pacific Dragon-22[b,c]	Regional/Theater Defense	The MDA participated in this multilateral warfighter exercise. During three events, U.S. and allied naval vessels conducted a live intercept of a ballistic missile target with an SM-3 Block IA, simulated engagements against ballistic missile targets, and tracked two ballistic targets simultaneously. The test supported the 2017 and 2019 NDAA requirement for international interoperability.
August 2022	Patriot PDB 8.1 DT-1b,c[b,d]	Regional/Theater Defense	The Army demonstrated the capability of the Patriot PDB-8.1 system to detect, track, engage, intercept, and kill a subscale aircraft target employing electronic attack with a GEM-T interceptor.
September 2022	Glory Trip-244[b,d]	Homeland Defense	The MDA participated in this Air Force Global Strike Command event to collect data, exercise MDS communication links, perform future capability assessments, and provide confidence to participating MDS elements and component.

Notes:
[a] Testing performed per DOT&E approved test plan. [b] Test plan not required by DOT&E. [c] Test observed by DOT&E. [d] Test not observed by DOT&E

Acronyms: AA – Adversarial Assessment; 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; CVPA – Cooperative Vulnerability and Penetration Assessment; DARPA – Defense Advanced Research Project Agency; DEVCOM – U.S. Army Combat Capabilities Development Command; DT – Developmental Testing; FBM – Forward-Based Mode; FY – Fiscal Year; GEM-T – Guidance Enhanced Missile – Tactical; GMD – Ground-based Midcourse Defense; HAWC – Hypersonic Air-breathing Weapon Concept; HWIL – Hardware-in-the-Loop; 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; NATO – North Atlantic Treaty Organization; NDAA – National Defense Authorization Act; NNSA – National Nuclear Security Agency; OTA – Operational Test Agency; PAC – Patriot Advanced Capability; PDB – Post Deployment Build; SBT – Sea-Based Terminal; SBX – Sea-Based X-Band; SDA – Space Domain Awareness; SM – Standard Missile; SRBM – Short-Range Ballistic Missile; THAAD – Terminal High Altitude Area Defense; TSMO – Threat Systems Management Office; UEWR – Upgraded Early Warning Radar; USCENTCOM – U.S. Central Command; USEUCOM – U.S. European Command; USINDOPACOM – U.S. Indo-Pacific Command; USNORTHCOM – U.S. Northern Command; VV&A – Verification, Validation, and Accreditation

The need for additional threat representations, independently accredited M&S, and system survivability data in a cyber-contested environment present significant challenges for DOT&E in completing a comprehensive assessment of the MDS. Specifically:

- Realistic and up-to-date representations of threat scenes are critical to the assessment of MDS performance. The rate of adversary threat development is currently faster than the pace of flight test target and ground test as well as high-fidelity M&S threat model development.

- The MDA and the MDS Operational Test Agency (OTA) continued to make progress in FY22 by increasing the number of OTA-accredited models and mitigating model limitations, but gaps remain. The MDA and MDS OTA are also now considering how to accredit the new MDS-level digital modeling architecture, the Enterprise Digital Integrated System Simulation, which presents a different set of challenges.
- The MDS is a large system of systems with an extensive cyberattack surface. Although the MDA and the MDS OTA made progress in cybersecurity T&E efforts, more realistic testing in accredited hardware-in-the-loop environments is needed, along with greater test planning collaboration with DOT&E. Frequent cyber Red Team events, emulating advanced adversaries, is needed to ensure MDS cyber defenses are adequate to protect MDS missions. Persistent Cyber Operations is the best way to emulate advanced cyber threats and find and fix mission-critical vulnerabilities.

Flight and ground test programs have been limited in the variety of realistic threat countermeasures, electronic attack, post-intercept debris scenes, raid sizes, and multi-element engagement scenarios tested. The MDA often designs flight tests to demonstrate a specific new capability, but relevant intercept flight tests could provide needed referent data to support verification, validation, and accreditation models used in high-fidelity M&S ground testing, provide realistic data on multi-element interactions, and provide data in multi-domain operations. Furthermore, M&S limitations in ground tests are sometimes minor when assessing an element alone, but combine to create substantial impediments at the MDS-level.

The MDA is currently developing a concept for a persistent, 360-degree, layered integrated air and missile defense capability for the defense of Guam. This concept involves interoperability and coordination between multiple assets defending against cruise, ballistic, and hypersonic threats. The proposed architecture is made of both new and existing components in close proximity and with overlapping areas of regard. This presents a significant test planning challenge. DOT&E currently assesses that the proposed test strategy needs further development to be adequate. An agile test program that fully explores interoperability and engagement planning through ground testing, tracking exercises, and intercept flight testing is warranted.

PERFORMANCE

» BALLISTIC MISSILE DEFENSE FOR THE HOMELAND

With the support of the full architecture of MDS sensors, the GMD weapon system has demonstrated the capability to defend the U.S. Homeland from a small number of ballistic missile threats employing simple countermeasures and with ranges greater than 3,000 kilometers.

» BALLISTIC MISSILE DEFENSE FOR THE REGIONAL/THEATER

The Regional/Theater MDS has demonstrated a capability to defend the USINDOPACOM, USEUCOM, and USCENTCOM areas of responsibility from a small number of medium- or intermediate-range ballistic missile threats with ranges less than 4,000 kilometers, and from representative raids against SRBM threats.

Aegis BMD has demonstrated that it can intercept non-separating, simple-separating, and complex-separating ballistic missiles in the midcourse phase of flight with Standard Missile-3 (SM-3) guided missiles, although flight testing and M&S have not addressed all expected threat types, ground ranges, and raid sizes. Aegis BMD has also demonstrated a capability to intercept select ballistic missiles in the terminal phase of flight with SM-6 guided missiles. However, corrective actions are needed to address failure review board findings from the two Sea-Based Terminal Increment 2 flight tests in FY21. All fielded Aegis BMD variants have demonstrated sufficient reliability, with operational availabilities that exceed the specification. However, SM-3 Block IIA missile reliability is not known with a high degree of certainty, due to the relatively small number of live firings and ground test data collection events to date. The MDA is implementing a process to monitor the health and status of deployed SM-3 Block IIA missiles, which will provide additional reliability data for future assessments.

THAAD has proven capability to intercept and destroy, by ballistic missiles of varying types (short- to intermediate-range) inside or outside the earth's atmosphere during the terminal phase of flight, although the test program still needs to address more complex engagement conditions and more realistic raid scenarios. In FY22, MDA demonstrated THAAD launch and control of MSE interceptors. This new function expands options for theater defense, though more testing of full THAAD/Patriot integration is needed to assess overall MDS capability. The United Arab Emirates THAAD weapon system successfully intercepted ballistic missiles operationally for the first time in FY22. The MDA and 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 has long-standing shortfalls in reliability, training, and survivability. The ongoing Patriot PDB-8.1 Limited User Test will assess how Patriot effectiveness, suitability, and survivability have changed since the last Patriot operational test in 2016 – 2019. The Patriot M&S representations for ground tests used the new Battalion Simulation in development by the Army, but the Army has not yet provided sufficient verification and validation evidence to accredit Battalion Simulation for performance assessments.

AN/SPY-1 and AN/TPY-2 Forward-Based Mode (FBM) radars contribute to regional/theater defense and monitoring. In the future, AN/SPY-6(V)1 will also contribute to those missions. In FY22, Aegis BMD, with AN/SPY-1, demonstrated the capability to detect, track, and report on resident space objects based on SDA tasking received by C2BMC during an at-sea demonstration. The AN/SPY-6(V)1 radar prototype at the Pacific Missile Range Facility continues to track all classes of ballistic missiles, as available, during MDS flight tests. In FY22, MDA and the Army completed processor upgrades in all deployed AN/TPY-2 FBM radar electronic equipment units.

» HYPERSONIC MISSILE DEFENSE

The MDA collected data throughout FY22 to inform future sensors, sensor detection and tracking algorithms, and M&S validation. The MDA also conducted ground impact and wind-tunnel testing to support the development of the M&S architecture specifically for hypersonic missile defense.

» COMMAND AND CONTROL AND SPACE SENSORS

Almost every FY22 test conducted by the MDA included space sensors, as well as sensors unique to Homeland and Regional/Theater Defense to acquire, track, and report on observed objects. C2BMC globally and regionally integrates and synchronizes autonomous sensors, weapon systems, and operations. C2BMC is a part of all system ground and flight tests, which verify and exercise current and future MDS capabilities. C2BMC and BOA also supported real-world situational awareness in USEUCOM in FY22, and the MDA added an additional C2BMC management node to the MDS this year to improve resiliency. The C2BMC tasked an Aegis BMD with a SDA tasking and Aegis BMD detected and tracked a resident space object and reported back to C2BMC.

RECOMMENDATIONS

The MDA should:

1. Increase the rate of target and threat model development to keep pace with emerging real-world threats.
2. Continue to prioritize independent accreditation of M&S used in ground tests and ensure M&S can adequately represent current threat missile capabilities, electronic attack, countermeasures, debris, and realistic raid sizes.
3. Ensure that relevant intercept flight testing is conducted prior to any planned high-fidelity M&S operational testing runs for record to support verification, validation, and accreditation of the models.

4. Ensure comprehensive cyber test and evaluation plans are created and included in the IMTP, and developmental and operational cyber testing is completed prior to capability delivery to the warfighter.
5. Work with DOT&E and Combatant Commands to conduct Persistent Cyber Operations – Red Teams emulating advance adversaries – across MDS systems and networks.
6. Ensure the test strategy for the defense of Guam incorporates multi-element interoperability and coordination into intercept flight testing.

The Army should:

1. Continue to develop the Patriot Battalion Simulation to address current shortfalls in supporting performance assessments.

DOT&E-MANAGED ACTIVITIES

Center for Countermeasures (CCM)

The Center for Countermeasures (CCM) accomplishes its mission by operating and deploying specialized mobile test instrumentation capable of simulating an array of threats to measure and evaluate operational effectiveness of countermeasures (CMs) employed by U.S. DOD and foreign weapon systems. The portability of CCM test tools and personnel provide the necessary test agility and efficiency for the DOD to develop and field warfighting capabilities at operationally relevant speeds, minimizing the logistical burden requirements of the Program Office, and preserving schedules and resources. In FY22, CCM executed 42 test events in support of the following: 1) successful development of instrumentation for characterizing directed energy weapons (DEWs) operational performance; 2) delivery of missile plume simulators to test Aircraft Survivability Equipment (ASE), including fixed- and rotary-wing platforms; 3) high-threat environments for pre-deployment training; 4) Counter-Unmanned Aerial Systems (C-UASs) programs; and 5) project arrangements with allies to advance CM testing and evaluation. Overall, CCM expedited the development and fielding of CM systems; enabled credible T&E of directed energy (DE)-based CMs, C-UASs, and survivability equipment; provided a threat environment for pre-deployment training; and leveraged partnerships with allies to advance T&E of infrared (IR)- and radio frequency (RF)-based CMs (IRCMs and RFCMs).

CCM Expedites the Development and Fielding of CM Systems

In FY22, CCM continued to upgrade the following test infrastructure and capabilities to keep pace with adversary advances, data management demands, as well as expedited testing, development, and fielding of CMs needed to dominate and survive in an increasingly complex, multi-domain environment:

- **The Joint Mobile IRCM Test System (JMITS) and Multi-Spectral Sea and Land Target Simulators** – five dual-band IR and ultraviolet simulators capable of replicating threat missile plumes. Upgrades to the missile simulator emitters include improved bandwidth and processing capabilities to adequately represent threats and evaluate advanced missile warning sensors (MWSs) and directed IR countermeasures (DIRCMs). Upgrades to the simulators will be completed by 4QFY23.
- **The Towed Airborne Plume Simulator (TAPS)** – an airborne-towed body missile plume simulator that replicates the IR temporal characteristics of a threat missile approaching an aircraft. TAPS can also approximate the spectral and spatial behavior of threat missiles, simulating the movement of a threat in different backgrounds to more adequately evaluate aircraft MWSs. A Quick Reaction Test Capability, termed TAPS-Helicopter, will expand the TAPS test capabilities for rotary-wing aircraft. Flight validation testing will be completed in 2QFY23.
- **The Joint Standard Instrumentation Suite (JSIS)** – a suite of instrumentation used to collect missile plume/hostile fire threat signatures and Time-Space-Position Information data during threat live fire events. This data collection and management of threat signatures will further develop the Missile Space and Intelligence Center's threat models to support MWS and CM development and evaluation. The JSIS baseline was developed from FY13 – FY18. JSIS Full Operational Capability will provide all remaining JSIS equipment requirements, including radiometers, spectrometers, and tracked imagery by 3QFY23.
- **The High-Power Portable Range Threat Simulator** – a ruggedized, deployable, ground-based, open-loop RF threat radar simulator designed to provide open-space emulation of threat radar signals and full threat modulations. The upgrade, completed in 2QFY22, replaced a legacy signal generator and increased CCM's capabilities with new, higher-fidelity threat radar signals.
- **The JMITS Seeker Instrumentation Suite** – a suite capable of operating up to four IR Man-Portable Air Defense System (MANPADS) seekers to provide real-time data collection of actual seeker signals required to determine effectiveness trends of current CM expendable flares and/or DIRCM laser jammers. The JMITS Seeker Instrumentation Suite simulates a missile engagement and collects seeker responses to provide end-to-end ASE testing. Upgrades will be completed in 2QFY23.
- **The High Energy Laser (HEL) Remote Target Scoring (HRTS) System** – an integrated optical and sensor suite that will provide radiometric and multi-spectral imaging of targets, starting at the systems acquisition and including HEL engagement up to target flight path termination. HRTS enables the tracking and scoring of a variety of targets during HEL engagements, including light boats, rocket-artillery-mortars, unmanned aircraft systems, and subsonic/supersonic cruise missiles. HRTS will be available by 2QFY23.
- **DOD Space T&E Instrumentation Initiatives** – investments in space capabilities increase the effectiveness of operations in every other domain. To ensure the United States continues building an enduring advantage, the DOD must accelerate the delivery of space systems and ensure they are adequately tested and have the appropriate infrastructure and resources needed to assess effectiveness. In collaboration with the Test and Evaluation Threat Resources Activity (TETRA), CCM is participating in DOT&E's Space Electronic Warfare (EW) and Cyber Working Group (WG). The objectives are to identify gaps in space EW T&E capabilities and actions/investments required to fill those gaps. This WG will undergo a yearlong effort and will provide the DOD findings and recommendations in 4QFY23. CCM is supporting this initiative by collecting data, conducting the gap analysis, and working with TETRA to report the results.

CCM Enables Credible T&E of DE-based CMs

DEW capabilities that could be integrated with kinetic fires to counter more advanced adversaries have continued to emerge. In FY22, CCM continued to build its portfolio of DE-based projects to fulfill T&E instrumentation capability gaps in developing and implementing credible tools to support High Power Microwave (HPM) and HEL testing. Specifically, CCM supports projects that include airborne free-flying and tethered Unmanned Aerial System (UAS) with HEL target boards, HPM diagnostic instrumentation, dynamic HEL beam characterization equipment, and UAS detect and track radar systems.

In FY22, CCM executed the following test series supporting the rapid capabilities development and fielding of prototype DEWs and has made significant progress in equipping the DOD with tools and methods needed to adequately test and evaluate the operational effectiveness of DEWs and DE-based CMs:

- Army DE Maneuver Short Range Air Defense Developmental T&E (DT&E) with CCM-developed, multi-spectral tracking and scoring imagers.
- Air Force DE prototype DT&E programs by collecting and evaluating beam diagnostics and system analysis to include beam characterization and system performance.
- Experimentation integration and developmental testing to evaluate the probability of weapon effectiveness and measure HEL lethality against dynamic targets.
- Electromagnetic environmental effects assessments of ground combat vehicles against HPM simulators.
- Development and acceptance testing of the following joint DE T&E tools and instrumentation under the Mobile HEL Measurement system and DE Instrumentation Initiative portfolios led by the Test Resource Management Center:
    - Target boards for directly measuring HEL performance (stationary or mounted on an inflight, operationally representative cruise missile and UAS).
    - Range safety tools for measuring nominal ocular hazard distances for use in HEL test preparation.
    - Diagnostic suites for imaging, characterizing, and measuring HEL and atmospheric effects as they are propagated in an open-air environment.
    - Diagnostic suites for measuring HPM fields using an ad-hoc network of sensor nodes enabling a flexible and mobile measurement system for remote locations and moving targets.
    - 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.

CCM Enables Credible T&E of C-UAS

Because of the rapid technological advancements and growth of UAS threats, CCM supported operational performance assessments of a select set of C-UAS as installed, integrated, and employed in an operationally representative environment. In FY22, CCM provided certified UAS operators for the following six test events to evaluate and improve C-UAS systems for the protection of U.S. forces, facilities, and assets:

- Three tests that evaluated the capabilities of C-UAS to detect, classify, identify, track, and defeat Group 1 and 2 UAS threats.
- One test to evaluate next generation passive, medium-range UAS detection systems with man-out-of-the-loop operations.
- One test to demonstrate the capabilities of system architecture (i.e., a radar, a fire distribution center, and a HEL weapons system) to detect, track, and destroy small UAS threats.
- One test to evaluate the ability of a layered laser defense system to engage and destroy rockets, mortars, and UAS threats at close ranges.

CCM Enables Credible T&E of Survivability Equipment

In FY22, CCM used unique capabilities to generate more than 20,000 threat missile plume signatures and executed 17 tests (1 ground system test and 16 ASE test events) supporting the expedited development and fielding of several Quick Reaction Capability and Joint Urgent Operational Needs Statement CM programs, as well as hardware and software upgrades of fielded systems against IR-guided, RF-guided, and/or laser threats. Testing included the following:

- HH-60W IOT&E that evaluated the aircraft and an HH-60W-equipped unit's ability to conduct operational missions in a realistic environment. Aircrews utilized appropriate tactics, techniques, and procedures (TTPs) and CMs during different flight modes and sorties to assess the HH-60W's operational effectiveness, suitability, and survivability while also addressing crewmember and maintainer feedback from the missions.
- Initial integration verification flight test of Advanced Threat Warner Missile Warning System as installed on the CH-53K.
- Common Missile Warning System (CMWS) and Common IRCMs operational test to support a fielding decision intended to increase the survivability for rotary-wing aircraft.
- Limited Interim MWS quick reaction capability test to support a fielding decision intended to increase survivability for rotary-wing aircraft.
- Army and Navy Distributed Aperture IRCM operational test to determine system effectiveness and improve survivability for small rotary-wing aircraft.
- Large Aircraft IRCM (LAIRCM) Next Generation integration test to support Air Force efforts to improve survivability of fixed-wing aircraft.
- Advanced Threat Warner software upgrade testing to support Navy efforts to improve survivability for fixed- and rotary-wing aircraft.
- LAIRCM system upgrade performance testing to support Air Force Life Cycle Management Center efforts to improve survivability for C-130J transport aircraft.
- Integration verification flight test of LAIRCM as installed on the Allied Head of State aircraft.
- Testing of the Radar Warning Receiver (AN/APR-39C[V]1), as installed on the UH-60V, to provide a realistic, RF threat environment for basic identification, threat reaction, and counter-maneuver training/testing and provide data to the trainers to assist with the development and refinement of their TTPs.
- Layered Soft-Kill System, as installed on the M2 Bradley vehicle, to evaluate the integrated Modular Active Protection System Framework Layered Soft-Kill System's performance to defeat current and emerging anti-tank guided missile threats and deliver multiple coordinated survivability and awareness capabilities that include shot detection, laser warning, and soft-kill of moving anti-tank guided missiles.

CCM Provides Threat Environments for Pre-Deployment Training

In FY22, CCM provided its unique assets — such as a missile plume simulator, an instrumented MANPADS surrogate system, and the Portable Range Threat Simulator — to support the Emerald Warrior test/training exercise. Emerald Warrior was a Joint interoperability large force exercise that was conducted by aircrew planners and staff in a realistic, contested, and near-peer environment. The training included multiple U.S. military Services and Allied forces with the latest IRCM technology. CCM provided data to the trainers to assist in developing and refining their TTPs, thus enhancing their survivability potential in a combat environment.

CCM Leverages Allies' Support to Advance T&E of ASE

In FY22, CCM and TETRA continued to support the execution of the Australia, Canada, Great Britain, and U.S. Airborne EW Cooperative T&E Project Arrangement (Air EW CTE PA) intended to advance coalition EW T&E capabilities, resulting in the following:

- All Air EW CTE PA Project Officers and Steering Committee members from the four nations met to review advances made by the four PA WGs;
  - Modeling and simulation (M&S) and Threat Environment Representation WG
  - T&E Methodology WG
  - Integrated Aircraft Survivability Equipment WG
  - RF Threats & Countermeasure WG

- The Virtual Rider Series Hydra 1 Trial Event, conducted at the Redstone Test Center Aviation Systems Test and Integration Laboratory, Huntsville, Alabama, demonstrated the integrated ASE T&E methodologies using a man-in-the-loop flight simulator. Classified results were shared with the four participating nations.
- WGs advanced the development of M&S evaluation capabilities required for combat aircraft survivability assessment within complex threat environments. This work focused on the four nations' joint development of the system-of-systems architecture design, which allowed the integration of multiple evaluation tools and provided a larger scale (battlespace-wide) synthetic evaluation capability. Specifically, the WGs:
  - Developed plans and requirements for integrated system-of-systems test events for complex airborne EW RF and electro-optical (EO) combined scene generation. Canada hosted a trial in Ottawa, with participation by the four nations, to further develop EO digital modeling tools and integration into airborne EW battlespace-wide simulation environments.
  - Developed a high-speed classified network, which provided the ability to share large amounts of classified data among the four nations.
  - Conducted a series of trials (executed by the United Kingdom in 1QFY22 with remote participation by the other three nations) to support the development of two new airborne EW T&E M&S capabilities. These trials successfully combined EO and RF synthetic tests at a high level of fidelity.
  - Conducted of a series of tests (executed by Canada throughout FY22 with remote participation by the other three nations) to demonstrate an improved level of EO/IR and RF fidelity in airborne EW system-of-systems M&S.
  - Held the annual test (executed by the United States in 1QFY22 with remote participation by the other three nations) focusing on the requirements, capabilities, and tools needed for RFCM technique evaluation at the system-of-systems level.

Cyber Assessment Program (CAP)

The 49 cyber assessments conducted in FY22 demonstrated that the limited Zero Trust principles and practices emerging within the Department, when executed by well-trained cyber defenders, will help protect critical DOD missions. Radio frequency and other unconventional cyber threats pose new and serious challenges, and the DOD's abilities to assess against Red Teams portraying nation-state adversaries remain limited due to persistent resource and personnel shortfalls.

Summary of Cyber Assessment Program FY22 Assessments

Cyber Assessment Program (CAP) observations show that even partial implementation of Zero Trust principles by Combatant Commands and Services, if supported by well-trained, experienced cyber defenders, could improve their capability to fight through cyberattacks and accomplish critical missions. The Zero Trust concept assumes the DOD's networks have been breached by adversaries, an assumption borne out by years of DOT&E cyber assessments. Instead of trusting perimeter defenses around a network, which are readily evaded by advanced cyber actors and DOD cyber-Red Teams, Zero Trust relies on strict controls on data access and encryption to secure information.

During FY22, the DOD CIO focused on developing a Zero Trust Strategy and Framework and building a Zero Trust portfolio management office; these are appropriate first steps, but effective implementation of Zero Trust for DOD critical missions will require initial investments, a significant culture shift across the DOD, and a sustained focus of resources. Congressional support for Zero Trust, reflected in Section 1528 of the FY22 National Defense Authorization Act (NDAA), has helped drive this change.

A critical element of Zero Trust is well-trained and equipped cyber defenders supporting defense of critical DOD missions. There is no cyber defense without cyber defenders, however many critical DOD missions lack the support of capable cyber defenders, which include dedicated network defenders as well as weapon system operators and mission commanders trained to respond to cyberattacks. In conflict with an advanced adversary, DOD missions are not likely to succeed without effective cyber defenses, operators, and leaders who are familiar with indications of attacks and the response actions they must be prepared to execute in a timely manner. Implementation of Zero Trust will require significant new technologies to support cyber defenders, such as cyberattack warning systems for operators of weapon systems, methods to routinely tag critical mission data to control who can access that data, and automatic ways to monitor the cyber defense status of mission networks.

As the newest Service, the U.S. Space Force is aware of the threat cyberattacks pose to its missions; missions which are foundational to most DOD combat capabilities. The U.S. Space Force plans to deploy cyber Mission Defense Teams to support all of its missions. As a key component of Zero Trust, the Mission Defense Teams will require sustained support and resources in order to succeed.

The focus of the DOD's current cyber-related strategies and cyber defenses is on protecting data on internet protocol-based networks and systems. While it is essential to improve defenses of these networks and systems, as Zero Trust is designed to do, such defenses are not sufficient to prevent advanced nation-states from threatening critical DOD missions. A significant shortfall in DOD's cyber posture is defense against unconventional cyber threats, such as those posed by radio frequency (RF)-enabled cyberattacks (e.g., disrupting a system's operations using cyber payloads contained in radio emissions), or direct attacks on weapons systems (e.g., the 1553 busses and other control systems that are essential to many DOD aircraft, ships, and vehicles). FY22 CAP events, recent major exercises, as well as a small number of cyber operational tests have revealed major mission disruptions that can be caused by relatively simple RF-enabled cyberattacks. Future DOD cyber strategies, resource allocation, and Research, Development, Test, and Evaluation efforts must all consider such cyber threats.

Another persistent shortfall in the DOD's cyber posture is the lack of adequate cyber test capabilities. Nation-states, notably Russia and China, are devoting significant resources to offensive cyber capabilities directed against the United States. Comparable test capabilities are needed to adequately assess the DOD's ability to withstand cyberattacks by such nations. Previous DOT&E annual reports have noted this problem, and several recent factors have made the problem more acute: 1) the need to assess the capabilities of the Joint Cyber Warfighting Architecture (JCWA), 2) the demand for cyber operators in the Space Force discussed above, and 3) rapid losses of experienced cyber operators to private industry. JCWA is the DOD's effort to develop an advanced, well-integrated set of cyber capabilities spanning the full spectrum of cyber operations. To succeed, JCWA and the Service branches require top level cyber developmental and operational test capabilities. Currently there are not enough skilled cyber operators in the DOD to support these requirements.

While the DOD's requirements for cyber expertise are rapidly growing, the private industry, spurred by coronavirus (COVID-19) pandemic restrictions, is offering increasingly lucrative offers to the best cyber operators in the DOD, including the ability to earn high salaries while working from home. Many of the DOD's cyber operators are taking these offers, further reducing the available pool of cyber talent in the DOD. To reverse this trend and support the DOD with adequate test capabilities will require the DOD to invest in automated test capabilities to relieve the burden from overtaxed cyber operators and test teams. Other helpful changes to current policies would allow for significantly higher pay, more efficient hiring processes, and more flexible work-from-home opportunities for key personnel such as experienced Red Team operators.

Despite improvements facilitated in part by DOT&E's CAP, DOD development of cyber defenses continues to fall behind the growing offensive capabilities of potential adversaries. DOD missions remain at risk of disruption from adversary cyber actions. The most effective way to reduce this risk is for DOD to place increased emphasis on training in contested cyber environments, especially during major exercises. A cyber "fight-through objective" should be established for every major exercise to provide warfighters and cyber defenders the opportunity to experience the full spectrum of cyber threats and effects, and allow them to improve their defenses, detections, and resilience. To highlight the importance of cyber defenders and expose non-experts to key aspects of cyber warfare, the Institute for Defense Analysis, with the support of DOT&E's CAP, piloted a tabletop cyber wargame in FY22. Initial results were promising, and DOT&E plans to include this wargame as part of future Cyber Readiness Campaigns.

The DOD migration of critical missions and classified data to commercial clouds continues to expand, but current contracts with cloud vendors do not allow the DOD to independently assess the security of cloud infrastructure owned by the commercial vendor. Limited access to the proprietary cloud infrastructure prevents the DOD from fully assessing the security of commercial clouds and the DOD missions that they support.

Advances in artificial intelligence (AI) and machine learning are expanding in the commercial sector and are expected to add new warfighter capabilities as well as cybersecurity challenges. Future assessments with the Combatant Commands (CCMDs) will be expanded to help ensure warfighter awareness of cybersecurity considerations in employing new AI-enabled technologies.

DOT&E CAP Overview

DOT&E's CAP is a unique, congressionally-directed effort focused on emulating realistic nation-state cyber threats during major CCMD and Service exercises to assess and help improve the Department's ability to fight through cyberattacks to accomplish critical missions. Despite limitations from both COVID-19 and Russian activities in Ukraine, both of which contributed to canceled and/or scaled-back exercises, DOT&E's FY22 assessments included persistent cyber operations, assessing unconventional cyber threats (e.g., combined cyber and electronic warfare attacks), evaluating emerging cyber technologies and offensive cyber capabilities, and special projects to support key mission areas and initiatives such as nuclear command and control and advanced data analytics. Table 1 provides a comprehensive list of major FY22 assessment activities.

As part of the CAP, DOT&E employed Cyber Readiness Campaigns, which are a series of assessment events designed to help CCMDs and Services assess and potentially improve their cyber operations and decision-making. Cyber Readiness Campaigns use a CCMD exercise as the capstone event to assess cyber warfighting in a realistic mission context. Precursor Cyber Readiness Campaign events include cyber-stimulation events to help train cyber defenders, tabletop exercises, and range-based exercises to assess the ability of an adversary to disrupt critical missions and impact U.S. operational decision-making. DOT&E worked with cyber defenders during these events to identify critical problems and help improve defenders' capabilities.

Program Activities

Combatant Command and Service Assessments

Of the 49 events in FY22, DOT&E assessed multiple Combatant Commands and Services via Cyber Readiness Campaigns to identify both logical and process issues impeding effective cyber defenses. DOT&E and three of the Operational Test Agencies conduct these assessments in collaboration with the Joint Staff, USCYBERCOM, the Joint Force Headquarters for the Defense Information Networks, and coalition allies and partners. While COVID-19 and events in Ukraine imposed limits on global cyber activities in FY22, there were several notable findings associated with these assessments. CCMD staffs have hardened headquarters networks to the point that in at least two commands, DOD Red Teams were unable to penetrate or maneuver when given network accesses. Assessments also covered new special-purpose or coalition networks, and implemented aggressive remediation processes to address the findings. DOT&E oversaw the integration of offensive cyber operations capabilities into the exercises in FY22, which will continue to expand across the CCMDs. Within the Navy service exercises, the CAP continues to provide key cyber assessment and training to deploying carrier and amphibious troops, and confirmed key practices that harden Navy networks, which the Navy is looking to expand in coming years.

Persistent Cyber Operations

Persistent cyber operations (PCO) provide Red Teams with longer dwell time on DOD networks to probe selected areas and portray more advanced adversaries. As opposed to one- to two- week exercises or tests, long-duration activities offer Red Teams time for stealthier cyber reconnaissance to identify cybersecurity weaknesses and access points that might otherwise go undetected. These activities help identify subtler and more pervasive vulnerabilities and provide more realistic training for cyber defenders. Based on lessons learned in early FY22, DOT&E revamped PCO planning and execution to be less driven by geographic CCMD areas of responsibility, and more focused on campaign-style assessments organized around selected missions. Long-duration assessments of selected DOD missions span multiple CCMDs, and we expect to see the results of the revamped approach in FY23.

Advanced Cyber Operations Team

DOT&E has access to advanced cyber operators (ACO) across multiple organizations to support special assessments, augment Red Teams with specialized cyber expertise, and assist in the portrayal of more advanced adversaries. Organizations with ACO talent include government Red Teams, Federally Funded Research and Development Centers, National Labs, University-Affiliated Research Center Laboratories, academia, and industry. During FY22, the DOT&E ACO supported:

- Cybersecurity testing of the F-35, Ground-Based Strategic Deterrent, and F-22
- Assessments of offensive cyber operations capabilities
- Assessment of Zero Trust architectures in Microsoft Software-as-a-Service environments
- Assessments of military aircraft transponders and critical aircraft systems
- Development of enhanced Red Team capabilities
- Expansion of Red Team accesses via PCO

Demand for ACO support continued to grow in FY22, and DOT&E expects that trend to continue into FY23, with confounding challenges of talent retention due to competing opportunities in the private sector for cyber professionals.

Assessment of Offensive Cyber Capabilities

DOT&E continued assessments of Offensive Cyberspace Operations (OCO), defined as the application of force in or through cyberspace. DOT&E assessments included OCO and their enabling capabilities, such as RF capabilities, as well as OCO planning and integration with other warfare domains. Capability assessments performed in FY22 focused on realism of the representative network, and realism of the threat, which includes a thinking opposing force or adversary. FY22 assessments on the application of OCO in realistic scenarios were performed primarily with USINDOPACOM, U.S. Forces Korea, and Joint Special Operations Command.

Engagement with the Intelligence Community

DOT&E's collaboration with the Intelligence Community remains an essential element of CCMD mission-focused assessments and OT&E events. High classifications assigned to intelligence information on advanced adversary capabilities and intent limit the ability of assessment teams to fully emulate the full-spectrum adversary against which warfighters should routinely practice the execution of their missions. DOT&E is working with the Office of National Intelligence, the Defense Intelligence Agency, DOD Red Teams, the National Ground Intelligence Center, the National Air and Space Intel Center, and the Missile and Space Intelligence Center to improve the information sharing and the resulting realism of the threat portrayed in assessments and OT&E.

Special Project Assessments

DOT&E performed the following special assessments in FY22 in collaboration with USCYBERCOM, USSTRATCOM, the DOD Chief Information Officer (CIO), the Chief Digital and AI Office (CDAO), Joint Forces Headquarters DOD Information Network (JFHQ-DODIN), the Defense Information Systems Agency (DISA), and the Department of Energy Sandia National Labs:

- Zero Trust architectures in Software-as-a-Service environments
- Industrial Control Systems
- RF-enabled cyber operations
- Small Business Innovative Research projects for enhanced cybersecurity of software applications
- Transponder-Combat Identification
- Commercial cloud assessments

- Preparations for assessments of AI and machine learning technologies
- Nuclear command, control, and communications
- Wargames to improve and expand assessments beyond the limits of exercises

Special assessment methodologies and outcomes were shared with requesting organizations and will inform the broader CCMD and Service Cyber Readiness Campaigns, as well as cybersecurity OT&E of acquisition programs.

Results

Combatant Command and Service Assessments

A decade ago, and with SECDEF endorsement, the Chairman of the Joint Chiefs of Staff directed DOD components to incorporate a realistic operational environment into all major DOD exercises. The stated purpose was to improve the DOD capability to sustain operations in a denied or degraded cyber environment. DOT&E was directed to conduct operational assessments of cyber defenses and mission assurance during these exercises. On the 10-year anniversary of the SECDEF-endorsed Chairman of the Joint Chiefs of Staff Execute Order, DOT&E notes the following trends:

- Most exercise authorities allow some level of cyber adversary portrayal during their exercises
- Some CCMDs support longer-duration cyber-Red Team activities (see section on PCOs)
- Network defenses have improved against low- and mid-level cyber threats
- Some CCMDs are showing increased interest in cyber mission rehearsals to augment traditional training exercises

These are positive trends, with the last one critically needed to make up for exercise cancellations and reductions in FY20-21 due to COVID-19. The negative trends are:

- Adversary play during most exercises falls well below the stresses expected from an advanced persistent threat
- Realistic effects that would stress leadership, operators, and network defenders are seldom permitted
- Training objectives receive higher priority than including representative cyber-threat environments.

As a result, DOT&E has limited data to assess whether warfighters can sustain missions in cyber-contested conditions representative of an advanced adversary. In conflict with an advanced adversary, DOD missions will not succeed without effective cyber defenses or operators and leaders who are familiar with indications of attacks and the response actions they must be prepared to execute in a timely manner. In the absence of routine exercises that practice fighting through advanced cyberattacks, DOD missions are at risk of disruption from adversarial cyber actions.

The remainder of this section covers assessment activities that the DOT&E CAP supported in FY22, ranging from Zero Trust validation events, special assessments of emerging and commercial technologies, and assessments of specific mission areas, such as NC3 challenges and concerns about the ability of DOD Red Teams to portray advanced adversaries.

Zero Trust Validation Events

The DOD CIO describes Zero Trust as “protecting critical data and resources, not just the traditional network or perimeter security” (Department of Defense Zero Trust Reference Architecture). For several years, DOT&E CAP has recommended moving from boundary-focused to data-focused protections. Throughout 2022, DOT&E CAP continued to see failures of the DOD’s defense-in-depth architecture due to failures in technologies and defenses at higher levels that lower-tiered organizations are fully dependent on, and yet are unaware of the failures. The complexity of the current architecture creates significant challenges to adequate cyber survivability of critical DOD missions.

The DOD has many ongoing efforts to move to a Zero Trust architecture and DOT&E CAP has observed positive outcomes as a result of adoption of various combinations of the tenets and pillars of Zero Trust, as defined by the DOD CIO. DOT&E CAP has not yet observed a complete implementation of Zero Trust that includes continuous multi-factor authentication, micro segmentation, encryption, endpoint security, automation, analytics, and robust auditing. Listed below, under the tenets and pillars of Zero Trust, are DOT&E CAP observations so far:

TENETS:

- Assume a Hostile Environment – DOT&E's assessment results support this assumption.
- Presume Breach – DOT&E-sponsored cyber–Red Teams routinely breach network perimeters.
- Never Trust, Always Verify – The concept of least-privilege and locking down access to data continues to be a challenge across the DOD enterprise.
- Scrutinize Explicitly – Cyber defenders with training and capabilities continue to be identified as the most critical attribute to cyber survivability.
- Apply Unified Analytics – Multiple efforts are ongoing across the DOD to improve logging and analytics for every action but the efficacy of these actions is still unclear.

PILLARS:

- Users – Shortfalls in multi-factor authentication and privilege access management remain.
- Device – Device monitoring, comply-to-connect, and continuous monitoring of devices across the DOD has improved but is not yet complete.
- Network – Segmentation and granular access to the multitude of DOD networks remains a challenge.
- Data – Organizations have started to review the criticality of data elements in preparation for Zero Trust.
- Visibility and Analytics – Improvements in visibility have contributed to cyber defenders' successes.
- Automation and Orchestration – Some organizations have implemented automated security processes to orchestrate security changes at a faster pace, but this is not ubiquitous across the DOD.

Collaboration with Commercial Sector to Assess Cybersecurity of Infrastructure Supporting DOD Operations

DOT&E observed growing instances in FY22 where critical elements of a DOD capability reside in networks or infrastructure deemed proprietary by the commercial sector; this is especially true with commercial clouds. The DOD migration of critical missions and classified data to commercial clouds continues to expand, but current contracts with cloud vendors do not allow the DOD to independently assess the security of cloud infrastructure owned by the commercial vendor. This prevents the DOD from fully assessing the security of commercial clouds and the DOD missions that they support. Future contracts must provide for threat-realistic, independent security assessments by the DOD of commercial clouds to ensure critical data is protected.

During FY22, DOT&E continued to collaborate with Amazon Web Services, which is providing commercial cloud services that support critical DOD missions. Planning is underway for assessments of cloud infrastructure, and events that will bring DOD network defenders into closer coordination with Amazon Web Services defenders. This will help ensure both sets of defenders gain appreciation for their counterpart's sensors, tools, and approaches to detecting and responding to cyberattacks, and improve responses to attacks. Collaboration between DOT&E and cloud service providers enables DOD and cloud vendors to develop and share best practices and information on emerging technologies and threats, and helps ensure DOD's commercial clouds are secure against advanced cyber adversaries.

DOD Ability to Portray Advanced Cyber Threats

A large gap exists between the cyberattack capabilities of advanced threats and the ability of DOD Red Teams to emulate these threats during exercises assessments and OT&E. One dimension of this gap is insufficient time on network for cyber aggressors;

persistent cyber operations are expected to reduce this component of the capability gap. Other gaps include limited Red Team toolsets, deficiencies in Red Team tactics, techniques, and procedures, unrealistic rules of engagement during exercises, and lack of end-to-end planning for a coherent cyber threat campaign.

DOT&E sponsors a Red Team Development Working Group that identifies requirements for emulating various adversaries and pursues the acquisition of development of tools for Red Teams that will improve the realism of assessments on operational networks. Resources for tool development and acquisition are limited, as are the number of master-level operators needed to portray advanced adversaries.

Aircraft Combat Identification

DOT&E consolidated two years of data showing the mission effects from degraded Transponder Combat Identification (T-CID), including potential effects from an adversary manipulating T-CID messages These results are now included in planning efforts for selected FY23 CCMD and Service exercises.

Artificial Intelligence and Machine Learning

DOT&E continued efforts to prepare for assessments of AI-enabled technologies. This included engagement with CDAO representatives at multiple CCMDs to prepare for deployments of AI-enabled technologies via the DOD's AI and Data Acceleration (ADA) initiative, as well as other efforts already underway at USINDOPACOM and USNORTHCOM. The DOT&E CAP initiated an AI/Machine Learning (AI/ML) working group with Federally Funded Research and Development Centers, National Labs, Academia, and DOD Red Teams. This working group began to identify best practices for AI/ML assessment methods and tools, metrics unique to AI/ML technologies, Red Team tools and tradecraft needed to perform counter-AI/ML assessments, and specific requirements for range environments.

Data Standards, Training, and Automation

DOT&E relies on data from the Red Teams to correlate adversarial activities with mission assurance findings and defensive cyber processes. Historically, Red Team data products required manual collection of their adversarial cyber activities. DOT&E analytical objectives for FY23 and beyond will require improved Red Team data standards and training, and automated collection of Red Team data. DOT&E established a working group to create automated data collection procedures that will assist Red Teams in capturing and reporting required data.

Missile Defense PCO Assessment

The Missile Defense Agency (MDA) continued a PCO assessment of the MDA unclassified and classified networks (UNet/CNet) in FY22. While not the operational networks for the Missile Defense System, the UNet/CNet are paramount to the development effort leading to a combat-capable Missile Defense System. The goal of this PCO is to discover potential cybersecurity vulnerabilities and identify potential fixes to help make UNet/CNet more secure.

Nuclear Command, Control, and Communications (NC3) Hardening

DOT&E and Commander, USSTRATCOM have committed to a partnership for assessing and improving the cyber survivability of the NC3. USSTRATCOM has directed NC3 enterprise organizations to conduct hardening actions on their respective NC3 systems.

In FY22, DOT&E met with 20 NC3 enterprise organizations to discuss how they implemented the requested NC3 hardening actions, observed and reported on challenges in the NC3 hardening process, and provided recommendations to USSTRATCOM for future NC3 hardening efforts. As a result of these efforts, many important improvements have been made to the NC3 mission.

The complex nature of the hybrid legacy and modernized system-of-systems that comprises the NC3 poses challenges to assessments of this mission space, however, progress is being made across the NC3 enterprise as a result of the continued partnership. Barriers to cyber assessments of the NC3 enterprise include a lack of operational capacity to support operations and testing simultaneously, as well as ongoing modernization efforts.

Offensive Cyber Capability Assessments

The DOD continues to develop offensive cyber capabilities without formal operational testing to ensure such capabilities will work when used against in representative operational conditions. Although DOT&E's CAP supports operationally realistic testing against a small subset of offensive cyber capabilities, there are many more offensive cyber capabilities being developed in multiple DOD Components with no such testing. This risks such capabilities failing to work when needed and lowers commanders' confidence in the capabilities. DOT&E collaborated with USCYBERCOM representatives in FY22 with the goal of making such testing more routine and placed the JCWA on the DOT&E oversight list. OT&E of the JCWA will provide the opportunity to assess many smaller OCO capabilities not on oversight.

U.S. Space Force

U.S. Space Force, as the newest Service, recognizes the importance of cybersecurity and cyber survivability as key elements to its ability to perform its missions; this recognition and commitment to improvement has been instilled in the Space Force by the Chief of Space Operations. For example, the Space Force is building units that will assign cyber defense forces to critical space systems. This effort directly aligns with findings from DOT&E assessments that knowledgeable defenders with training and tools are vital to cyber survivability. At the request of the Chief of Space Operations, DOT&E is providing cybersecurity assessments, training opportunities with DOD Red Teams, and lessons learned from other assessments across the DOD in order to speed the establishment and maturation of these critical forces.

Wargames to expand Mission Assurance Assessments

To highlight the importance of cyber defenders and expose non-experts to key aspects of cyber warfare, the Institute for Defense Analysis, with the support of DOT&E's CAP, piloted a tabletop cyber wargame in FY22. Initial results were promising, and DOT&E plans to include this wargame as part of future Cyber Readiness Campaigns. Wargames may also help demonstrate potential mission impacts of advanced cyberattacks to warfighters and leaders.

Way Ahead and Recommendations

Increasing the realism of the assessments to accurately assess the warfighter's ability to sustain missions in environments contested and degraded by an advanced cyber adversary will continue in FY23. Ready access to a talented cyber workforce and advanced tools remains essential, and DOT&E continues to advocate that the DOD establish a well-resourced pipeline of cyber talent from Academia, Federally Funded Research and Development Centers, National Labs, and the commercial sector. Overarching recommendations and assessment objectives for FY23 are discussed in the following subsections.

Combatant Command and Service Exercises Should Increase Emphasis on Fighting Through Cyberattacks

The DOD should continue to emphasize improving the skills of cyber defender personnel. Increased focus should encompass not only the technology, but also the doctrine, organization, and training needed to ensure cyber defenders can effectively thwart cyber adversaries' attempts to disrupt DOD missions. All personnel performing DOD missions – including commanders and system and network operators – should be trained and equipped to recognize and help fight through cyberattacks commensurate with the degree of training provided to kinetic warfare operators. This will require the development of, and training for, new technologies capable of identifying potential cyberattacks to system operators and mission commanders. Such "cyberattack warning" technologies must be developed in order to identify and react to cyberattacks on mobile platforms such as aircraft, ships, and combat vehicles. Critical DOD missions should always be supported by trained teams dedicated to providing cyber defense for those missions. The DOD should establish a cyber "fight-through objective" for every major exercise to provide warfighters and cyber defenders the opportunity to experience the full spectrum of cyber threats and effects; allow them to improve their defenses, detections, and resilience; and demonstrate they can fight through representative cyberattacks.

Assessment of Zero Trust Implementation

DOT&E will continue performing rigorous assessments of Zero Trust implementation across the DOD.

Commercial Cloud Infrastructure Independent Assessments

DOT&E will continue collaboration with commercial cloud providers to identify risks to DOD critical missions and ways to mitigate these risks. The DOD should renegotiate contracts and establish requirements for future contracts with commercial cloud providers that enable the DOD to perform independent and threat-representative cybersecurity assessments of cloud infrastructure which hosts critical DOD capabilities.

Advanced Cyber Threat Emulation

Cyber operations increasingly involve interactions with the other warfighting domains (air, land, sea, space) and electromagnetic spectrum operations. DOT&E will increase focus on the following areas to achieve a more-realistic portrayal of full-spectrum threats during CCMD and Service assessments:

- Cyber-physical systems such as industrial control systems and aircraft transponders
- Cyber-electromagnetic spectrum operations that use radio frequencies to cause cyber effects
- Cyber operations at tactical levels for better integration into military maneuvers in other domains

DOT&E will continue to sponsor the Red Team Development Working Group to provide more advanced tools and tradecraft for Red Teams that support CAP assessments and OT&E. DOT&E will also pursue additional resources for tool development and acquisition that include IP, non-IP, and special capabilities that will be needed for assessments of new technologies such as AI-enabled capabilities.

Aircraft Combat ID

DOT&E will assess T-CID in FY23 Northern Edge and Bold Quest exercises. DOT&E will include other cyber-RF threats in CAP events, and transition mature threat emulations into relevant OT&E.

AI- and ML-Enabled Technology Assessments

DOT&E will work with CDAO representatives to assess the cybersecurity of AI-enabled technologies deployed to the CCMDs, in conjunction with the assessment activities that DOT&E already performs at the CCMDs. DOT&E will continue efforts to identify best practices for AI/ML assessment methods and tools, metrics unique to AI/ML technologies, Red Team tools and tradecraft needed to perform counter-AI/ML assessments, and specific requirements for range environments.

Data Standards and Automation

DOT&E will invest in new technology and personnel to achieve improved Red Team data standards and improve automation for collecting Red Team data.

Missile Defense PCO Assessments

The MDA should continue PCO assessments of the MDA unclassified and classified networks (UNet/CNet) in FY23. DOT&E will monitor progress of these assessments, ensure this PCO effort is executed to the same standards as other PCO assessments sponsored by DOT&E, and synchronize findings with missile-defense assessments performed with CCMDs.

Nuclear Command, Control, and Communications (NC3) Hardening

DOT&E will continue close collaboration with Commander, USSTRATCOM and the NC3 enterprise organizations to assess the hardening actions on their respective NC3 systems.

Offensive Cyber Operations Capability Assessments

DOT&E will continue engagement with USCYBERCOM and the Service developers of OCO capabilities to increase test the realism of OCO capabilities and tools not covered under formal OT&E. The DOD should ensure critical offensive cyber capabilities are operationally tested prior to their fielding.

U.S. Space Force

In FY23, DOT&E will continue to ramp up assessment activities with the U.S. Space Force and the U.S. Space Command. New assessment teams will be established and supporting resources identified to support planning and execution of mission-focused exercises with representative threat emulation.

Wargames to Expand Mission Assurance Assessments

DOT&E will use cyber wargames at CCMDs in FY23 as a complementary approach to assessing their cyberspace capabilities and processes. DOT&E will tailor each wargame using the applicable cyberspace terrain, participating cyber units, adversarial objectives and tactics, and overall scenario to enable stakeholders to explore cyberspace decisions and their relationship to improved mission assurance. These wargames should be particularly helpful to extend beyond exercise events that were limited due to competing training objectives, and to explore in focused ways the potential mission impacts of advanced cyberattacks; the indications and warnings of these attacks; and the types of responses that defenders, operators, and leaders should have at the ready to sustain their critical missions in cyber-contested environments.

Table 1. Cybersecurity Assessment Program FY22 Activity

Type of Event
Physical Security Assessment (4 Events) USINDOPACOM, USSOCOM, USSTRATCOM, USFK
Range Event (1 Event) USCENTCOM
Assessments of Network Security, Stimulation Exercises, and Tabletop Exercises (11 Events) USCENTCOM, USCYBERCOM (2), USEUCOM, USINDOPACOM (2), USSOCOM, USSOUTHCOM, USSPACECOM, USSTRATCOM, USFK
Assessment of Mission Effects during Exercises (13 Events) USAFRICOM (2), USINDOPACOM, USNORTHCOM, USSOCOM (2), USSOUTHCOM, USTRATCOM, US Air Force, US Navy (3), USFK
Assessment of Cyber Fires Processes for Offensive Cyber Operations (2 Events) USINDOPACOM, USFK
Assessment of Special Capabilities and Projects (12 Events) Capability Assessment (2), OCO Capability (4), SME Support (2), TCID (4)
Assessments Employing Persistent Cyber Operations (6 Efforts) USCENTCOM, USEUCOM, USINDOPACOM, USSTRATCOM, U.S. Air Force, Missile Defense Agency
OCO – Offensive Cyberspace Operations; SME – Subject Matter Expert; TCID – Transponders, Combat Identification; USAFRICOM – U.S. Africa Command; USCENTCOM – U.S. Central Command; USCYBERCOM – U.S. Cyber Command; USEUCOM – U.S. European Command; USFK – U.S. Forces Korea; USINDOPACOM – U.S. Indo-Pacific Command; USNORTHCOM – U.S. Northern Command; USSOCOM – U.S. Special Operations Command; USSOUTHCOM – U.S. Southern Command; USSPACECOM – U.S. Space Command; USSTRATCOM – U.S. Strategic Command

International Test and Evaluation Program (ITEP)

The International Test and Evaluation Program (ITEP) permits establishment of bilateral and multilateral agreements 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. These agreements facilitate the planning and execution of cooperative T&E projects, transfer of necessary test equipment and materials, exchange of T&E relevant information through working groups, and reciprocal use of test facilities.

The United States holds 11 bilateral agreements with international partners. During FY22, discussions continued with additional prospective international partners pursuant to negotiating more bilateral agreements. Additionally, two multilateral agreements are in place. They are the Multinational Test and Evaluation Program (MTEP) Memorandum of Understanding (MOU) with Australia, Canada, New Zealand, and the United Kingdom, and the Transatlantic MTEP MOU with France, Germany, Italy, and the United Kingdom. The addition of other NATO partners to the Transatlantic MTEP MOU is under consideration.

Table 1 below lists the current agreements in effect prior to FY22.

Table 1. IT&E Ongoing Project Agreements in Effect

No.	IT&E Projects	Partner(s)	Test Activity Locations	Expiration
1	Advanced Distributed Modular Acquisition System (ADMAS) Instrumentation Equipment and Material Transfer Arrangement	Germany	Koblenz, Germany	October 25, 2024
2	Sky Sabre System (SkS) Reciprocal Use of Test Facilities (RUTF) Project Arrangement (PA)	United Kingdom	White Sands Missile Range, New Mexico	November 9, 2025
3	Flight Test Working Group (WG) Terms of Reference (TOR)	Australia, Canada, New Zealand, United Kingdom	Not Applicable	December 31, 2023
4	Heterogeneous Multiphase Reactive Blast (HMRB) Cooperative T&E (CTE) PA	Canada	Suffield Research Centre, Ralston, Alberta, Canada	December 3, 2023
5	T&E of the United Kingdom 28 Engineer Regiment, Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Defense Tactics, Techniques, and Procedures (TTPs) RUTF PA	United Kingdom	Dugway Proving Grounds, Utah	January 13, 2031
6	Flight Test Aegis Weapon Systems-31 (FTM-31) RUTF PA	Australia	Pacific Missile Range Facility, Hawaii	March 28, 2023
7	Electronic Warfare Operational Test 2016 RUTF PA	Canada	Naval Research Laboratory, Hawaiian Operating Areas, Marine Corps Air Station, Kaneohe Bay, Hawaii	May 19, 2024
8	CF-18 Software Upgrade T&E RUTF PA	Canada	Naval Air Warfare Center, China Lake, California	June 14, 2024
9	T&E of the German Bundeswehr CBRNE Defense TTPs RUTF PA and Annex A	Germany	Dugway Proving Ground, Utah	June 15, 2026
10	Aircraft Electronic Warfare CTE PA	Australia, Canada, United Kingdom	Various partner test locations	August 5, 2026
11	Amendment Six to the Integrated Air and Missile Defense (IAMD) RUTF PA (Formidable Shield)	United Kingdom	Hebrides Test Range, United Kingdom	November 19, 2022
12	T&E of Protective Ensembles Using the Porton Man Test Fixture CTE PA	United Kingdom	Porton Down, United Kingdom	May 11, 2025
13	SIMULATION DISPLAY (SIMDIS™) Sustainment for Sensors, Weapons, Analysis and Tactical Display Developments RUTF PA	Canada	Naval Research Laboratory, Washington, D.C.	October 29, 2025
14	Project Raider Data Evaluation RUTF PA	Canada	Naval Research Laboratory, Washington, D.C.	March 10, 2023
15	Tactical Armored Patrol Vehicle Testing RUTF PA	Canada	Aberdeen Test Center, Aberdeen Proving Ground, Maryland	December 31, 2023
16	CH-146 Radar Warning Receiver (RWR) Validation and Operational Readiness Assessment RUTF PA	Canada	Naval Air Warfare Center (Weapons Division), China Lake, California	February 2, 2023
17	Land Platforms Autonomy and Robotics WG Terms of Reference (TOR)	Italy	Not Applicable	January 21, 2030

Table 1. IT&E Ongoing Project Agreements in Effect

No.	IT&E Projects	Partner(s)	Test Activity Locations	Expiration
18	Joint-Improvised-Threat Defeat Organization Electronic Counter Measures RUTF PA	Australia	Naval Air Warfare Center (Weapons Division), China Lake, California	December 5, 2023
19	Partnership for Autonomous Robotic Test Instrumentation WG TOR	Germany	Not Applicable	April 11, 2028
20	Low Frequency Acoustic Characteristics RUTF PA	United Kingdom	Naval Research Laboratory, Acoustic Measurement Facility, Washington, D.C.	January 19, 2023
21	Combat Archer II Omnibus RUTF PA	Canada	Tyndall Air Force Base, Florida	December 21, 2025
22	Combat Hammer Omnibus RUTF PA	Canada	Various U.S. Air Force Bases	November 23, 2026
23	T&E of Shipboard Jammer and Off-Board Decoy Electronic Countermeasure-Electronic Attack Techniques RUTF PA	Canada	Naval Research Laboratory, Washington D.C.	September 29, 2022
24	TOR for Live Fire WG	United Kingdom	Not Applicable	December 20, 2025

1. Advanced Distributed Modular Acquisition System (ADMAS) Instrumentation Equipment and Material Transfer Arrangement

This 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 at Koblenz. 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. In FY21, the Army was unable to transfer the equipment as planned due to the coronavirus pandemic.

2. Sky Sabre System RUTF Project Arrangement

This testing was executed in 2021 and the agreement allowed the United Kingdom's Ministry of Defence to leverage U.S. Army personnel and facilities at White Sands Missile Range to test the vertically-launched Sky Sabre integrated Ground Based Air Defence system prior to declaring its Initial Operating Capability. Through this agreement, the United Kingdom Ministry of Defence received data on threat detection, threat prioritization, weapon allocation, and threat engagement, as well as post-launch analytical support to evaluate the system's capability.

3. Flight Test Working Group (WG) Terms of Reference

This WG was established to identify and study future collaborative efforts to improve the effectiveness of joint weapons systems T&E through the harmonization of T&E requirements, investment strategies, and evaluation of test matters of mutual interest. Specifically, the Flight Test Working Group focuses on adoption and establishment of interoperable flight test instrumentation architecture to allow contributing participants to collaborate on flight test programs.

4. Heterogeneous Multiphase Reactive Blast (HMRB) Cooperative T&E (CTE) Project Arrangement

This agreement between the United States and Canada supports a series of tests over a three-year period at the Suffield Research Center, Alberta, Canada. The purpose of this agreement is to develop, test, and deploy diagnostics developed to address an HMRB based on a series of explosive charges.

5. T&E of the United Kingdom 28 Engineer Regiment, CBRNE Defense TTPs RUTF Project Arrangement

This agreement with the United Kingdom has enabled the development and testing of partner defense TTPs against CBRNE threats. The U.S. Army Dugway Proving Ground, Utah hosted the tests, providing threat-representative scenarios to support evaluation of the operational effectiveness of new detectors, personal protective equipment (PPE), and decontamination equipment in an operationally representative environment. Tests also included the firing of various weapons by soldiers in protective clothing to evaluate potential impact on mission effectiveness.

6. Flight Test Aegis Weapon Systems-31 (FTM-31) RUTF Project Arrangement

This agreement with Australia permitted the use of a High-Power Phased Array Radar located at the Pacific Missile Range Facility to track a target test vehicle in the Missile Defense Agency's FTM-31 flight test. The radar successfully tracked the target vehicle. Resultant data will support and improve threat characterization. This test was conducted in 2021

7. Electronic Warfare Operational Test 2016 RUTF Project Arrangement

This agreement enables the United States and Canada to continue the at-sea T&E of the electronic warfare suites fitted in Canadian Navy ships. This testing was postponed due to the coronavirus pandemic. It is expected to be conducted in Hawaii, where the United States will simulate anti-ship missile attacks to validate the Canadian Softkill System.

8. CF-18 Software Upgrade T&E RUTF Project Arrangement

This agreement enabled Canada to test upgrades for the CF-18 Hornet at the U.S. Naval Warfare Center, China Lake, California in July and August 2021. This testing validated and verified the upgraded software of the CF-18 and the aircraft's ability to intercept radar signals, identify signal sources, prioritize emitters, and take defensive action against threat weapon systems. Testing was conducted July – August 2021.

9. T&E of the German Bundeswehr CBRNE Defense TTPs RUTF Project Arrangement and Annex A

This agreement enabled the German Bundeswehr to develop and test its defense TTPs against CBRNE threats. The U.S. Army Dugway Proving Ground, Utah hosted the tests, providing threat representative scenarios to support the evaluation of the operational effectiveness of new detectors, to include mass spectrometers, multi-gas measuring devices, radiation detection devices, PPE, and decontamination equipment in an operationally representative environment. Tests also included the firing of weapons by soldiers in protective clothing to evaluate impacts on mission effectiveness. Additionally, tests assessed post attack reconnaissance after an Improvised Explosive Device attack. Also tested were new radios and other communications equipment. Testing was conducted October – November 2019.

10. Aircraft Electronic Warfare Cooperative T&E Project Arrangement

This agreement was established under the MTEP MOU in 2016 and is an important ongoing multinational effort. It is expected to continue through at least 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.

11. Amendment Six to the IAMD RUTF Project Arrangement (Formidable Shield)

This agreement with the United Kingdom has permitted large scale missile defense tests every two years, including the latest in the series, Formidable Shield 21. Formidable Shield 21 was conducted at the United Kingdom's Hebrides Test Range and included 11 nations and 16 ships. This event involved use of ground-launched supersonic low altitude targets and ballistic missiles as targets. Formidable Shield 21 witnessed the first ever use of a Pathfinder Zombie short range ballistic missile target, provided by the Missile Defense Agency. Additionally, there were two U.S. Medium Range Ballistic Missile Target presentations. These tests demonstrated the potential for launch on remote engagements wherein target data are passed from one ship to another. The Formidable Shield exercise series provides the most comprehensive opportunity to evaluate IAMD capability in the Atlantic area of operations. The next event will continue to increase in complexity. A key feature of this test series is the demonstration of combat systems interoperability among the participating nations.

12. T&E of Protective Ensembles Using the Porton Man Test Fixture CTE Project Arrangement

This agreement with the United Kingdom has enabled extensive use of a mannequin named Porton Man to test chemical protective clothing for military personnel. Currently, the Porton Man tests are developing test methods and conducting 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 CTE PA supports U.S. DOD requirements to protect personnel from Chemical Biological threats. Figure 1 displays the Porton Man protective equipment uniform used during testing.

Figure 1. Porton Man Testing of Uniform Integrated Protective Equipment

13. SIMULATION DISPLAY (SIMDIS™) Sustainment for Sensors, Weapons, Analysis and Tactical Display Developments RUTF Project Arrangement

This 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 will be evaluated for use in operational analyses for tactical development and platform procurement programs.

14. Project Raider Data Evaluation RUTF Project Arrangement

This agreement supports testing and validating Canadian ships' ability to generate Maritime Domain Awareness data for the RAIDER-M and the Sealink Advanced Analysis (S2A) or similar system. This project assesses the ship's ability to detect, precision track, and report low altitude aerial vehicles and surface targets. Test results will be collected and validated using Naval Research Laboratory, Washington, D.C. equipment and facilities.

15. Tactical Armored Patrol Vehicle Testing RUTF Project Arrangement

This agreement permits the U.S. DOD to provide T&E support to a Canadian Department of National Defence acquisition program. The testing and validation of the tactical armored patrol vehicle will consist of, but not be limited to, Tilt Table Test (one and two axles), Circular Test in both dry/wet conditions to determine understeer and oversteer conditions, double-lane change test, J-turn test, Sine and Dwell Test, On-Center Steer Test and potentially a Step Steering test, suspension vibration, and tire characterization.

16. CH-146 Radar Warning Receiver (RWR) Validation and Operational Readiness Assessment RUTF Project Arrangement

This agreement allows the U.S. DOD to evaluate the performance and effectiveness of the APR-39 Version-C RWR and assess the capability of Canadian tactical aviation personnel to conduct realistic mission sets in an electronic warfare threat environment.

17. Land Platforms Autonomy and Robotics Working Group TOR

This Working Group, led by the U.S. Army, exchanges data on Test Operating Procedures and Standard Operating Procedures relevant to testing unmanned vehicle maneuverability and weaponized autonomous platforms with Italy. The group is also sharing technology development updates on data acquisition, precision tracking and system surveillance, and other measurement techniques concerning T&E of autonomous vehicle systems. This WG effort will facilitate demonstration of test capabilities at key facilities responsible for testing mobility and weapon systems performance for autonomous systems.

18. Joint Improvised-Threat Defeat Organization Electronic Counter Measures RUTF Project Arrangement

This agreement covers testing of the Australian Department of Defence electronic countermeasures (ECM) systems. The U.S. DOD, through the Naval Air Warfare Center Weapons Division (NAWC-WD) China Lake Facility, provided T&E support to the Australian Department of Defence (test facilities, simulators, and technical staff) for testing and validation of ECM equipment. Such testing included electromagnetic interference and electromagnetic compatibility issues as well as system reaction and processing limitations in the electromagnetic environment.

19. Partnership for Autonomous Robotic Test Instrumentation Working Group TOR

This Working Group, led by the U.S. Army, was established to harmonize T&E instrumentation and autonomous/robotic requirements, study feasibility of future cooperative Test and Evaluation Program (TEP) Activities, and exchange data reports on specific T&E issues of mutual interest with Germany.

20. Low Frequency Acoustic Characteristics RUTF Project Arrangement

This agreement concerns testing objects of interest to acquire high fidelity low frequency acoustic scattering data. The test will determine the low frequency acoustic characteristics of a set of test objects suitable for characterization. The consistency of acoustic measurements produced by the acoustic measurement facility will be evaluated.

21. Combat Archer II Omnibus RUTF Project Arrangement

This agreement addresses operational effectiveness and suitability testing of the Canadian Air Force's CF-18 air-to-air weapon systems using a total system approach that includes man, munitions, and machines.

22. Combat Hammer Omnibus RUTF Project Arrangement

This agreement addresses operational effectiveness and suitability testing of all aspects of the CF-18 air-to-ground weapons system.

23. T&E of Shipboard Jammer and Off-Board Electronic Countermeasure-Electronic Attack Techniques RUTF Project Arrangement

This agreement concerns performance of Canada's shipboard jammer and off-board decoy ECM techniques and tactics via laboratory testing at the Central Target Simulator facility at the Naval Research Laboratory, Washington, DC.

24. TOR for Live Fire Working Group

This Working Group, led by DOT&E, was established to identify potential collaborative efforts in LFT&E, to include ground combat vehicles and PPE with the United Kingdom.

In FY22, in support of the ITEP mission, DOT&E reviewed and approved nine agreements. Table 2 lists all of the agreements and location of testing.

Table 2. IT&E Documents Signed into Effect in FY22

No.	IT&E Projects	Entry into Effect Date	Partner	Test Activity Locations
1	High Intensity Radiated Field (HIRF) Testing on the CC-295 Kingfisher RUTF PA*	September 20, 2021	Canada	Naval Air Warfare Center (Aircraft Division), Patuxent River, Maryland
2	T&E of the Australian SOER CBRN Defense and EOD TTPs RUTF PA and Annex A*	September 21, 2021	Australia	Dugway Proving Ground, Utah
3	Amendment One to Tactical Armored Patrol Vehicle Stability Characterization Testing RUTF PA	February 11, 2022	Canada	Aberdeen Test Center, Aberdeen Proving Ground, Maryland and the Ground Vehicle Systems Center, Warren, Michigan
4	Her Majesty's Canadian Ship (HMCS) Windsor Testing RUTF PA	April 28, 2022	Canada	Andros Island, Commonwealth of the Bahamas
5	Laboratory and Field T&E of Australian Defence Science and Technology Group (DSTG) Chemical and Biological Defensive Material RUTF PA*	April 28, 2022	Australia	Dugway Proving Ground, Utah
6	Amendment Two to the T&E of Shipboard Jammer and Off-Board Decoy Electronic Countermeasure-Electronic Attack Techniques RUTF PA	June 23, 2022	Canada	Naval Research Laboratory, Washington, D.C.
7	Annex B to the T&E of the German Bundeswehr CBRNE Defense TTPs RUTF Project Arrangement	August 18, 2022	Germany	Dugway Proving Ground, Utah
8	Annex B to the T&E 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	September 12, 2022	Australia	Dugway Proving Ground, Utah
9	Amendment Seven to the Integrated Air and Missile Defense (IAMD) Testing Reciprocal Use of Test Facilities (RUTF) Project Arrangement (PA)	September 21, 2022	United Kingdom	Hebrides Test Range, United Kingdom

1. High Intensity Radiated Field (HIRF) Testing on the CC-295 Kingfisher RUTF Project Arrangement

Under this agreement, the Naval Air Warfare Center provided HIRF T&E support to Canada's testing of the newly acquired CC-295 Kingfisher Fixed Wing Search and Rescue aircraft. This included use of test facilities, set up and operation of test equipment, and data collection including equipment readings, still photography, and video. Testing was conducted September 30 –November 5, 2021.

2. T&E of the Australian SOER CBRN Defense and Explosive Ordnance Disposal (EOD) TTPs RUTF Project Arrangement and Annex A

This agreement with accompanying Annex A allowed the Australian SOER to conduct a full range of evaluated CBRN mission requirements at multiple Dugway Proving Ground, Utah locations. Execution of TTPs addressed Australian DOD SOER tactical operational needs and management of situations involving CBRN threats and homemade explosives. The objective was to improve current TTPs, as well as develop additional TTPs to address operational gaps identified during testing. Testing was conducted September 27 - October 15, 2021.

3. Amendment One to the Tactical Armored Patrol Vehicle Stability Characterization Testing RUTF Project Arrangement

Refer to Table 1, entry 15 and its accompanying narrative for information on this agreement.

4. Her Majesty's Canadian Ship Windsor Testing RUTF Project Arrangement

This agreement covers testing of the MK 48 Mod 7 Advanced Technology Torpedo as well as the combat systems of the Her Majesty's Canadian Ship Windsor.

5. Laboratory and Field T&E of Australian Defence Science and Technology Group (DSTG) Chemical and Biological Defensive Material RUTF Project Arrangement

This agreement with the Australian Defence Science and Technology Group covers testing of the Australian Defence Force's CBRN defensive capabilities for the protection of personnel from the strategic, tactical, and physiological effects of exposure to toxic chemicals, materials, and CBRN weapons. Testing was conducted June 6 – 30, 2022. Figure 2 shows the chemical detection process in progress.

Figure 2. Conducting Chemical Detection at Dugway Proving Ground

6. Amendment Two to the T&E of Shipboard Jammer and Off-Board Decoy Electronic Countermeasure-Electronic Attack Techniques RUTF Project Arrangement

Amendment two of this agreement permits additional testing of the type addressed in Table 1, entry 23 and its accompanying narrative providing information on this agreement.

7. Annex B to the T&E of the German Bundeswehr CBRNE Defense TTPs RUTF Project Arrangement

Refer to Table 1, entry 9 and its accompanying narrative for a full description of this agreement.

8. Annex B to the T&E 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 Project Arrangement

Annex B of the agreement allowed the Australian SOER to continue 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 TTPs and to develop additional TTPs for operational gaps identified during this test event. Refer to Table 2, entry 2 and its accompanying narrative for further detail. Testing was conducted at Dugway Proving Ground, Utah September 26 – October 14, 2022. Figure 3 shows the tunnel where testing was conducted.

9. Amendment Seven to the Integrated Air and Missile Defense (IAMD) Testing RUTF Project Arrangement

This Amendment to the agreement allows for the planning and execution of the interoperable testing that will be conducted during the Formidable Shield 2023 event in May 2023. During the Formidable Shield 23, the U.S. Navy will test its maritime IAMD system at the United Kingdom's Hebrides Test Range with 11 other partner nations. This testing will include employment of ground-launched supersonic low altitude targets.

Table 3 below lists potential future test agreements and IT&E projects.

Figure 3, Tunnel Chemical Target at Dugway Proving Ground

Table 3. Future Test Agreements

No.	IT&E Projects	Objective
1	NATO Defence Innovation Accelerator for the North Atlantic	Develop a TEP MOU
2	U.S.-Japan Test and Evaluation Program (TEP) Memorandum of Understanding (MOU)	Develop a TEP MOU
3	U.S.-Czech Republic TEP Memorandum of Agreement (MOA)	Develop a TEP MOA
4	U.S.-Netherlands TEP II MOU	Develop an updated TEP MOU
5	U.S.-Republic of Korea TEP MOU	Develop a TEP MOU

1. NATO Defence Innovation Accelerator for the North Atlantic (DIANA) TEP MOU

At the June 2021 NATO Summit, allied heads of state endorsed the NATO 2030 agenda, which includes the DIANA initiative to promote technologies. DIANA accelerates technology fielding by leveraging NATO member private sector, academia, government, and military organizations and science and technology communities. The ITEP will support the DIANA initiative through development of an appropriate agreement.

2. U.S.-Japan TEP MOU

The United States will negotiate a TEP MOU with Japan. Significant test opportunities have been identified.

3. U.S.-Czech Republic TEP MOA

The United States will open technical discussions with the Czech Republic pursuant to developing a TEP agreement. Test opportunities have been identified.

4. U.S.-Netherlands TEP II MOU

The United States will open negotiations with the Netherlands to update the current TEP MOU in order to incorporate new international agreement policy provisions. Test opportunities have been identified.

5. U.S.-Republic of Korea TEP MOU

Upon completion of an umbrella agreement with the Republic of Korea, the United States will negotiate a TEP agreement. The umbrella agreement will allow negotiations to begin on the MOU.

Joint Aircraft Survivability Program (JASP)

The Joint Aircraft Survivability Program (JASP) develops cross-Service aircraft survivability solutions and evaluation methods needed to dominate the multi-domain battlefield and mitigate U.S. aircraft losses in combat. JASP products support: 1) weapons tactics schools, air operations, and training; 2) operational and live fire test and evaluation of aircraft systems; 3) aircraft combat damage reporting; and 4) transition of technologies to the battlefield intended to improve aircraft survivability and force protection.

Specifically, JASP:

- Advances the capability and credibility of joint aircraft combat effectiveness tools used in combat mission planning, training, and weapon schools to support the development of air combat tactics, techniques, and procedures (TTPs).
- Manages enterprise-level modeling and simulation (M&S) tools required for credible evaluation of aircraft effectiveness and survivability.

- Supports the Joint Combat Assessment Team, which collects and analyzes U.S. aircraft combat damage and losses to develop the requirements for joint aircraft survivability solutions that provide force protection and remedy operational shortfalls.
- Leverages advances in science and technology to develop innovative survivability enhancement features.

JASP Advances the Capability and Credibility of Joint Aircraft Combat Effectiveness Tools

In coordination with the Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME), JASP co-develops and maintains the Air Combat Effects Library (ACEL). ACEL serves as a joint suite of Service-based data and models used for modeling air-to-air, surface-to-air, and air-to-surface engagements and the resulting aircraft survivability and lethality. ACEL is a library of data and models, to include shooter detection, target tracking, threat and friendly aircraft performance/kinematics, weapon trajectory/shot logic, pilot logic, and standardized threat models.

JASP also supports the development of the Joint Anti-Air Model (JAAM) tool used to conduct combat effectiveness analyses, which underpins air combat TTP development and training. JAAM simulates the kinematic engagement of multiple U.S. (blue) and enemy (red) platforms, including their missiles and weapons. JAAM connects to test and training debrief tools through the use of an application program interface. Figure 1 shows an air-to-air missile engaging a fighter aircraft. Figure 2 shows a proximity fuze fragmenting warhead impacting a target.

Figure 1. JAAM Engagement Example

In FY22, JAAM v5.4 was completed and fielded to over 4,500 users across more than 360 sites. Compared to the prior version, JAAM v5.4 included additional aircraft, updated blue weapons, new and updated threat simulations, an updated Endgame Manager, and the latest time-space-position information format. JAAM v6.0 is an entirely new software design leveraging ACEL. JAAM v6.0 is on schedule for fielding in 4QFY23.

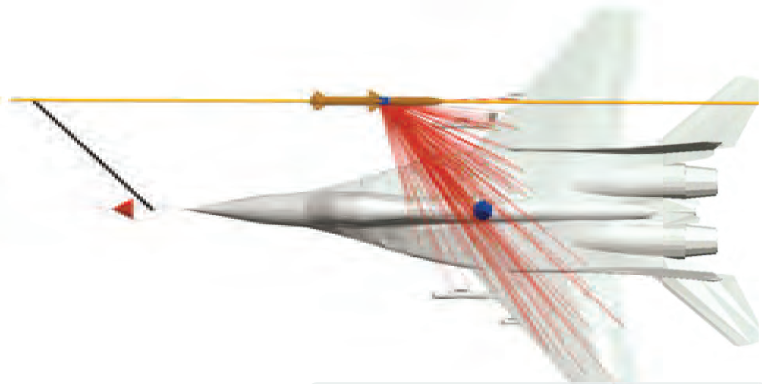


Figure 2. Terminal Endgame

Survivability and Lethality of Aircraft in Tactical Environments (SLATE) is another notable application supporting the acquisition and research and development T&E community by assessing weapons effects in an advanced, contested environment. SLATE development focuses on long-lead capabilities, which are being incorporated within ACEL. SLATE provides the capability to assess aircraft survivability against the full spectrum of threats, including surface-to-air missile systems, air defense artillery, and air-to-air missiles. SLATE also provides insight for future JAAM features within a warfighter-friendly application. In FY22, the Defense Systems Information Analysis Center distributed an initial limited capability beta release (SLATE v0.1) in April, followed by the first general release (SLATE v1.0) in August 2022. Figure 3 depicts an aircraft firing an air-to-air missile in the SLATE application v1.0.

In FY22, JASP and JTCG/ME continued to advance the ACEL numerical engine and data, underpinning both SLATE and JAAM v6.0. JASP advanced ACEL for the low altitude battlespace, by maturing rotary-

Figure 3. SLATE Application

wing aero performance modeling, surface-to-air missile systems radar modeling (i.e., ESAMS), air defense artillery gun modeling, and environment modeling. JTCG/ME advanced the ACEL application programming interface, tying the numerical engine to application layers leveraging ACEL (JAAM v6.0).

JASP Develops and Manages Enterprise-level M&S Tools Required for Credible Evaluation of Aircraft Effectiveness and Survivability

Through tri-service configuration control boards, JASP continues the management of major M&S tools used to estimate air combat effectiveness and survivability against an array of operationally representative kinetic and non-kinetic threats. The toolset includes:

- Brawler – an air-to-air combat simulation
- Enhanced Surface-to-Air Missile Simulation (ESAMS) – a surface-to-air engagement model
- SLATE
- Machine Assisted Exploitability Simulation for Testing Resilient Operations (MAESTRO) – a cyber survivability model
- Computation of Vulnerable Area Tool (COVART) – a vulnerability analysis code, along with its supporting penetration and fire prediction codes:
  - Projectile Penetration (ProjPen)
  - Fast Air Target Encounter Penetration (FATEPEN)
  - Next Generation Fire Model (NGFM)

Table 1 provides a matrix of JASP-supported modeling tools used for acquisition programs under DOT&E oversight.

Table 1. DOT&E Oversight Programs Supported by JASP Tools

Acquisition Program Type	ACAT	Brawler	ESAMS	SLATE	COVART	FATEPEN	ProjPen	NGFM	MAESTRO
Aircraft Survivability Equipment	IC		1						
Bomber Aircraft	-		1		1		1	1	
Fighter Aircraft	ID, IC	3	3		3		3	2	1
Rotary-Wing Aircraft	IC			1	2				
Transport/Tanker Aircraft	IC		1		1	1	1	1	
Special Use Aircraft	ID, III				2	2	2	2	
Weapons	IC	2							
Totals		***5***	***6***	***1***	***9***	***3***	***7***	***6***	***1***

Acronyms: ACAT – Acquisition Category; BCAT – Business System Category; COVART – Computation of Vulnerable Area Tool; ESAMS – Enhanced Surface-to-Air Missile Simulation; FATEPEN – Fast Air Target Encounter Penetration; MAESTRO – Machine Assisted Exploitability Simulation for Testing Resilient Operations; NGFM – Next Generation Fire Model; ProjPen – Projectile Penetration; SLATE – Survivability and Lethality of Aircraft in Tactical Environments

JASP continued development of MAESTRO software to improve the survivability evaluation of U.S. aircraft against cyber threats. This effort, which was done in collaboration with the Air Force, Army, and Navy aviation cyber survivability communities, is providing M&S tools and data standardization to develop and evaluate aircraft survivability in a cyber-contested environment.

In FY22, JASP initiated a new effort intended to develop and validate the M&S capability to evaluate the effectiveness of radio frequency (RF) countermeasures. This 15-month effort will include the collection of flight test data for validation: 1) threat model simulation, 2) countermeasure model, 3) simulated engagement analysis lab, and 4) red and blue system models suitable for RF countermeasure evaluation. Similarly, for infrared (IR)-guided threats, the effort will develop the M&S capability to evaluate the effectiveness of IR countermeasures to include the development of a hardware-in-the-loop capability to collect validation data for advanced countermeasure features.

JASP is also improving the accuracy of aircraft vulnerability assessments that inform design and risk decisions. In FY22, JASP conducted testing needed to validate the NGFM methodology to predict fuel tank dry bay ignitions due to impacts from operationally relevant threats. Figure 4 is a frame capture from the test high-speed video. JASP also evaluated the variation of contact-fuzed exploding threat characterizations on the probability of fire. Lastly, JASP conducted sensitivity studies that will provide uncertainty quantification for analyses and inform resource prioritization for threat characterizations.

JASP supports the Joint Combat Assessment Team to Collect and Analyze U.S. Aircraft Combat Damage and Losses

In FY22, JASP continued to enable aircraft combat damage incident reporting and aviation combat injury analyses through the Joint Combat Assessment Team and the U.S. Army Aeromedical Research Laboratory. The Joint Combat Assessment Team completed combat damage assessments supporting operational forces. To enable combat incident reporting and data sharing across the DOD, Services, and Combatant Commands, JASP transitioned the Combat Damage Incident Reporting System to the National Ground Intelligence Center for hosting.

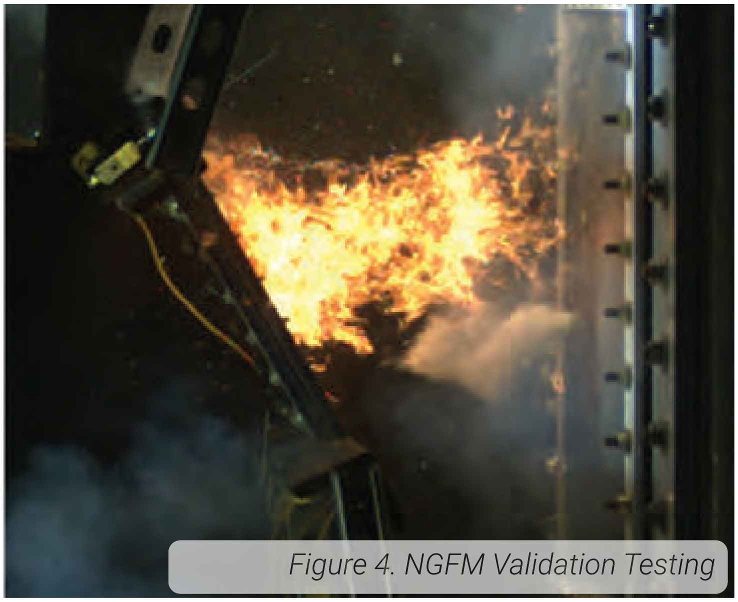


Figure 4. NGFM Validation Testing

JASP Leverages Advances in Science and Technology to Deliver Innovative Survivability Enhancement Features

In collaboration with the OSD and Service organizations, JASP matures threat detection and countermeasure technologies needed to defeat advanced electro-optical/IR- and RF-guided threat systems. JASP's adaptability allows it to adjust its portfolio to quickly fill critical gaps in technologies required by Service programs in addition to maintaining its core efforts of self-protection countermeasure technique development and testing.

In FY22, in addition to on-going efforts to improve missile warning sensor detection and classification, JASP continued advancing the development of an innovative use of electro-optical/IR missile warning sensors for missile threat detection outside customary scenarios. A new effort, started in July, will further expand U.S. missile detection capabilities against advanced threats with the potential for fleet-wide benefits.

A JASP study on the effects of laser jammer amplitude variation caused by rotor blade blockage and engine-plume-induced scintillation was a major influence on the placement of jam heads on a Navy/Marine Corps helicopter laser jammer countermeasure for IR-guided missiles. Informed by data-based system performance impacts at various platform locations, the Program Office was able to make timely and informed decisions on the placement of the jam heads for their airframe, maximizing platform effectiveness.

JASP continued its partnership with the Naval Research Laboratory in the development and demonstration of aircraft self-protection RF electronic attack technologies. Specifically, JASP leveraged the validated threat simulator at the NAVAIR Electronic Combat Simulation and Evaluation Laboratory to demonstrate the effectiveness of advanced techniques against a class of stressing RF threats. Where validated threat simulators are not yet available, JASP, in coordination with the intelligence community, developed an electronic warfare environment around a particular threat model in order to further develop and test electronic attack techniques to counter such threats. This provided the Services with a unique capability for developing countermeasure techniques.

Figure 5. U.S. Marine Corps UH-1Y Venom aircraft

JASP Develops and Tests Technologies that Improve Aircraft Force Protection

In FY22, JASP continued to develop and test technologies that improve the protection of aircraft aircrew and passengers against persistent and emerging threats. JASP successfully demonstrated the effectiveness of a fire-mitigating mist control additive for avionics cooling fluid to reduce the vulnerability of aircraft to onboard fires. The additive had negligible weight impact. JASP will conduct qualification efforts for the additive and investigate applying the technology to other common aircraft flammable fluids.

JASP addressed shortfalls in the self-sealing and crashworthiness capability of fuel cell bladders commonly used to improve rotorcraft safety and survivability. JASP developed revised fuel bladder qualification procedures and test fixtures to improve fuel cell test quality and assessment credibility and conducted testing to quantify the improvements. JASP also tested for crashworthiness a lightweight fuel bladder that was optimized using advanced computer design and simulation methodologies.

JASP demonstrated design improvements to an impulsive hydrodynamic loading test setup for candidate structural joints. The improvements enable characterization of composite joint designs under shear loading and more than doubled test execution efficiency. Republic of Korea collaboration partners conducted parallel testing, providing additional verification data for the experimental method that enables more survivable aircraft structural designs. JASP also continued validation of a rapid structural vulnerability assessment tool that provides a new capability to evaluate structural vulnerability earlier in the aircraft development lifecycle.

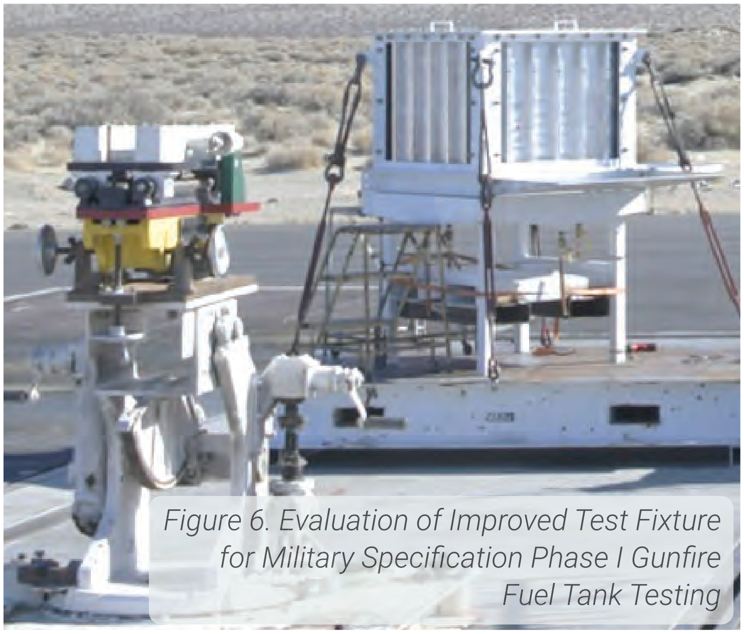
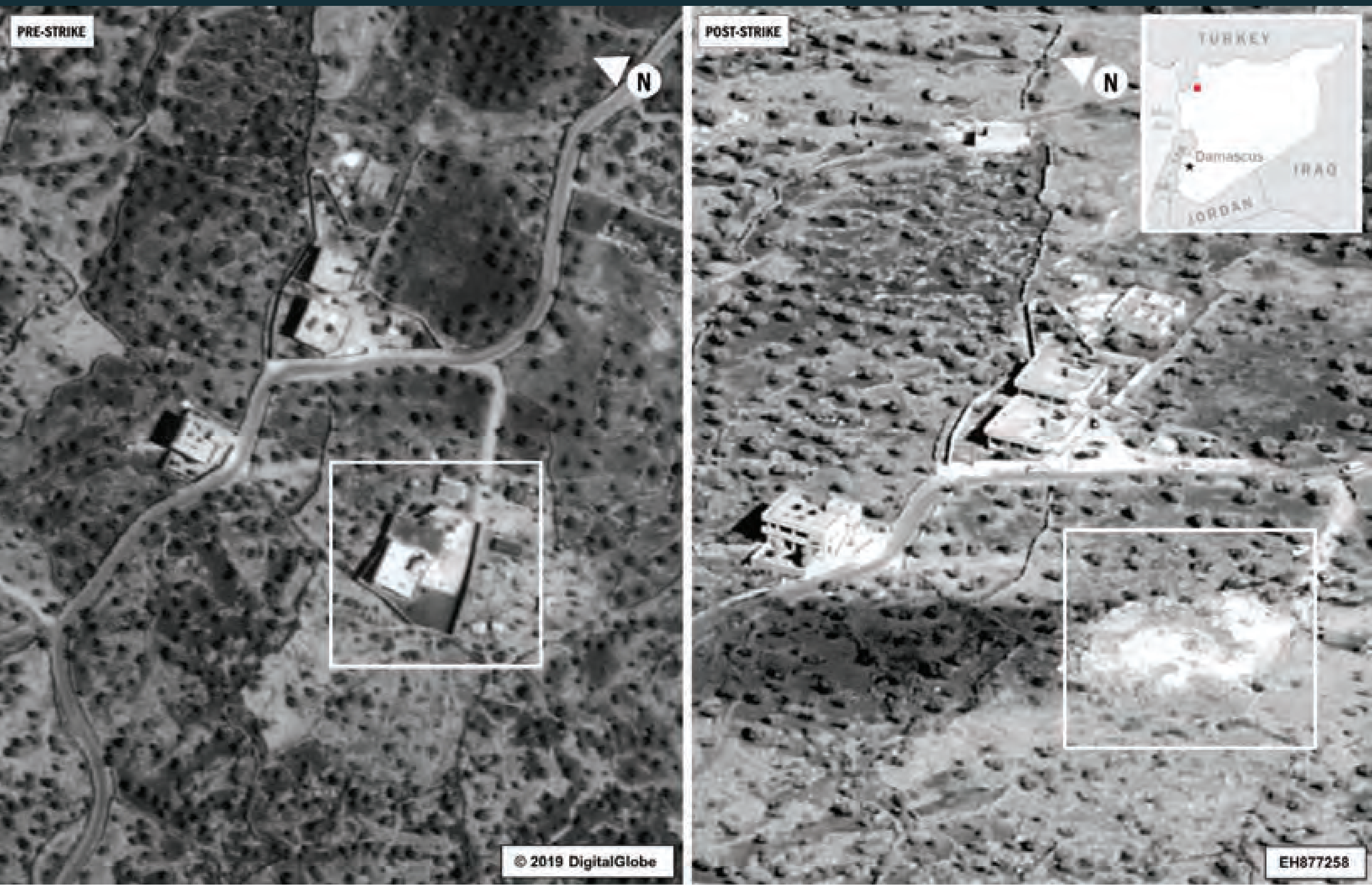


Figure 6. Evaluation of Improved Test Fixture for Military Specification Phase I Gunfire Fuel Tank Testing

Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) Program



Combatant Command strike authorities rely on weaponeering tools developed by the Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) program to estimate and optimize the type and number of U.S. weapons required to achieve the desired lethal effect against a range of strategic or tactical targets, while mitigating risk for collateral damage including civilian casualties.

Current Joint Munition Effectiveness Manual (JMEM) products include:

- The Digital Imagery Exploitation Engine (DIEE), a tool that enables users to plan and execute strikes by seamlessly performing the following Advanced Target Development steps: 1) geographically locate and characterize the target, 2) weaponeer the target using JMEM Weaponeering Software (JWS) and perform target coordinate mensuration, 3) estimate collateral damage effects using the Digital Precision Strike Suite Collateral Damage Estimation (DCiDE) tool, and 4) produce output graphics to the appropriate databases.
- Weaponeering tools capable of estimating lethal effects for directed energy weapons (DEW), cyber, and electromagnetic spectrum (EMS) fires.
- The Joint Anti-Air Combat Effectiveness (J-ACE) tool used in combat mission planning, training, and in weapon schools to support the development of air combat tactics, techniques, and procedures. The J-ACE tool's main module is the Joint Anti-Air Model, which is discussed in the Joint Aircraft Survivability Program section of this report.

In FY22, the JTCG/ME continued to provide oversight of the Joint Live Fire (JLF) program to facilitate the development of adequate LFT&E tools, methods, and infrastructure required for credible development of both JMEM products and LFT&E programs. Examples of FY22 progress include the following: 1) development of new tools and methods to advance lethality evaluation of kinetic weapons, including hypersonic weapons, 2) advancement of a survivability and lethality assessment for maritime targets, 3) improved assessment of traumatic brain injuries (TBIs) due to kinetic threat engagements, 4) improved survivability assessments for U.S. weapon systems and forces against kinetic threat engagements, 5) development of new tools and methods to enhance the survivability and lethality evaluations against non-kinetic threats, and 6) advancement of the use of digital engineering tools to support full-spectrum survivability and lethality evaluations.

JTCG/ME Delivers Credible Weaponeering Tools to Combatant Command Strike Authorities

JMEMs are used daily by warfighters in direct support of operations, mission planning, and training. The user base includes approximately 26,000 personnel, spanning all of the following entities:

- DOD Service members
- Joint Staff/Combatant Commands
- Acquisition community, T&E enterprise, Intelligence Community, and laboratories

In FY22, JTCG/ME conducted multiple Operational User Working Group meetings to facilitate open communication, gather additional operational requirements, and allow units to provide feedback on the products. As a result, JTCG/ME fielded updates to both DIEE and JWS to improve their accuracy and efficiency. Specifically:

- In collaboration with Office of the Under Secretary of Defense for Intelligence and Security and the Joint Staff Directorate for Intelligence, JTCG/ME is enhancing the Joint Targeting Intelligence process by developing and standardizing Advanced Target Development processes in support of the Joint Targeting Cycle. The process of linking desired effects to operational plan (OPLAN) outlined tactical tasks will increase the likelihood of meeting the commander's objective via enhanced integration and connectivity.
- JTCG/ME continued to field and develop DIEE and JWS with enhanced capabilities and incorporated new user interfaces to increase JWS tool usability. JTCG/ME provided a series of new weapon system characteristics, delivery accuracy, and target vulnerability data to the tool to more accurately estimate the final aimpoint, delivery conditions, and number of rounds on target to achieve the desired lethal effects. JTCG/ME included new weapon and weapon trajectory data to keep pace with technology development allowing the strike authorities to account for such enhanced capabilities in their calculations of target defeat. JTCG/ME also implemented an approved software development environment

for continuous JMEM evolution. In support of continued evolution of the DIEE/JWS Advanced Target Development capabilities, JTCG/ME conducted multiple technical reviews of the next generation, scene-based weaponeering product, to include enhanced product level testing, applicability of Development/Security/Operations (DevSecOps) for continuous and incremental increase in capability, and for increased user interface and experience. To maintain consistency with the latest National Geospatial-Intelligence Agency mensuration methods, JTCG/ME updated calculation tools for both Mensuration Services Program and Common Geopositioning Services.

- JTCG/ME enabled data-based updates to collateral effects radii tables, reducing their error margins. It advanced the collateral effects library mitigation tool to increase the efficiency of collateral effects analysis and enhance risk estimate distance calculations used by DCiDE to determine friendly force risk estimates. JTCG/ME also provided assistance with reach-back support for current operations. Multiple reach-back packages for weaponeering, Collateral Damage Estimation (CDE), and Munition Effectiveness Assessment were provided to operational units to assist Combatant Commanders in the decision making process. DCiDE output capability provides aimpoint and collateral effects radii graphics to aid in the decision-making for strike approval authority that are compliant with the Chairman of the Joint Chiefs of Staff Instruction. FY22 updates included collateral effects radii for weapons that implement Proximity and Point Detonation Fuzes.
- JTCG/ME has leveraged the JLF program to better understand collateral damage effects associated with TBI. In FY22, JLF initiated a project to develop a capability to assess possible TBI risk in different operational environments. JLF reviewed and assessed currently available TBI methodologies and models, conducted combat data analysis in coordination with the Joint Trauma Analysis and Prevention of Injury in Combat program, and awarded a contract to the University of Virginia for the development of TBI risk curves.
- JTCG/ME product training is imperative to the user community. To support this end, JTCG/ME facilitated 40 training classes/events for over 500 students at 27 locations. Training of integrated product capabilities (DIEE/JWS) continues to enable the operational community to successfully employ munitions while minimizing collateral damage.

JTCG/ME Advances the Capability and Accuracy of Weaponeering Tools

JTCG/ME continues to advance the capabilities and accuracy of weaponeering tools to respond to Combatant Command needs in an increasingly complex and dynamic multi-domain operational environment. JTCG/ME upgraded existing capabilities to increase the effectiveness of kinetic strikes and developed new capabilities to enable deliberate and dynamic strikes using cyber, EMS, and DEW capabilities.

Kinetic threat lethal effects are complex phenomena that need to be adequately characterized to credibly predict their effect on the target of interest. Similarly, targets of interest are complex and the lethal effect predictions largely depend on our understanding of the target vulnerabilities.

Collateral Damage Estimates

In FY22, JTCG/ME made progress in improving the DOD's ability to accurately characterize the lethal effects of U.S. weapons. Specifically, JTCG/ME leveraged the multi-year, Enhanced Weaponeering and CDE test program originally

Figure 1. Buried Ordnance Test

initiated by JLF to quantify the lethal effects of munition burial and building debris.

Figure 1 depicts a buried ordnance test, showing the potential collateral damage effects of munitions buried within the ground. Figure 2 shows a multi-sided collateral structure used to assess ground shock and secondary or collateral damage hazards on nearby structures.

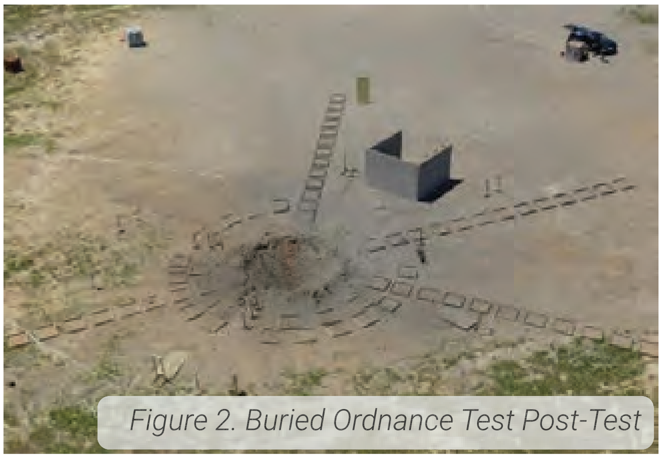


Figure 2. Buried Ordnance Test Post-Test

Figure 3 depicts a building debris test, showing the effects of munitions detonated inside structures.

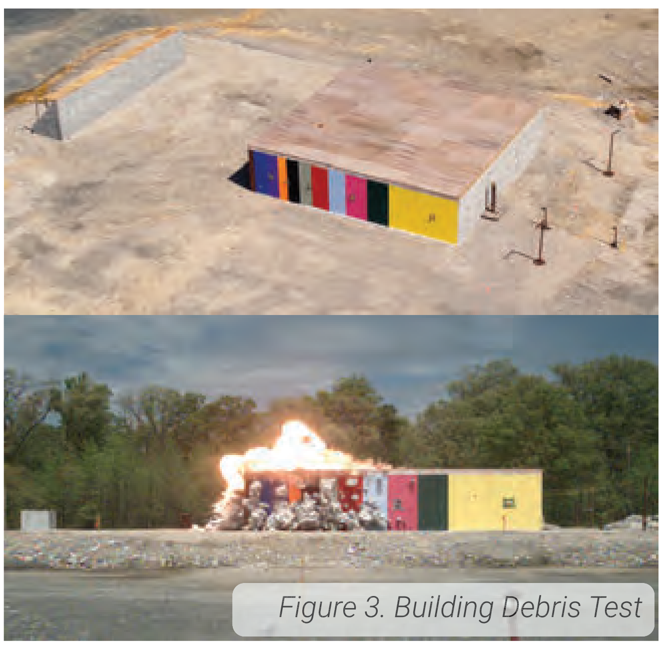


Figure 3. Building Debris Test

Data sets from the Enhanced Weaponeering and CDE test program have been used to improve, verify, and validate high fidelity modeling and simulation (M&S) tools used to predict building debris mass and velocity distributions from multiple structure types, along with crater ejecta, ground shock, and blast pressure for various soil and munition burial configurations. These predictions must be credible since they are the foundation of fast running engineering models used by DIEE and DCiDE to estimate weapon lethality and collateral damage. In FY22, under the Enhanced Weaponeering and CDE test program, JTCG/ME conducted several tests to further the understanding of munition burial and building debris effects on noncombatant personnel and nearby structures. A significant effort is underway to update the weaponeering tools using these newly generated data.

Lethal Effect Estimates

JTCG/ME continues to leverage the Advanced Warhead Characterization project initiated by the JLF program to improve the fidelity of weapons data. In FY22, the program conducted a test series to further validate advances in science and technology that could be used for advanced warhead characterizations. Examples include emerging diagnostics tools (e.g., computed tomography imaging, digital image correlation, x-ray imaging, photon Doppler velocimetry, pressure measurements, and optical fragment tracking) to support efficient data collection and high-fidelity model validation for multiple munitions. Figure 4 shows advanced diagnostic test configuration to support improved fragmentation data with legacy z-data overlay.

The Advanced Warhead Characterization project has gained significant interest throughout the Department of Energy and DOD communities as it advances experimentation, M&S, data fusion, and policy guidance applicable to both Departments. JLF leveraged these successes and adopted the same approach for behind armor debris characterization that results from target/penetrator interaction with ground vehicle armor solutions. This FY22 project is developing credible high-fidelity finite element models of the Behind Armor Debris phenomena and validating it using optical tracking methods to capture fragment characteristics of the debris for use in fast-running vulnerability and lethality engineering models.

In addition, JTCG/ME leveraged the small-scale blast test program initiated by the JLF program to

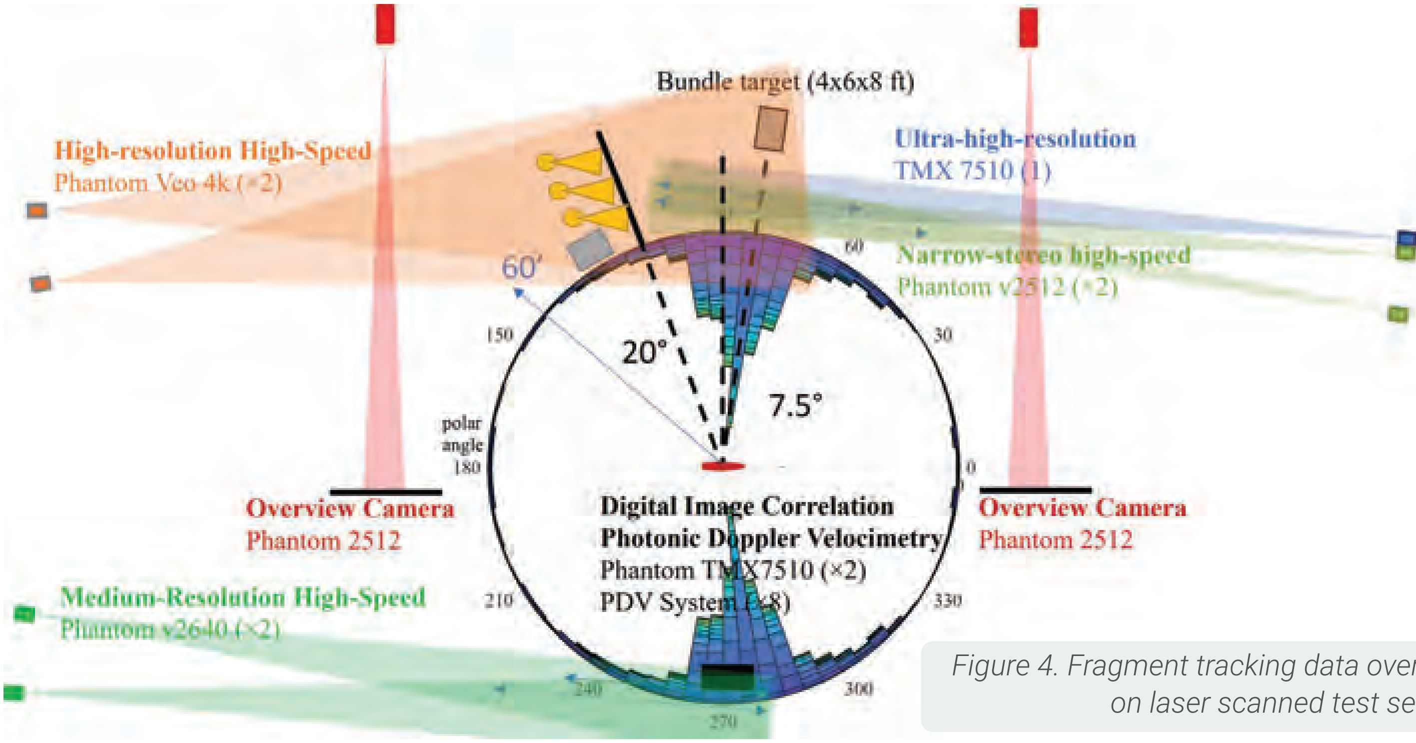


Figure 4. Fragment tracking data overlaid on laser scanned test set-up

provide a tailorable scale target model that will be used to efficiently collect larger volume and higher fidelity lethality data. In FY22, the Air Force Research Laboratory completed the design and fabrication of the test fixture modifications that included a new second-story wing (shown in Figure 5) to include highly non-orthogonal geometry, stairwell, and an elevator shaft, allowing vertical blast propagation across building levels. Blast data generated from tests using this fixture will be used to further update, verify, and validate the blast effects M&S.

In FY22, the JLF program continued to execute the Multiphase Blast Explosive (MBX) weapon system test program designed to increase the capability of weaponeering tools to estimate MBX lethal effects used in low-collateral-damage munitions. This effort is currently pursuing parallel efforts related to weaponeering of MBX against structural targets as a collaborative partnership with the Air Force Research Laboratory, the University of Florida, and Lawrence Livermore National Laboratory, through updated versions of JWS and high-fidelity Arbitrary Lagrangian–Eulerian three-dimensional analysis (ALE3D) modeling of reduced collateral weapons.

Lethal Effect Estimates – Hypersonic Weapons

In FY22, JTCG/ME initiated a new effort focused on addressing lethality evaluation and weaponeering tool shortfalls to include collateral damage effects for hypersonic weapons. The initiative includes

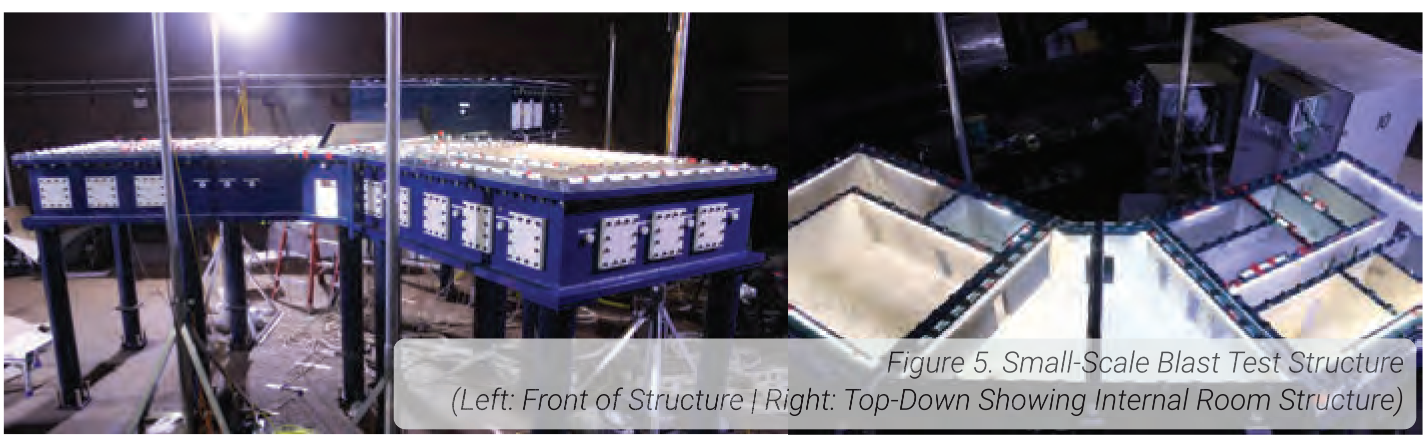


Figure 5. Small-Scale Blast Test Structure (Left: Front of Structure | Right: Top-Down Showing Internal Room Structure)

advancement of high-fidelity M&S comprised of an experimentation program to generate the required validation data. Near-term efforts will account for weapon characterization, including terminal effects, delivery accuracy, and associated data and methodology verification and validation. Calibrated model development is also being executed for capturing the required range of blast phenomena for weapon integration. Parallel efforts will develop fast-running engineering models. This hypersonic initiative will address longer-term hypersonic T&E improvements for broad-ocean-area tests, enabling weapon accreditation with greater granularity at reduced costs and with simplified logistics. Lastly, JLF continues to make progress in luminescent technology development and testing, which will enable optical characterization of fragment dispersion in flight tests in order to adequately evaluate emerging hypersonic weapons.

Lethal Effect Estimates – Maritime Targets

In FY22, JTCG/ME initiated an effort to enhance the ability of DOD weaponeering tools to support the warfighter with credible and timely lethal effects estimates against adversary maritime (surface and subsurface) targets. Current weaponeering capabilities and data sets are either insufficient or non-existent for conventional surface, subsurface, and unconventional small-boat threats, which are capable of conducting attacks against the United States or allies. JTCG/ME leveraged the Maritime Survivability and Lethality Test program initiated by JLF to pursue a cohesive, enterprise-wide strategy that seeks to improve efficiency, collaboration, knowledge sharing, and analytical techniques across maritime organizations. To build on this effort, JTCG/ME has worked on developing weaponeering guides for several maritime targets not currently in JTCG/ME inventory. A prototype of a credible maritime weaponeering analysis tool for surface and subsurface targets was also developed under this effort and will be integrated and fielded in DIEE by December 2023. JTCG/ME will execute a collaborative test program that procures data to close knowledge gaps, improve current analytical tools and methods, and develop advanced M&S tools (e.g., the Advanced Survivability Assessment Program) required to support the delivery and fielding of weaponeering tools against such targets. Other M&S tools that will be advanced as part of this initiative include: Submarine Vulnerable Effects Model, Navy Enhanced Sierra Mechanics, and Dynamic System Mechanics Advanced Simulation. This effort will not only increase weapons systems' lethality against foreign maritime platforms but also will support the delivery of more survivable ships and submarines to the U.S. Navy and the DOD.

M&S Verification and Validation

To further improve confidence in the JTCG/ME M&S efforts, the JLF program held Verification, Validation, and Accreditation (VV&A) and Uncertainty Quantification coordination meetings with the Army, Air Force, Navy, Lawrence Livermore National Laboratory, Los Alamos National Laboratory, and Sandia National Laboratories representatives. VV&A experts presented current techniques, efforts, challenge areas, data gaps, and future development areas to foster potential areas for cross-organizational collaboration, which could improve practices and ensure confidence in JTCG/ME and T&E tools.

Battle Damage Assessment (BDA)

One of the most comprehensive efforts used to verify, validate, and advance the effectiveness of weaponeering tools is tied to a multi-year effort to improve the BDA. The primary benefit of the BDA program is to enable credible post-strike analysis to ensure commander's intent has been achieved. To meet this intent, JTCG/ME continued to collect all BDA data to not only analyze strikes and inform reach-back support, but also to support weaponeering tool verification and validation, training, and expenditure analysis. In FY22, the BDA team developed automated data collection tools and collected data products for tens of thousands of strikes. The data from these strikes will be stored in a Microsoft Azure cloud environment named the Joint Battle Damage Analysis Repository.

As part of the Microsoft Azure Cloud architecture development, the BDA team took the first steps in the development of a virtual environment to provide efficient scalability and agility to enhance processing performance and storage. This environment will allow for the connectivity to DIEE to enable the storage of new strike information through an application programming interface. This will ensure accurate and timely archival of strike reporting in the cloud-based Joint Battle Damage Analysis Repository for future use and reference, and the ability for the user community to interact with the data though a data analytic and mapping user interface.

Data Management

JLF continues to evaluate a framework capable of consolidating available and future LFT&E data in support of data mining and data analytics intended to more effectively inform requirements, performance evaluations, and development of T&E tools. The U.S. Army Combat Capabilities Development Command (DEVCOM) Analysis Center performed a requirements analysis through stakeholder surveys and interviews in the development of a requirements definition document. In FY22, the DEVCOM Analysis Center focused on tracking the development of the Cloud Hybrid Edge-to-Enterprise Evaluation and Test Analysis Suite (CHEETAS), a big data analytics and knowledge management framework developed by the Test Resource Management Center, with the intention to leverage its capabilities to standardize and share LFT&E data. The DEVCOM Analysis Center has continuously collaborated with the CHEETAS development team to both verify and integrate T&E requirements into the software suite's development.

To support data and methodology enhancements discussed above, the JTCG/ME Capabilities and Standardization Integrated Product Team provided repositories for archival, review, approval, and access of data, methodology, and documentation. These 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 tri-Service review and approval processes. This data repository also serves the T&E and Acquisition Community by providing JTCG/ME-approved target vulnerability packages. JARVIS is under consideration to expand support in other focus areas, including directed energy and cyber data.
- For methodology, the Joint Effects Library is a repository of approved models, modules, plug-ins, and methodologies for Capabilities and Standardization Integrated Product Team Technical Working Groups.
- For documentation, the Bugle is a wiki-style website built on Defense Technical Information Center's (DTIC's) DOD Techipedia platform. This approach allows the JTCG/ME to contribute content while maintaining knowledge management. Hosting on DTIC makes JTCG/ME's technical reports, data requests, and model documentation accessible to the DOD community.

These three repositories work in conjunction to provide tri-Service approved munition effectiveness data, methodology, and documentation within JTCG/ME and throughout the DOD.

JTCG/ME Enables Multi-Domain Superiority with DEW, Cyber, and Electromagnetic Spectrum (EMS) Fire Weaponeering Tools

JTCG/ME has made significant progress in supporting the warfighter with weaponeering tools intended to integrate kinetic and non-kinetic fires for optimized mission and lethal effects while mitigating collateral effects to noncombatants, infrastructure, facilities, and equipment. While JTCG/ME has focused on the development and fielding of separate weaponeering tools that can account for DEW, cyber-attacks, and EMS fires, it has also initiated the plans to provide an architecture for a single JMEM capable of estimating the appropriate number and type of both kinetic and non-kinetic weapons required to achieve superiority in a multi-domain operational environment.

DEW

In FY22, JTCG/ME has continued the development of validated Joint Laser Weaponeering Software (JLaWS) and High-Power Microwave (HPM) Weaponeering Software (HPMWS) tools designed

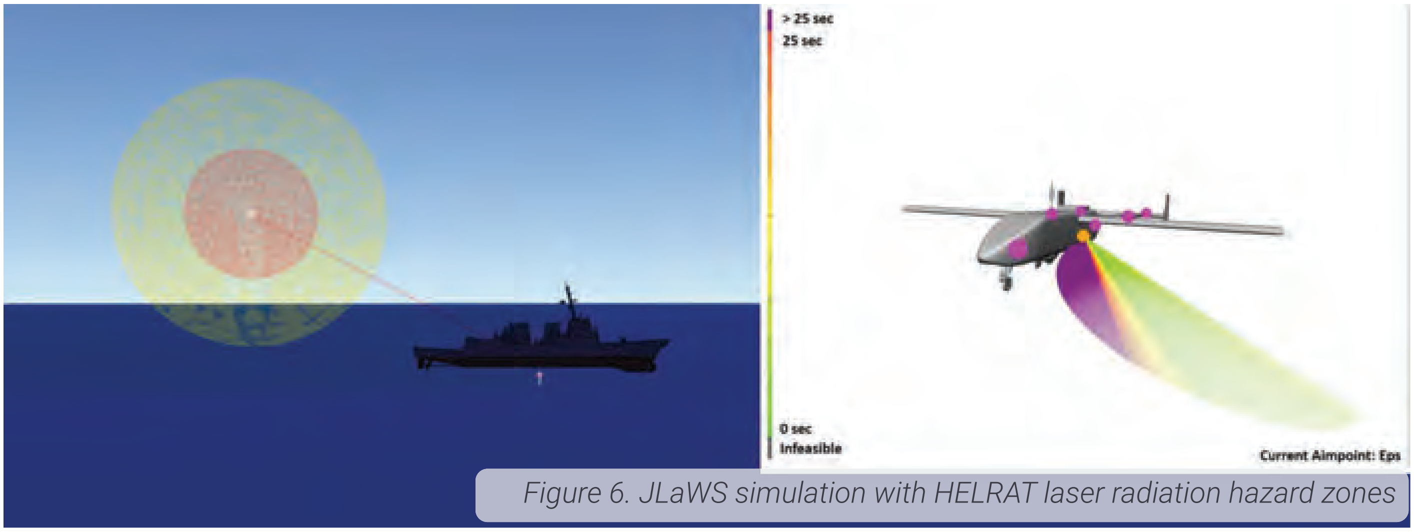


Figure 6. JLaWS simulation with HELRAT laser radiation hazard zones

to enable the Combatant Commands to estimate lethal effects on the target of interest using DEW (either high energy lasers (HEL) or HPM). Specifically, JTCG/ME conducted solid state laser weapon demonstrator testing against various targets and different component materials to collect critical data that were used to provide target vulnerability information. A previous release of JLaWS provides a tool that is accredited for use in functional domains, such as DOD exercises, training scenarios, and weapon system demonstrations. The newest release of JLaWS incorporates the HEL Risk Assessment Tool (HELRAT), a sophisticated software package that provides JLaWS with the ability to graphically portray the zones around a target that contain reflected laser radiation levels that could cause ocular hazards to friendly forces in the area. Figure 6 shows a JLaWS graphical rendering of a ship-based laser weapon system engagement with an unmanned aerial vehicle target – shown on the right – and the spherical zones around the target, as calculated by HELRAT, in which ocular hazards exist.

JLaWS was provided to HEL operators for feedback that will be used to further advance JLaWS utility, establish HEL reach-back support, and continue to advance the development of collateral risk tools for HEL. In the meantime, JTCG/ME supplied operators with JLaWS-developed target cards, which provide lethality estimates based on targeting aimpoints.

JTCG/ME is also developing a threat surrogation tool for use by the Laser Weapon System community, when information is limited or unavailable. The tool will map well matched donors to surrogates.

To advance the development, testing, and fielding of HPMWS (example system shown in Figure 7), JTCG/ME developed HPM lethal effects data standards and analytical tools required to characterize target vulnerability. JTCG/ME also identified and developed M&S tools required to estimate lethality and collateral damage effects due to an HPM engagement, to include a probabilistic risk assessment tools. While DEW tools are being developed in parallel with kinetic tools, users are still leveraging existing JMEM architecture until future integration of these capabilities.

Cyber

In FY22, JTCG/ME continued the development and fielding of JMEM tools intended to estimate cyber effects with a focus on building a DOD user community. These efforts will accelerate the delivery

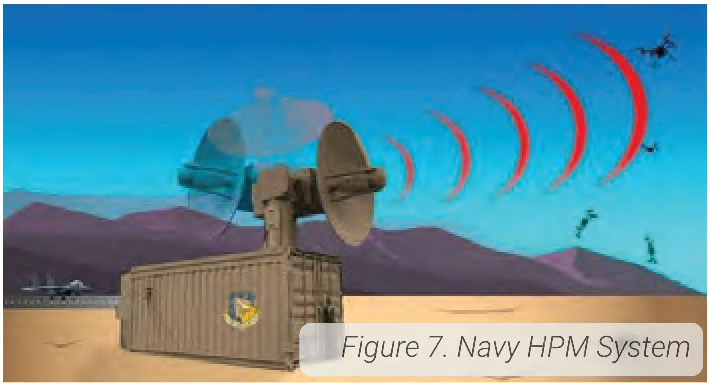


Figure 7. Navy HPM System

of a full-spectrum cyber effectiveness analysis capability for development, testing, and operational engagement. It will enable evaluation of defensive and offensive actions from the weaponeering and T&E perspectives. The Cyberspace Operations Lethality and Effectiveness (COLE) tool and deployment gateway is the foundational product, which enables commanders' operational decisions through advanced analytics used to adequately visualize, plan, evaluate, and assess the full spectrum of cyberspace activities. As shown in Figure 8, the COLE Mission Planning application provides the warfighter with a model that highlights nodes that have been compromised, designated by a hacker icon, and target nodes that are vulnerable (highlighted in red) and potentially accessible (highlighted in blue). Vulnerable nodes that are accessible from the warfighters' location and have a cyber-capability option in the database can hold those target nodes at risk. The state model includes information about the network and nodes such as connectivity, firewall rules, and operational status.

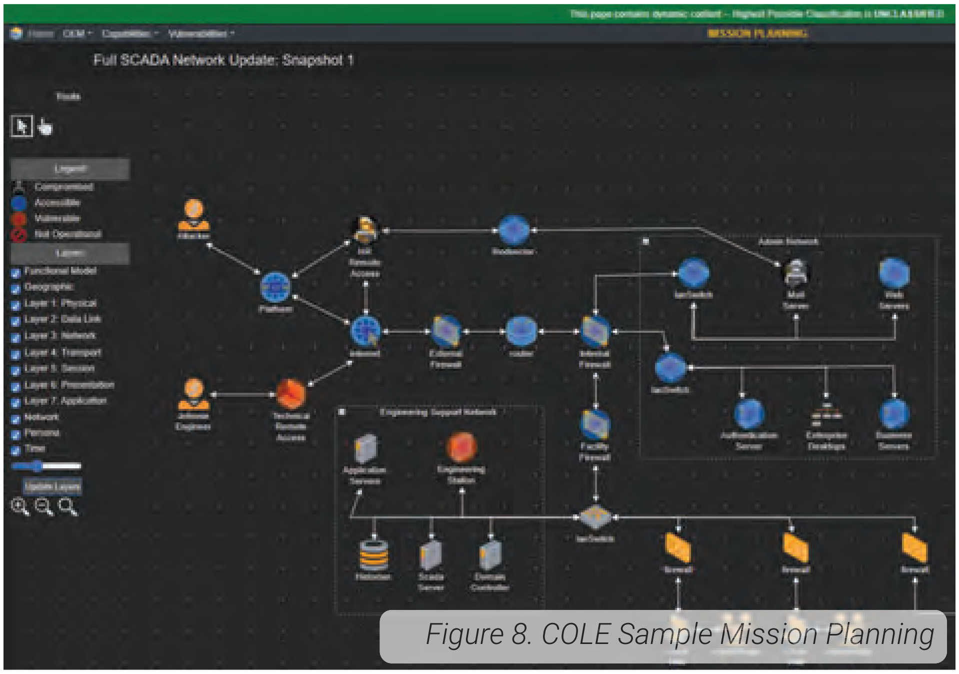


Figure 8. COLE Sample Mission Planning

In FY22, major contributions included completion and enhancements of data standards, demonstration of target vulnerability assessment, attack sequence modeling, effects-based modeling, functional tests, continued fielding across multiple security domains, and numerous engagements throughout the DOD in conducting capability briefings and demonstrations.

JTCG/ME teamed up with the Joint Aircraft Survivability Program to deliver an initial Machine Assisted Exploitability Simulation and Testing for Resilient Operations (MAESTRO) tool via the COLE deployment gateway. MAESTRO is intended to be used for assessment of U.S. platforms in a cyber-contested environment. It enables automated early discovery of system vulnerabilities that can be used to inform and refine cyber survivability T&E.

Additionally, the JLF program continued the Cyber Automated threat Discovery and Vulnerability Evaluation Reinforcement (CADAVER) tool development, which will also be deployed via COLE deployment gateway. CADAVER integrates enhanced vulnerability discovery fuzzing results into COLE/MAESTRO to increase fidelity of attack planning calculations, while adding parallel processing to improve the scale and speed of T&E. These efforts will also leverage artificial intelligence to allow identification of potential vulnerabilities to mitigate cyberattack access points through automated and semi-automated means.

These three programs are intended to deliver to the warfighters and the T&E enterprise the necessary tools to assess cyber effectiveness/vulnerability using tri-service approved data standards and streams. Leveraging technology and lessons learned of these three programs provide consistent, credible data and methodology for both offensive and defensive cyberspace operations.

EMS Fires

In FY22, JTCG/ME continued the development of JMEM and weaponeering tools for EMS fires. The JMEM for EMS fires will estimate electronic attack (EA) effects and the ability of the warfighter to effectively prosecute adversary targets in contested and congested EMS environments. JMEM for EMS fires will allow mission planners and targeteers to assess weapon and combat effectiveness in the presence of adversary EA (e.g., GPS denial and its effect on kinetic weapon guidance systems). It will also estimate the effects of friendly EA capabilities against adversary targets (e.g., jamming), which create a foundation of Joint standard EA effectiveness data and models used across the Joint Targeting Cycle. In FY22, JTCG/ME further refined the program plan, data standards, Capabilities Needs Statement, and the mission area analysis for EA effectiveness, which resulted in a plan to develop an initial set of JMEM capabilities via the Joint EA Prediction tool by 1QFY24.

JTCG/ME Supplies Weaponeering Tools to Support Interoperability with U.S. Allies and Partners

In FY22, JTCG/ME supported the delivery of weaponeering tools, data sets, and training to 22 coalition partners in support of current operations under Foreign Military Sales agreements. This included the release of weapon effectiveness tables, collateral effects radii tables, and advanced target development capabilities to coalition partners to minimize collateral damage and reduce civilian casualties. These efforts directly supported the Presidential Conventional Arms Control Policy to build partner capacity and prevent civilian casualties. A second effort supported information exchange forums via information exchange annexes with coalition partners. These exchanges facilitate collaboration with partners on methodologies and efforts of mutual interest in the area of weapons effectiveness and CDE for both kinetic and non-kinetic weapons. In FY22, a new International Exchange Agreement was finalized to continue weapons effectiveness analytical exchanges and to expand the scope of topics to better represent complex strategic and operational environments.

Joint Test and Evaluation (JT&E)

The Joint Test and Evaluation (JT&E) Program considers emerging technologies and the increasingly complex and dynamic, joint, multi-domain operational environment to plan and execute joint tests intended to deliver non-materiel solutions and enhance the United States' operational effectiveness, suitability, and survivability in combat. The Services and Combatant Commands (CCMD) help identify critical challenges that need to be addressed in their areas of responsibility to maintain superiority across joint, multi-domain operations. The JT&E Program provides operational test and evaluation management and expertise to develop, test, and validate joint solutions, including agile warfighting tactics, techniques, and procedures (TTP), concepts of employment (CONEMP), and concepts of operations (CONOPS). In turn, Services and CCMDs provide leadership and support to the planning and execution of JT&E projects and their successful transition to the warfighter. Given the increased integration and dependencies of platform, network, and command and control solutions across the domains, joint all-domain command and control solutions, and the rise of kill-webs, JT&E's mission and unique focus on system of systems testing is becoming increasingly critical to the Department's strategic objectives. JT&E test techniques, workforce talents, and reach-back are essential to the adequate evaluation of the effectiveness, lethality, suitability, and survivability of operational plans across the CCMDs.

In FY22, the JT&E Program managed three Joint Tests and nine Quick Reaction Tests (QRT). A Joint Test averages about two years in duration and is preceded by a six-month Joint Feasibility Study. QRTs provide a quicker response to urgent joint needs but must focus their objectives to execute within the shortened, one-year schedule.

Joint Tests

Joint Integrated Fire Control – Directed Energy Weapons for Air Defense (JIFC-DAD)

The advancement of adversaries' ballistic and cruise missiles threatens U.S. interests. U.S. Indo-Pacific Command (USINDOPACOM) J8 recognized the benefits of emerging technologies, specifically directed energy weapons (DEW), in improving air defense capabilities against such threats for U.S. joint forces and coalition partners. When employed with existing kinetic systems, DEW may enhance area air defense capabilities and enable commanders to effectively, affordably, and rapidly defeat massed attacks. In January 2021, JT&E initiated the JIFC-DAD Joint Test to deliver a validated CONEMP that optimizes the integration of DEW with kinetic weapon systems and provides a layered defense of critical assets against a mix of wartime air threats. The JIFC-DAD field test event was conducted in July 2022. The results and their effect on the USINDOPACOM mission are documented in a classified report.

Joint Interoperability through Data Centricity (JI-DC)

Data centricity represents a paradigm shift in mission partner information sharing that enables operational information sharing of multiple CCMD missions in one common data-centric environment. Managing a single data-centric environment using attribute-based access control software enables the sharing of information only to authorized users of a specific operation. Not only is this more efficient in resource savings, it supports flexible and timely information sharing with coalition partners to meet dynamic, simultaneous mission requirements. DOD Chief Information Officer recognized the need for more efficient and dynamic information sharing networks at the operational and tactical levels. U.S. Central Command J6 took the lead in developing the hardware and software for the data-centric environment. In parallel, the JI-DC Joint Test focused on developing and testing procedures to administer and operate the environment as a SECRET releasable network with security-enhanced features and data management protocols.

The JI-DC Joint Test conducted three test events with U.S. and coalition warfighters in a simulated target development cycle. These events used a prototype data-centric network to test data sharing procedures and network administration of user permissions and security protocols. Participants distributed across the United States, Canada, Germany, Norway, Sweden, and England used virtual desktops and screen sharing to conduct test trials and collect data for analysis. The results not only demonstrated the ability to access the environment and conduct secure information sharing but also validated the utility and usefulness of the JI-DC TTP to the warfighters and information technology administrators. In October 2021, the JI-DC test products were received by U.S. Central Command for final coordination and distribution. Since project closing, the products have been instrumental in CCMD implementation, network administrator management, and warfighter operation of a data-centric environment called the Collaborative Partner Environment.

Recovery Enhanced by Synchronizing Capabilities to Unify Effects (RESCUE)

Joint forces will face challenges in conducting personnel recovery (PR) in a complex multi-domain, anti-access/area denial (A2/AD) environment without access to employing the full range of all-domain capabilities in today's arsenal. The Joint Personnel Recovery Agency recognized a gap in existing doctrine and identified the need for integration and synchronization of information-related capabilities (IRC) into PR operations. In August 2019, JT&E initiated the RESCUE Joint Test to develop and test a TTP that integrates and synchronizes IRCs with traditional kinetic fires for support and recovery of isolated personnel. The team used data generated from the U.S. Marine Corps Special Operations Command Raven risk reduction event and field testing at KEEN EDGE 22 along with warfighter input to shape the TTP.

The RESCUE TTP enables PR improvements to reduce risk to isolated personnel and recovery forces as well as addresses information operations collaboration across the DOD. The TTP not only improves operations in an A2/AD environment but also integrates all-domain capabilities into PR operations for complex urban scenarios. The RESCUE test product is already being integrated in CCMD standard operating procedures for mission planning and execution. Ultimately, the RESCUE TTP will influence future revisions to PR and IRC training curriculums; Joint Publication 3-50, Personnel Recovery; and Air Land Sea Application Center multi-Service TTP for PR.

Quick Reaction Tests

Assessment of Joint Maritime Mining on USINDOPACOM Operational Plans (AMMO)

Maritime mining is a low-cost and effective means to deny an adversary access to geographic locations and delay their action. U.S. adversaries have advanced their integrated air defense systems and substantially increased risk to the warfighter when deploying mines. USINDOPACOM J8 recognized the need to develop, test, and validate a joint CONEMP to maximize the wartime effect of legacy and advanced maritime mines given the increased risk in their deployment. In April 2021, JT&E initiated the AMMO QRT to develop a CONEMP for near-term and legacy mine capabilities. The objective was to maximize operational and strategic effect within USINDOPACOM operational plans and minimize risk to U.S. forces and coalition partners. The AMMO QRT completed two table top exercises, two rounds of modeling and simulation, and two warfighter advisory working groups. These resulted in the successful test and validation of a Maritime Mining CONEMP as the final product delivered to the warfighter at project completion. Additionally, the AMMO QRT continued to provide critical updates to the Office of the Chief of Naval Operations N81 Capabilities Based Analysis for Maritime Mining through project completion in August 2022.

Integration of Joint Optimization for Electromagnetic Spectrum (EMS) Superiority (I-JOES)

Joint forces are critically dependent on the electromagnetic spectrum (EMS) across all domains and functions. To achieve EMS superiority, USINDOPACOM J8 recognized the need for validated cross-functional TTP that integrates intelligence, electromagnetic warfare, and spectrum management at the component level. In April 2021, JT&E initiated the I-JOES QRT to develop component-level TTP that: 1) incorporates EMS targets and collection requirements into joint targeting or collection cycles, 2) integrates EMS operations into the joint air tasking cycle, and 3) develops component EMS operations plans to feed the CCMD and Joint Task Force Joint Electromagnetic Spectrum Operations. The I-JOES QRT executed two test events, which included a field test at KEEN EDGE 22 in January 2022 and a table top exercise in May 2022. Following project completion in August 2022, the I-JOES TTP transitioned to USINDOPACOM J8 and is actively being used by Pacific Air Forces, U.S. Pacific Fleet, and the Joint Electronic Warfare Center.

Joint Basin-Scale Communications (J-BASC)

U.S. Strategic Command recognized an emerging communications technology that could be integrated within the existing architecture to meet a critical joint force need. In April 2021, JT&E initiated the J-BASC QRT to develop, test, and evaluate the new communications CONOPS that considers this technology. J-BASC QRT conducted field testing in March and May 2022. The results and their effect on the U.S. Strategic Command mission are documented in a classified report.

Joint Discreet Adversary Strategy Defeat (J-DASD)

U.S. Strategic Command J8 recognized the need to apply tailored deterrent strategies for specific adversaries by integrating the full spectrum of U.S. military capabilities, both nuclear and conventional, with elements of U.S. national power. In April 2021, JT&E initiated the J-DASD QRT to develop and test CONOPS that specifically addresses the following areas: 1) integration of strategic deterrence action, 2) development of deterrence options, 3) degrading potential impact of threat actors, 4) executing deterrence operations in a timely manner, and 5) reducing the risk of deterrence failure. The J-DASD QRT conducted a field test at the Power Game event in June 2022 to collect measurements for messaging processes.

Joint Integrated Network – Korea (JIN-K)

U.S. Forces Korea are updating their near real-time, joint/coalition integrated air-ground common operational picture (COP). The update will enhance integration and distribution of sensor and targeting data to mobile and command post sites throughout the theater of operations. Joint Staff J6 recognized the need to develop new TTPs that optimize the benefits of this update and deliver the required joint capabilities within the Combined Enterprise Regional Information Exchange System - Korea network. This will assist modernization of mobile and command post sites throughout the Republic of Korea based on upgraded capabilities to integrate data feeds and targeting sensors into a COP. The TTPs will also include sensor-to-shooter integration guidelines through tactical datalinks to various air/land/sea strike platforms and mobile/command post sites. In January 2021, JT&E initiated the JIN-K QRT to develop, test, and validate such TTPs. The JIN-K QRT conducted field tests in Spring 2022. The validated TTPs will enable warfighters to effectively utilize available data within a COP and retain real-time situational awareness from the tactical through strategic levels. Further, the TTPs will reduce bandwidth consumption and directly contribute to projection of combat power.

Joint Interagency – 5G Radar Altimeter Interference (JI-FRAI)

The Federal Communications Commission reallocated the 3.7–3.98 GHz frequency spectrum to 5G C-band applications in March 2020. Later that year, the Radio Technical Commission for Aeronautics assessed that 5G out-of-band emissions could interfere with civil aircraft radar altimeters (RADALT) operating in the 4.2–4.4 GHz C-band spectrum range. Cellular technology companies disputed the assessment citing discrepancies in bench test models and a lack of operationally realistic live testing. In 2021, the Federal Aviation Administration imposed restrictions on the aviation communities and cellular providers based on the Radio Technical Commission for Aeronautics report findings. The Office of the USD(A&S) and U.S. Transportation Command recognized the need to assess these potential impacts on military systems and develop a test methodology for evaluating 5G C-band interference on military and civil aircraft avionics. In April 2021, JT&E initiated the JI-FRAI QRT to develop and test a combined test methodology for evaluating 5G interference and to provide an initial assessment of 5G interference on selected military RADALT systems.

The JI-FRAI QRT executed a phased test strategy comprised of enhanced bench testing, radio frequency over-the-air testing, and operational flight tests in a real 5G environment. These test activities brought together participants from across the federal government, the commercial aviation community, major cellular service providers, RADALT manufacturers, and government partners. The cooperative nature of the project led to a rapid initial assessment of potential 5G interference on 80 percent of currently used RADALT models onboard manned fixed wing and rotary aircraft. Upon completion in FY22, JI-FRAI delivered a combined test methodology summarizing best practices, lessons learned, operational considerations, resource requirements, and mitigation strategies. The test product will enable expanded testing of 5G interference on other manned and unmanned aircraft avionic systems. The findings and conclusions of the JI-FRAI project enabled DOD to address an issue of national interest and establish a position for ensuring the safety of military aircraft within 5G areas of operation.

Joint Interagency Net-Centric Cross-Domain Risk to Operational Cyber Systems (JINX ROCS)

The Eastern Air Defense Sector (EADS) and Western Air Defense Sector (WADS) rely on a range of radars, interrogators, aircraft transponder systems, and associated datalinks. These are used to generate and transport the operational data underpinning the battlespace situational awareness critical to providing air defense and control in support of the homeland defense mission. DOT&E recognized the need to evaluate cyber risks to EADS/WADS architecture, system, and information for mission assurance. In April 2021, JT&E initiated the JINX ROCS QRT to develop, test, and validate a time-critical TTP enabling detection, response to, and recovery from cyber interference within the data stream and architecture. Additionally, the TTP provides an operational framework and supporting instructions to optimize available sensors to support these activities.

The JINX ROCS QRT implemented a "test-fix-test" approach with the first field test series occurring at EADS/224th Air Defense Group Battle Control Center from December 2021 through February 2022. The project conducted the second field test in May 2022. Analysis of field test data validated that the JINX ROCS-developed TTP improved performance of air defense sector operations and cyberspace personnel detection, response to, and recovery from cyber interference of operational missions. The integrated and enhanced performance gained using the JINX ROCS TTP further enabled air defense sector operators to maintain battlespace situational awareness and "fight through" cyber-contested environments.

Joint Littoral Fire Support Coordination (J-LIFE)

The joint warfighter requires doctrine to deconflict, coordinate, and integrate attacks that include newly fielded capabilities and emerging technologies. USINDOPACOM J8 recognized the need for effective doctrine that minimizes the risk of fratricide, reduces duplication of effort, and assists in shaping the operating environment for land-based fires into the maritime domain. In January 2021, JT&E initiated the J-LIFE QRT to develop and validate TTPs to update existing joint and Service doctrine. These will support the U.S. Marine Corps's Expeditionary Advanced Base Operations and U.S. Army's Multi-Domain Task Force. To meet these objectives, the J-LIFE QRT conducted two field tests. In March 2022, the first field test served to validate the employment of the TTP by fires elements at the tactical level during SPARTAN FURY 22.1. In August 2022, the J-LIFE test team conducted a second field test to monitor identification of hostile maritime tracks through Naval Strike Group planning and coordination in order to execute operational-level land-to-maritime fires during PACIFIC DRAGON 22.

Joint Sustainment in the Littorals – Fuel and Water Distribution (JSL-FWD)

Expeditionary Advanced Base Operations require forces to continue to distribute fuel and water in an evolving A2/AD environment. USINDOPACOM J8 recognized the need for joint CONOPS to enable flexible and resilient logistical supply and sustainment to maintain operations in such an increasingly complex and dynamic environment. In January 2021, JT&E initiated the JSL-FWD QRT to develop, test, and validate a joint CONOPS for agile and scalable expeditionary fuel and water distribution. The focus is on connecting the existing tactical fuel and water distribution systems ashore to locations beyond the high water mark via an over-the-shore connection. The JSL-FWD QRT executed three field test events, which included two table top exercises in March and June 2022 and a live demonstration event in May 2022. Following project completion in August 2022, the CONOPS transitioned to USINDOPACOM J8. It is actively being used by U.S. Marine Corps Forces, Pacific; U.S. Pacific Fleet; and Naval Facilities Engineering and Expeditionary Warfare Center.

Test and Evaluation Threat Resource Activity (TETRA)

Test and Evaluation Threat Resource Activity (TETRA) is a joint duty activity between DOT&E and the Defense Intelligence Agency (DIA), established in 2000, to ensure that OT&E and LFT&E programs, as well as warfighter training, are adequately informed by the latest intelligence data. TETRA is composed of DIA analysts responsible for supplying authoritative and timely intelligence assessments of the current and emerging multi-domain threat environment to the T&E Enterprise. Specifically, TETRA: 1) generates products that include intelligence-based analyses of current and emerging threats, 2) facilitates the acquisition of foreign materiel needed for testing or development of threat surrogates, 3) oversees threat surrogate verification and validation to include threat modeling and simulation (M&S), and 4) leverages emerging science and technologies to project expected threat capabilities. TETRA's position as a threat and intelligence liaison between the acquisition, test, and intelligence communities ensures one-of-a-kind, tailored intelligence support to the T&E Enterprise.

TETRA Executes Intelligence Analysis to Support Credible OT&E and LFT&E

In coordination with the DIA and the Services' Intelligence Production Centers, TETRA conducts independent intelligence research and analysis to generate products required to adequately define scenarios for the evaluation of U.S. weapon systems, equipment, and infrastructure against operationally representative threats and targets. TETRA's products include assessments of order of battle; threat Concept of Operations; and adversary tactics, techniques, and procedures (TTPs) used against U.S. systems. TETRA also supplies the T&E community with threat and target signatures and characteristics, as well as the status (availability, verification, and validation) of threat surrogates required for an adequate OT&E or LFT&E program. For example, in FY22, TETRA:

- Successfully developed analytic exercises and accompanying reports addressing ballistic and hypersonic missile threats to the United States homeland. TETRA led a cooperative effort between the Missile Defense Agency (MDA), DOT&E, OUSD(R&E), OUSD(A&S), and the Intelligence Community (IC), to ensure compliance with a 2021 OUSD(A&S) Acquisition Decision Memorandum and to inform future operational test planning and adequacy assessments for homeland defense systems.
- Initiated the Space Electronic Warfare (EW) and Cyber for T&E Working Group intended to identify space EW and cyber system T&E challenges, gaps, requirements, and investments needed, and to develop recommendations for addressing gaps in intelligence and T&E environments to meet DOD and commercial space platform requirements.
- Updated the assessment of emerging technology threats and changing adversaries' TTPs of tactical, operational, and strategic significance to U.S. ground forces and programs under DOT&E oversight, while making recommendations on threat portrayals focusing on threat capabilities for EW, cyber, navigation warfare improvements, and kinetics from artillery and anti-tank guided munitions.
- Provided IC threat scenario assessments to meet operational test planning objectives. Scenarios defined the adversarial order-of-battle and force laydown, as well command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities for specific areas of responsibility. TETRA's analysis of foreign naval force composition and employment tactics, C4ISR capabilities, and projected trends helped to increase the T&E community's awareness of foreign military systems and to inform threat realism for operational testing.
- Provided specific characteristic and performance data for foreign submarines, and anti-air warfare systems data for foreign naval surface combatants. Improved threat characterization will aid accurate portrayal of foreign capabilities and increase threat realism for operational testing.
- Supplied intelligence assessments of ballistic missile and counter-space threats to inform testing of ballistic, hypersonic, and cruise missile defense systems.
- Identified and coordinated the integration of strategic-level intelligence processes into the arenas of operational testing to inform threat emulation and near real-time intelligence distribution in a near-peer, cyber-contested environment, at every stage of an acquisition program lifecycle.
- Collected and analyzed IC reporting and open source intelligence information to supply cyber threat-specific data and cyber threat intelligence support.

TETRA Facilitates Acquisition of Actual Foreign Threats

OT&E and LFT&E programs benefit greatly from the availability of actual, foreign threat systems either to test U.S. systems against or to reverse engineer the threat or target to support the development of surrogates (either physical or digital).

To secure actual systems for intelligence analysis and use in operational testing, TETRA works directly with the Joint Foreign Materiel Program Office, overseen by the Office of the Under Secretary of Defense for Intelligence and Security. In coordination with the OT&E and LFT&E community, TETRA supplies a prioritized and coordinated list of foreign materiel to support upcoming operational and live fire tests and inform IC collection opportunities. The Joint Foreign Materiel Program is a critical link between the T&E community, DIA, and the Department of State, increasing the visibility of T&E requirements in support of operationally representative testing and warfighter training. Foreign materiel requirements span all warfare areas; TETRA is currently monitoring and coordinating over 100 acquisition efforts. The demand for a wide array of foreign man-portable air-defense systems (MANPADS) continues to be high for: 1) the development of MANPADS surrogates to enable adequate testing of countermeasures (as discussed in the Center for Countermeasures section of this report), 2) representative missile seekers and software for use in hardware-in-the-loop laboratories, and 3) LFT&E to test the vulnerability of U.S. weapon systems when engaged by such a threat. Foreign antitank guided missiles have also been in high demand to support the testing of the evolving Active Protection System employed by ground combat vehicles. GPS jammers have been in demand for testing of GPS-guided weapons, and very high frequency radars have been required for testing of programs such as the F-35.

While TETRA works with the T&E community to develop the foreign materiel priorities for T&E programs, there is a critical need to streamline the acquisition process of foreign materiel when they become available. Foreign materiel availability is unpredictable, and acquisitions are usually lengthy, making it difficult to identify appropriate year funding, resulting in missed opportunities to acquire such systems when they become available. A non-expiring dedicated funding line for foreign materiel acquisitions would mitigate this shortfall.

TETRA Supplies Accredited Threat and Target Models and Surrogates

In the absence of actual foreign threats, which can be difficult to acquire, TETRA supports the T&E community with the intelligence data and analytical expertise required to develop and accredit threat and target surrogates, either physical or digital replicates. In accordance with DOD Instruction 5000.61, and in coordination with the Services' Intelligence Production Centers, TETRA leads DOT&E's Integrated Technical Evaluation and Analysis of Multiple Sources (ITEAMS) projects that evaluate options to build threat-representative simulators and models from intelligence, open source, and industry data. TETRA also developed and continues to maintain the Threat Systems Database, which catalogs threat assets available for the T&E community. ITEAMS projects are critical to adequate OT&E and LFT&E.

TETRA is also responsible for the threat surrogate verification and validation process to assess the uncertainties of the threat surrogate compared to the actual threat system that the warfighter would encounter in combat. To accomplish this, TETRA leads the Threat M&S Working Group Enterprise development of common and authoritative threat models, delivering a threat surrogate verification and validation report, documenting the comparison of the threat representation to intelligence data, noting the differences, and explaining the potential effect of those differences on test adequacy. Threat model development efforts are often stove-piped, proprietary, and single use. TETRA strives to ensure threat M&S is based on an enterprise management process that provides developmental and interoperability standards to enable data correlation with threat models across the T&E spectrum.

In FY22, TETRA provided threat intelligence, validation expertise, and oversight for 14 Joint and Service threat representation validation efforts. These included the Navy's Maritime Survivability Library, the Next-Generation Jammer's efforts to develop a method to validate and certify the radar electronic attack countermeasure M&S suite, and the gap analysis and verification, validation, and accreditation of the Ballistic Missile Defense System ground test. TETRA also continued the development, validation, and delivery of 10 radio frequency and 10 infrared high-priority threat models, as well as 7 high-fidelity, closed-loop, EW-capable, emulative threat models: the Laboratory Intelligence Validated Emulators (LIVE) and the Common High Assurance

Internet Protocol Encryptor Interoperable Manager for Efficient Remote Administration (CHIMERA).

TETRA is also managing the Advanced Satellite Navigation Receiver effort intended to develop a next generation, Time-Space-Position Information Satellite Navigation Receiver test kit that provides high-fidelity and accurate GPS and inertial measurement unit instrumentation characteristics that operate in a highly dynamic environment. This effort meets the needs of new and upcoming near-peer missile autopilots, guidance, and M&S requirements identified during IC and T&E reviews.

TETRA Keeps Pace with Emerging Threats and Targets

TETRA focuses on projections of future technology and intelligence mission data availability to create adequate representation of threat system characteristics and performance. Artificial intelligence (AI), machine learning (ML), deep learning, and neural network capabilities are toolsets that TETRA intends to pursue to analyze variances in the threat characteristics and quickly identify design space parameters responsible for variances in weapon performance. This approach is necessary to enable the DOD to meet the challenges outlined in the 2022 National Defense Strategy given the emergence of the contested space environment and technologies such as cognitive EW systems.

DOD cognitive EW systems are rapidly developing and will soon become intrinsic to DOD air, land, sea, and space combat systems, supplying advanced EW self-protection and electronic attack capabilities to next generation DOD platforms. DOD cognitive EW systems will heavily rely on AI and ML techniques with the cognitive capability required to defeat advanced threat systems. Adversary threat systems are also projected to increasingly use cognitive capability. TETRA has been charged with leading the effort of identifying cognitive EW system T&E challenges and meeting the need for a standardized, reusable cognitive test environment, U.S. and foreign cognitive threat models, and common cognitive tool sets that can be used across a range of developmental and operational T&E activities.

In FY22, TETRA led the early stages of intelligence analysis and provided technical oversight of operational testing of threat AI and cognitive systems. TETRA's expertise on AI systems, autonomous systems, cognitive systems, and ML systems is important for testing of U.S. and allied cognitive EW systems against peer and near-peer cognitive threats. TETRA has provided data/gap analysis and recommendations on the path forward while continuing to facilitate intelligence coordination and collaboration, needed for an executable cognitive EW T&E roadmap.

APPENDIX

Oversight List

DOT&E Oversight List as of September 30, 2022

- 120MM Advanced Multi-Purpose (AMP), XM1147, High Explosive Multi-Purpose with Tracer (HEMP-T)
- 30mm Multi-Function Munition (MFM)
- Abrams M1A1 SA; M1A2 SEP; APS
- AC-130J
- Acoustic Rapid COTS Insertion for SONAR
- Advanced Airborne Sensor
- Advanced Anti-Radiation Guided Missile - Extended Range
- Advanced Arresting Gear
- Advanced Field Artillery Tactical Data System (AFATDS) Version 7
- Advanced Pilot Training
- Advanced Reconnaissance Vehicle (ARV)
- Advanced Threat Detection System
- AEGIS Modernization (Baseline Upgrades)
- AEHF - Advanced Extremely High Frequency (AEHF) Satellite Program
- Aerosol and Vapor Chemical Agent Detector
- AH-64E Apache Remanufacture/New Build
- AIM-120 Advanced Medium Range Air-to-Air Missile
- AIM-260A Joint Advanced Tactical Missile
- AIM-9X Block II Sidewinder
- Air and Missile Defense Radar (AMDR) / AN/SPY-6
- Air Force Integrated Personnel and Pay System (AF-IPPS)
- Air Force Intercontinental Ballistic Missile Fuze Modernization
- Air Force Maintenance, Repair and Overhaul Initiative (MROi)
- Air Force Next Generation Air Dominance
- Air Operations Center Weapon System Modifications
- Air Warfare Ship Self Defense Enterprise
- Air-Launched Rapid Response Weapon
- Amphibious Combat Vehicle (ACV) Family of Vehicles (FoV)
- AN/AQS-20X Minehunting Sonar and Tow Vehicle (all variants)
- AN/TPQ-53 Counterfire Target Acquisition Radar
- Armed Overwatch
- Armored Multipurpose Vehicle (AMPV)
- Army Contract Writing System
- Army Mobile Wheeled Howitzer (AMWH)
- Assault Breaching System Coastal Battlefield Reconnaissance and Analysis System (all variants)
- B-21 Long Range Strike Bomber
- B-52 Commercial Engine Replacement Program (CERP)
- B-52 Radar Modernization Program (RMP)
- B61 Mod 12 Life Extension Program Tailkit Assembly
- Barracuda Mine Neutralization System
- Bradley ECP; MOD; APS
- Cannon Delivered Area Effects Munitions (C-DAEM) Armor (Inc 1)
- Cannon-Delivered Area Effects Munitions (C-DAEM) Dual Purpose Improved Conventional Munition (DPICM) Replacement (Inc 2)
- Capability Set 21/23 Integrated Tactical Network - Rapid Fielding
- CH-47F Modernized Cargo Helicopter
- CH-53K King Stallion
- CMV-22 Joint Services Advanced Vertical Lift Aircraft - Osprey -- Carrier Onboard Delivery (COD)
- *Columbia* Class SSBN - including all supporting PARMs
- Command Post Computing Environment/ Tactical Services Infrastructure
- Common Infrared Countermeasures (CIRCM)

DOT&E Oversight List as of September 30, 2022

- Consolidated Afloat Networks and Enterprise Services
- Conventional Prompt Strike
- Cooperative Engagement Capability (CEC)
- Cooperative Engagement Capability Increment II
- CVN-78 - *GERALD R. FORD* CLASS Nuclear Aircraft Carrier
- DDG 1000 - *ZUMWALT* CLASS Destroyer and associated PARMs
- DDG 51 Flight III and associated PARMS
- Deep Space Advanced Radar Capability
- Defense Enterprise Accounting & Management System
- Defense Enterprise Office Solution (DEOS)
- Defense Medical Information Exchange (DMIX)
- Defense Security Assistance Management System (DSAMS BLK III)
- Deliberate and Crisis Action Planning and Execution Segments (DCAPES) Inc. 2B
- Digital Modernization Strategy (DMS) – Related Enterprise Information Technology Initiatives
- Dismounted Assured Positioning, Navigation, and Timing System (DAPS)
- Distributed Aperture Infrared Countermeasure
- Distributed Common Ground System - Army (DCGS-A)
- Distributed Common Ground System - Navy (DCGS-N)
- DoD Healthcare Management System Modernization (DHMSM)
- Dry Combat Submersible (DCS)
- E-2D Advanced Hawkeye
- EA-18G - Airborne Electronic Attack
- EC-37B Compass Call Rehost
- Electro-Magnetic Aircraft Launching System
- Electronic Warfare Planning and Management Tool (EWPMT)
- Enhanced Polar System
- Enterprise Air Surveillance Radar
- Enterprise Business Systems Convergence
- Evolved Sea Sparrow Missile Block 2
- Evolved Strategic Satellite Communications
- Extended Range Cannon Artillery (ERCA)
- EXTRA LARGE UNMANNED UNDERSEA VEHICLE (XLUUV)
- E-XX (Take Charge and Move Out) Recap
- F/A-18E/F Super Hornet Aircraft
- F-15 Eagle Passive Active Warning Survivability System
- F-15EX
- F-16 Radar Modernization Program
- F-22 - RAPTOR Advanced Tactical Fighter Aircraft
- F-22 Capability Pipeline
- F-35 - Lightning II Joint Strike Fighter (JSF) Program
- Family of Advanced Beyond Line-of-Sight Terminals
- Family of Advanced Beyond Line-of-Sight Terminals Force Element Terminal
- Family of Medium Tactical Vehicles A2 (FMTV A2)
- FFG(62) Guided Missile Frigate
- Future Long Range Assault Aircraft MTA
- Future Operationally Resilient Ground Evolution Rapid Prototype
- Future Vertical Lift (FVL) Future Unmanned Aircraft System (FUAS)
- Geosynchronous Space Situational Awareness Program
- Global Command & Control System - Joint (GCCS-J)
- Global Positioning System (GPS) Enterprise Oversight
- Global Positioning System III
- GPS III Follow-on Production

DOT&E Oversight List as of September 30, 2022

- 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
- Handheld, Man pack, and Small Form Fit (including Handheld and Manpack components)
- HH-60W Jolly Green II
- Hypersonic Attack Cruise Missile
- Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs)
- Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs)
- Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs)
- Improved High Explosive Dual Purpose 40mm Cartridge
- Improved Turbine Engine Program (ITEP)
- Indirect Fire Protection Capability Increment 2 - Intercept (IFPC Inc 2-I)
- Infantry Squad Vehicle (ISV)
- Infrared Search and Track
- Integrated Air and Missile Defense
- Integrated Personnel and Pay System-Army Increment 2
- Integrated Strategic Planning and Analysis Network Increment 5
- Integrated Tactical Network - Rapid Prototyping
- Integrated Visual Augmentation System (IVAS) Rapid Prototyping
- Integrated Visual Augmentation System Rapid Fielding
- Javelin Antitank Missile System - Medium
- Joint Air-to-Ground Missile (JAGM)
- Joint Air-to-Surface Standoff Missile
- Joint Air-to-Surface Standoff Missile Weapon Data Link
- Joint Assault Bridge (JAB)
- Joint Battle Command Platform (JBC-P)
- Joint Biological Tactical Detection System
- Joint Cyber Warfighting Architecture - Unified Platform
- Joint Light Tactical Vehicle Family of Vehicles
- Joint Operational Medicine Information Systems
- Joint Regional Security Stack (JRSS)
- KC-46A Tanker Modernization
- Key Management Infrastructure (KMI)
- Large Displacement Unmanned Undersea Vehicle (LDUUV)
- Large Unmanned Surface Vehicle
- LAV (NAVY)
- LGM-35A Sentinel
- LHA 6 Flt 0 and associated PARMs
- LHA 8 Flt I and associated PARMs
- Light Amphibious Warship
- Limited Interim Missile Warning System
- Littoral Combat Ship (LCS) Anti-submarine Warfare (ASW) Mission Package
- Littoral Combat Ship (LCS) Mine-countermeasures (MCM) Mission Package
- Littoral Combat Ship (LCS) Surface Warfare (SUW) Mission Package
- Littoral Combat Ship (LCS), FREEDOM and INDEPENDENCE Variant Seaframes
- Long Range Hypersonic Weapon (LRHW)
- Long Range Stand Off Weapon
- Lower Tier Air and Missile Defense Sensor
- LPD 17 Flt II
- M88A2 Heavy Equipment Recovery Combat Utility Lift Evacuation System
- Maneuver-Short Range Air Defense
- Massive Ordnance Penetrator Modification
- Medium Unmanned Surface Vehicle

- MH-139A Grey Wolf
- milCloud
- Military Global Positioning System (GPS) User Equipment Increment 1
- Military GPS User Equipment Increment 2 Miniature Serial Interface
- Military Personnel Data System
- Missile Defense System
- Mission Partner Environment (MPE)
- MK 48 ADCAP COMMON BROADBAND ADVANCED SONAR SYSTEM
- Mk 54 torpedo/MK - 54 VLA/MK 54 Upgrades Including High Altitude ASW Weapon Capability (HAAWC)
- Mk21A Reentry Vehicle
- Mobile Advanced Extremely High Frequency Terminal
- Mobile Protected Firepower
- Mobile User Objective System
- Mounted Assured Positioning, Navigation, and Timing System (MAPS)
- Mounted Mission Command - Software
- Mounted Mission Command-Transport (MMC-T)
- MQ-25 Stingray
- MQ-4C Triton
- MQ-8 Fire Scout Unmanned Aircraft System
- Multi-Function Electronic Warfare
- Multi-Functional Information Distribution System
- MV-22 Joint Services Advanced Vertical Lift Aircraft - Osprey
- National Background Investigation System
- Naval Integrated Fire Control - Counter Air (NIFC-CA) From the Air
- Naval Maintenance, Repair and Overhaul Solution
- Naval Operational Supply System
- Navy Personnel and Pay System
- Next Generation Jammer - Mid-Band
- Next Generation Jammer Low Band
- Next Generation Operational Control System
- Next Generation Overhead Persistent Infrared Space
- Next Generation Squad Weapons Rapid Prototyping (NGSW RP)
- Nuclear Planning and Execution System
- Offensive Anti-Surface Warfare Increment 1 (Long Range Anti-Ship Missile)
- Offensive Anti-Surface Warfare, Increment 2 (Air and Surface Launch)
- Optionally Manned Fighting Vehicle
- Over The Horizon Weapon System
- Paladin/FASSV Integrated Management (PIM)
- Patriot Advanced Capability 3
- Precision Guidance Kit Family of Fuzes
- Precision Strike Missile (PrSM)
- Presidential and National Voice Conferencing Integrator
- Protected Tactical Enterprise Service
- Protected Tactical SATCOM
- Public Key Infrastructure (PKI) Inc. 2
- Robotic Combat Vehicle-Light (RCV-(L))
- Rolling Airframe Missile Block 2
- RQ-7B Shadow Tactical Unmanned Aircraft System
- SBIRS - Space-Based Infrared System Program
- SF - Space Fence
- Ship Self Defense System (SSDS)
- Ship to Shore Connector
- Small Diameter Bomb Increment II
- Soldier Protection System
- Space Based Infrared System (SBIRS) Survivable and Endurable Evolution (S2E2)
- Space Command and Control
- Stand In Attack Weapon
- Standard Missile 2 (SM-2) including all mods

DOT&E Oversight List as of September 30, 2022

- Standard Missile-6 Including all mods and variants
- Stryker Family of Vehicles to include all variants (including NBCRV)
- Submarine Torpedo Defense System (Sub TDS) including Next Generation Countermeasure System (NGCM)
- Surface Electronic Warfare Improvement Program Block 2
- Surface Electronic Warfare Improvement Program Block 3
- Surface Mine Countermeasures Unmanned Undersea Vehicle (SMCM UUV)
- Surface Navy Laser Weapon System
- Survivable Airborne Operations Center E-4B Recap
- Tactical Intelligence Targeting Access Node
- Tactical Tomahawk Modernization and Enhanced Tactical Tomahawk (Maritime Strike) (includes changes to planning and weapon control system)
- T-AO 205 *John Lewis* Class Fleet Replenishment Oiler
- Teleport, Generation III
- Terrain Shaping Obstacles (TSO)
- Terrestrial Layer System (TLS)
- Theater Medical Information Program - Joint Increment 2
- Three-Dimensional Expeditionary Long-Range Radar
- Tranche 1 Transport Layer
- Trident II (D-5) Sea-Launched Ballistic Missile
- UH-60M Black Hawk Helicopter
- UH-60V Black Hawk Digital Cockpit
- Unified Network Operations (UNO)
- Unmanned Influence Sweep System (UISS) include Unmanned Surface Vessel (USV) and Unmanned Surface Sweep System (US3)
- VC-25B
- VH-92A Presidential Helicopter
- *VIRGINIA* Class SSN 774 and associated PARMS
- Weather Satellite Follow-on (WSF)
- Wide Area Surveillance
- XM1170 30x173mm Armor Piercing, Fin Stabilized, Discarding Sabot with Trace

DOT&E Activities

Table 1. FY22 DOT&E Reports to Congress

Program	Date
Early Fielding Reports (EFRs)	
Dismounted Assured Positioning, Navigation, and Timing System (DAPS) Operational Assessment EFR	January 2022
Evolved Sea Sparrow Missile (ESSM) EFR	September 2022
Integrated Tactical Network (ITN) Capability Set 21 Rapid Fielding Report	January 2022
Joint Operational Medicine Information Systems (JOMIS) Medical Common Operating Picture (MedCOP) EFR	September 2022
Mk 54 Mod 1 Inc 1 EFR	June 2022
Standard Missile 6 (SM-6) Future Capabilities Demonstration EFR	December 2021
Follow-on Operational Test and Evaluation (FOT&E) Reports	
Amphibious Combat Vehicle - Command and Control (ACV-C) Combined Operational Test and Live Fire FOT&E Report	March 2022
CMV-22B Joint Services Advanced Vertical Lift Aircraft - Osprey – Carrier Onboard Delivery (COD) FOT&E and LFT&E Report	June 2022
Command Post Computing Environment (CPCE) Increment 1 FOT&E Report	December 2021
High Altitude ASW Weapon Capability (HAAWC) FOT&E Report	July 2022
Stryker Common Remotely Operated Weapons Station – Javelin (CROWS-J) FOT&E Report	November 2021
Tomahawk Weapon System Navigation/Communications Modernization Recertification (NAVCOMM Modernization) FOT&E Report	October 2021
Updated Public Key Infrastructure (PKI) Increment 2 FOT&E Report	November 2021
Initial Operational Test and Evaluation (IOT&E) Reports	
Electronic Warfare Planning and Management Tool (EWPMT) IOT&E Report	May 2022
Independence-Variant Littoral Combat Ship (LCS) Surface Warfare (SUW) Mission Package (MP) INC 3 IOT&E Report	May 2022
Infantry Squad Vehicle (ISV) IOT&E Report	December 2021
Joint Air-to-Ground Missile (JAGM) IOT&E II Report	July 2022
Mk 48 Mod 7 Heavyweight Torpedo Advanced Processing Build (APB) 5 IOT&E Report	April 2022
Unmanned Influence Sweep System (UISS) IOT&E Report	June 2022
Wide Area Surveillance (WAS) IOT&E Report	October 2021

Table 1. FY22 DOT&E Reports to Congress

Program	Date
Operational Assessment (OA) Reports	
Integrated Visual Augmentation System (IVAS) Soldier Touch Point 5 (STP5) OA	June 2022
Live Fire Test and Evaluation (LFT&E) Reports	
Family of Medium Tactical Vehicles (FMTV) A1P2 Underbody Armor Kit (UAK) Upgrade LFT&E Report	November 2021
Joint Assault Bridge (JAB) Follow-on LFT&E Report	June 2022
M1158 Advanced Armor Piercing (ADVAP) 7.62 x 51-mm Cartridge LFT&E Report	October 2021
Special Reports /Responses	
Assessment of the Programs Selected for Development and Implementation of Digital Technologies for Survivability and Lethality Testing Special Report	July 2022
Certification of the Department of Defense's and Services' Funding of Test Infrastructure, Assets, and Personnel to Support Agreed Upon Test and Evaluation Master Plans for Major Defense Acquisition Programs and Test Assessments for Prototyping Programs	July 2022
Defensive Cyber Operations (DCO) FY14-20 Cyber Assessment Program (CAP) Report	December 2021
Digital Twin Assessment, Agile Verification Processes, and Virtualization Technology Special Report	July 2022
DOD COVID-19 Personal Protective and Diagnostic Test Equipment Evaluation Report	January 2022
DOT&E Update FY22 Additional Resources Spend Plan	June 2022
F-35A and A-10C Comparison Test Report	February 2022
FY22 DOT&E Certification and Risk Assessment of Test Strategies for Air Force, Army, Navy and United States Special Operations Command Middle Tier Acquisition (MTA) (804) and Accelerated Acquisition Programs	March 2022
Integrated Visual Augmentation System (IVAS) FY21 Special Interest Report	September 2022
Limitation on the Transfer of Certain Operational Flight Test Events and Reductions in Operational Flight Test Capacity Special Interest Report	September 2022
Self Defense Test Ship (SDTS) Congressional Response	April 2022
T&E Center of Excellence for Software and Cyber – Implementation Plan	July 2022
USS *Gerald R. Ford* (CVN 78) – Air Warfare Self-Defense Interim Assessment	April 2022
Ballistic Missile Defense System Report	
Missile Defense System (MDS) Annual Assessment	February 2022

Table 2. FY22 DOT&E Reports Not Sent to Congress

Program	Date
Operational Assessment (OA) Reports	
Joint Light Tactical Vehicle (JLTV) Utility Fires Variant OA Report	December 2021
Mobile Protected Firepower (MPF) Limited User Test Report – Black Vendor	April 2022
Mobile Protected Firepower (MPF) Limited User Test Report – Gold Vendor	April 2022
Mounted Assured Positioning, Navigation, and Timing System (MAPS) OA	February 2022
Operational Test and Evaluation Report	
Army Limited Interim Missile Warning System (LIMWS) Interim Report	May 2022
Special Reports/Responses	
Cybersecurity Assessment Report for U.S. Special Operations Command (SOCOM) FY20-21	July 2022
FY19-21 Navy Cybersecurity Assessment Report	December 2021
Internet Access Point (IAP) Assessment Report	March 2022
U.S. Central Command (USCENTCOM) FY20-21 Cyber Readiness Campaign (CRC) Report	August 2022
U.S. Indo-Pacific Command (USINOPACOM) FY20-21 Cyber Assessment Report	May 2022

Table 3. FY22 DOT&E-Approved Test and Evaluation Master Plans (TEMPs) and Test Strategy Documents (Live Fire test strategies marked with an *)

Program Document	LF
Acoustic Rapid COTS Insertion (A-RCI) Advanced Processing Build (APB) 17/19 TEMP	
Aerosol Vapor Chemical Agent Detector TEMP[1] Update	
AGM-88G Advanced Anti-Radiation Guided Missile Extended Range (AARGM-ER) TEMP Appendix C Cybersecurity Test Strategy Update	
CVN 78 Gerald R. Ford-Class Nuclear Aircraft Carriers and Advanced Arresting Gear TEMP, Test and Evaluation Identification Numbers 1610 and 1686 Rev A[2]	*
DDG 51 Flight III, Aegis BL 10, and AMDR (AN/SPY-6(V)1) TEMP	*

1 Memo includes approval of Operational Test Plan (OTP) for the Aerosol and Vapor Chemical Agent Detector Operational Assessment (AVCAD OA)

2 Includes two TEMPs signed out in one approval memo

Table 3. FY22 DOT&E-Approved Test and Evaluation Master Plans (TEMPs) and Test Strategy Documents (Live Fire test strategies marked with an *)

Program Document	LF
Distributed Common Ground System – Navy (DCGS-N) TEMP	
E-2D Advanced Hawkeye TEMP	
Enhanced Polar System – Recapitalization TEMP Annex	
Evolved Sea Sparrow Missile (ESSM) Block 2 TEMP	*
F-15 EPAWSS DP 2 TEMP	
Family of Medium Tactical Vehicles (FMTV) A2 TEMP Version 5.0	*
Ground Based Strategic Deterrent (GBSD) Post MS B ERB TEMP	*
High-Altitude Anti-Submarine Warfare Weapon Capability (HAAWC) TEMP	
Integrated Tactical Network (ITN) Capability Set 23 (CS23) Test & Evaluation Strategy (TES)	
Integrated Visual Augmentation System (IVAS) Program Evaluation Strategy (PES)	
Joint Air-to-Ground Missile (JAGM) System TEMP	*
Joint Operational Medicine Information Systems (JOMIS) Overarching Test and Evaluation Program Strategy	
Long Range Stand Off Weapon MS-B TEMP Update	
Miniature Air-Launched Decoy – Navy (MALD-N) TEMP	
MK 48 Torpedo MOD 7 Heavyweight Undersea Weapons Improvements Increment I APB 5+ Upgrades Joint TEMP Addendum	
Mobile Protected Firepower (MPF) TEMP	*
Mounted Assured Positioning, Navigation, and Timing System (MAPS) TEMP	
MQ-8C Fire Scout SUW Increment II TEMP	
Protected Tactical Satellite (PTS) Test and Evaluation Strategy	
Ship to Shore Connector Class Program TEMP Revision A. Change 2	*
Stryker Nuclear, Biological, Chemical, and Radiological Reconnaissance Vehicle (NBCRV) Sensor Suite Upgrade (SSU) Engineering Change Proposal (ECP) TEMP *	*
UH-60V Black Hawk Utility Helicopter Fleet TEMP	

Table 4. FY22 DOT&E-Approved Test Plans

Program Document
Acoustic Rapid COTS Insertion (A-RCI) APB-19 OT Test Plan
Advanced Airborne Sensor (AAS) FOT&E Test Plan
Aerosol and Vapor Chemical Agent Detector (AVCAD) OA Operational Test Plan (OTP) Appendix C Navy Testing Change
Aerosol and Vapor Chemical Agent Detector (AVCAD) OA Operational Test Plan (OTP)[1]
AIM-120 System Improvement Program-3F (SIP-3F) Test Plan
AIM-120D System Improvement Program-3 (SIP-3) Test Deviation Memo
America (LHA 6) Class Amphibious Assault Ship F-35B - Heavy FOT&E (OT-D1) Test Plan
Amphibious Combat Vehicle Command and Control Variant (ACV-C) Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan
Amphibious Combat Vehicle Command and Control Variant (ACV-C) Operational Test Plan (OTP)
Armored Multipurpose Vehicle (AMPV) Initial Operational Test (IOT) Operational Test Plan (OTP)
Army Integrated Air and Missile Defense (AIAMD) IOT&E Plan
Army Integrated Air and Missile Defense (AIAMD) IOT&E Plan Change
Army Integrated Air and Missile Defense (AIAMD) Test Plan Change
CH-47F Cargo Helicopter (Block I) Cooperative Vulnerability Penetration Assessment (CVPA) Test Plan
CH-53K King Stallion Cyber Survivability Test Plan OPTEVFOR (1683-OT-C1)
Close Terrain Shaping Obstacle, XM204 Top Attack System Adversarial Assessment (AA) Operational Test Plan (OTP)
CVN 78 Aircraft Launch and Recovery Equipment Systems Cyber Test Plan
CVN 78 Combat System Operational Rehearsal Event (CSORE) Integrated Test Data Collection Plan
DDG 1000 IOT&E Test Plan
Defense Health Modernization System (DHMS) Revenue Cycle Expansion Operational Assessment
Dismounted Assured Position, Navigation, Timing System (DAPS) Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan

1 Memo includes approval of the Changes to the Approved Aerosol Vapor Chemical Agent Detector TEMP

Table 4. FY22 DOT&E-Approved Test Plans

Program Document
Distributed Common Ground Systems – Army (DCGS-A) CD2 Adversarial Assessment (AA) Plan
Dry Combat Submersible (DCS) IOT&E Test Plan Change
E-2D Delta Systems Software Configuration 4 (DSSC-4) DCP Extension Memo
E-2D Delta Systems Software Configuration 4 (DSSC-4) Integrated Testing Data Collection Plan
F/A-18E/F Block III System Configuration Set (SCS) H16 FOT&E Plan
F/A-18E/F SCS H16 FOT&E Test Plan Live Fire Events
F/A-18E/F Subsequent Software Configuration Set (SCS) H16 Test Period
F-15EX IOT&E Test Plan
F-16 RMP FDE Test Plan
F-22 IMIS AA Test Plan
F-22 R2 OFP Test Plan
FFG(62) Guided Missile Frigate Early Operational Assessment (EOA) Test Plan
HH-60W IOT&E Plan
High-Altitude Anti-Submarine Warfare Weapon Capability (HAAWC) Operational Test Plan (OTP)
Integrated Tactical Network Cooperative Vulnerability and Penetration Assessment (CVPA) Test Plan
Integrated Visual Augmentation System (IVAS) Operational Demonstration (Ops Demo) Operational Test Plan (OTP)
Joint Air-To-Ground Missile (JAGM) Cyber Survivability Test Plan for approval
Joint Air-To-Ground Missile (JAGM) System IOT&E Test Plan; COMOPTEVFOR 3980 (1780-OT-C1)
Joint Common Access Platform (JCAP) Adversarial Assessment (AA) Plan
Joint Common Access Platform (JCAP) Cooperative Vulnerability Penetration Assessment (CVPA) Test Plan
Littoral Combat Ship (LCS) *Freedom*-Class Surface Warfare Mission Package Cyber Survivability Test Plan
Littoral Combat Ship (LCS) Mine Countermeasure (MCM) Mission Package IOT&E Test Plan

Table 4. FY22 DOT&E-Approved Test Plans

Program Document
Littoral Combat Ship (LCS) Mine Countermeasure (MCM) USV + Mine Hunt IOT&E Test Plan
Long Range Anti-Ship Missile Increment 1.1 Quick Reaction Assessment Test Plan
Miniature Air-Launched Decoy – Navy (MALD-N) Cyber Test Plan
Miniature Air-Launched Decoy – Navy (MALD-N) OA Test Plan
Missile Defense System (MDS) Integrated Master Test Plan (IMTP) v23.0
Missile Defense System (MDS) Integrated Master Test Plan (IMTP) v23.1
Multifunctional Information Distribution System (MIDS), Joint Tactical Radio System (JTRS), Tactical Targeting Network Technology (TTNT) Cyber Test Plan
National Background Investigative Services (NBIS) Cyber Test Plan
Over the Horizon Weapons System/Naval Strike Mission (OTHWS/NSM) Cyber Test Plan
Patriot Post Deployment Build 8.1 Adversarial Assessment (AA) Operational Test Plan (OTP)
Patriot Post Deployment Build-8.1 Limited User Test (PDB–8.1 LUT) Operational Test Plan (OTP)
Presidential National Voice Conferencing CVI/CVPA Multi-Service Test Plan Cybersecurity Annex
Ship to Shore Connector (SSC) Cybersecurity IOT&E Plan
SM-2 Block IIIC QRA Test Plan
Stryker Nuclear Biological Chemical Reconnaissance Vehicle (NBCRV) Sensor Suite Upgrade (SSU) Modification Work Order (MWO) Biological Aerosol Sensor (BAS) Component DT/OT Detailed Test Plan
Stryker Nuclear Biological Chemical Reconnaissance Vehicle (NBCRV) Sensor Suite Upgrade (SSU) Modified Work Order of the improved Mobile Chemical Agent Detector (IMCAD) Component DT/OT Detailed Test Plan
Stryker Nuclear Biological Chemical Reconnaissance Vehicle (NBCRV) Sensor Suite Upgrade (SSU) of the Vehicle Integrated Platform Enhanced Radiation (VIPER) Unit and Mounted Enhanced Radiac Long-Range Imagine Network (MERLIN) Component Level Testing, Engineering Change Proposal DT/OT Detailed Test Plan
TRIDENT II D5 Life Extension (D5LE) Commander Evaluation Test-4 (CET4) Flight Test Support Plan
UH-60V Adversarial Assessment (AA) Operational Test Plan (OTP)
UH-60V Black Hawk Utility Helicopter Initial Operational Test (IOT) 2 Operational Test Plan (OTP)
Unified Platform (UP) Caspian Pigeon Big Data Platform (BDP) Cybersecurity Assessment Plan
USS *Gerald R. Ford* IOT&E approval for August at-sea period

Table 4. FY22 DOT&E-Approved Test Plans

Program Document
USS Gerald R. Ford IOT&E Test Plan
VH-92A Presidential Helicopter FOT&E (OT-D1) Plan
XM204 Top Attack System Operational Assessment (XM204 OA) 2022-OA-MSS-CTSOB-I1987 Operational Test Plan (OTP)

Table 5. FY22 DOT&E-Disapproved Test Plans

Program Document
Distributed Common Ground System – Army (DCGS-A) Capability Drop 2 (CD2) Operational Utility Assessment (OUA) 2022-FO-IEW-DCGS2-I2040 Operational Test Plan (OTP)
Evolved Sea Sparrow Missile (ESSM) Block 2 IOT&E Phase 1 M&S RFR Test Plan
Warp Core Adversarial Assessment (AA) Plan

Service Secretary Comments

SECRETARY OF THE ARMY
WASHINGTON

22 DEC 2022

MEMORANDUM FOR Director, Operational Test and Evaluation, 1700 Defense Pentagon, Washington, DC 20301-1700

SUBJECT: Army Response to Fiscal Year 2022 Director, Operational Test and Evaluation Annual Report

1. Thank you for the opportunity to include the Army's comments in the Director, Operational Test and Evaluation (DOT&E) Fiscal Year 2022 Annual Report. This is the Department of the Army response.

2. I appreciate the thoroughness of the DOT&E report as well as the coordination between DOT&E and the Army. The Army provides the below insights from the Service level.

a. The Army is actively modernizing to ensure we provide the most capable and adaptable weapons systems to the Joint Force. Correspondingly, the Army remains focused on ensuring that effective capabilities are employed to test and evaluate emerging technologies. The Army's test and evaluation (T&E) community has already initiated actions to provide our workforce with more advanced skills, modernize test capabilities, and invest in future capabilities to address many of the technologies identified in this report.

b. The Army acknowledges the importance of the oversight role of OSD activities; however, the Army believes the management and execution of test capabilities to address new technology challenges is best retained at the Service level, thereby appropriately aligning authority, responsibility, and resources. For example, the Army is responsible for scheduling and executing critical Army live-fire tests with a sufficient quantity of anthropomorphic test devices (ATDs), yet this report recommends the Army investigate additional purchases of ATDs at $900,000 per unit.

c. The Army is very pleased with the Department's recognition of the T&E and recruiting challenges for chemical and biological defense (CBD) at Dugway Proving Ground, a remote and isolated installation. The Army would like to emphasize that adequate and predictable funding continues to remain an additional challenge for CBD T&E sustainment and infrastructure modernization.

SUBJECT: Army Response to Fiscal Year 2022 Director, Operational Test and Evaluation Annual Report

3. We look forward to working with your office on implementing the recommendations at the Service level to ensure we continue to provide effective capabilities to our Soldiers in support of the Joint Force. Thank you for your continued support of Army programs and our Soldiers.

4. My point of contact for this action is Ms. Laura Pegher, 571-256-9438 or laura.i.pegher.civ@army.mil.

Christine E. Wormuth

THE UNDER SECRETARY OF THE NAVY
WASHINGTON DC 20350-1000

JAN 4 - 2023

MEMORANDUM FOR DIRECTOR, OPERATIONAL TEST AND EVALUATION

SUBJECT: Department of the Navy Comments on the FY2022 DOT&E Annual Report

Pursuant to your e-mail dated December 6, 2022 requesting Department of the Navy comments on the Fiscal Year (FY) 2022 Director, Operational Test & Evaluation (DOT&E) Annual Report, the following is provided:

- CVN 78 Gerald R. Ford Class Nuclear Aircraft Carrier: The report notes risk associated with low or unproven reliability of systems critical for flight operations, specifically citing reliability regression for Electromagnetic Aircraft Launch System (EMALS) and Advanced Arresting Gear (AAG), and fastener issues for the Jet Blast Deflectors. In 2022 the Navy has addressed AAG and EMALS issues via a reliability growth plan that resulted in an average Operational Availability of ~0.98 for the last 5,500 (~45%) launches and recoveries across both systems. Advanced Weapons Elevators supported the on-load of over 1,470 tons of ammunition during preparations for deployment with very promising lower stage elevator performance and higher weapons transfer efficiency than NIMITZ, as noted in the DOT&E report.

- Advanced Anti-Radiation Guided Missile – Extended Range (AARGM-ER): To clarify, AARGM-ER will be employed by F-35 A, B and C, not just the A/C versions as stated in the report.

- Offensive Anti-Surface Warfare (OASUW): The Navy will continue to work with DOT&E to plan and execute an adequate OASUW Operational Test to support full-rate production and Engagement Operations Centers in 4QFY26, rather than FY24 as stated in the report.

- CH-53K King Stallion: CH-53K conducted all Developmental Test Center of Gravity (CG) testing required to approve a CG range that meets the fleet requirement to carry 30 troops down to minimum fuel. VMX-1 did not conduct troop transport missions with 30 combat equipped troops down to minimum fuel due to the overly conservative nature of the currently issued weight and center of gravity planning tools. The fleet will be issued updated and more accurate tools in FY23. CH-53K secondary mission operational test is scheduled for 3QFY23 vice 2QFY23, and integrated cyber survivability testing is scheduled for 3QFY24 vice 2QFY24.

- Conventional Prompt Strike: The Navy has four additional Joint Flight Campaigns planned through 4QFY24 (five total) to develop and demonstrate a hypersonic, cold-gas launched missile system prototype capability.

I appreciate DOT&E's coordination with our individual Program Executive Offices, and thank you for this final opportunity to comment on the FY2022 DOT&E Annual Report.

Erik K. Raven

Copy to:
ASN (RD&A)
PDD PMD ASN (RD&A)
DASN (DOT&E)

SECRETARY OF THE AIR FORCE
WASHINGTON

JAN 1 0 2023

MEMORANDUM FOR THE DIRECTOR, OPERATIONAL TEST AND EVALUATION

SUBJECT: Department of the Air Force Response to Fiscal Year (FY) 2022 Director, Operational Test and Evaluation (DOT&E) Annual Report

I appreciate the opportunity to review the FY22 report. Holistically, this report reflects an accurate status of oversight programs in the Department of the Air Force (DAF) and identifies the challenges and opportunities of resourcing the Department of Defense test enterprise. The DAF has also provided clarifications and amplifying information for your consideration in the final report.

Moving forward, I would like to see a clean distinction between the Air Force and Space Force. The sections where Air Force is used to address both the Air Force and Space Force entities should be listed as the DAF. This includes adding sub headers for the listed Air Force and Space Force programs to show the difference between the two Services.

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.

Frank Kendall

cc:
AF/CV
AF/TE

Index of Programs

#

A

B

C

D

E

U

V

www.dote.osd.mil