FY 2023 Annual Report

Director, Operational Test & Evaluation

January 2024

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

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

This page intentionally left blank.

Director's Introduction

In 2023 this office celebrated 40 years of service to the Department of Defense and Congress. While we honor our past, we are continuing our efforts to meet our strategic intent to *transform test and evaluation to enable delivery of the world's greatest warfighting capability at the speed of need*. U.S. systems are growing more complex, and those of our adversaries are becoming more sophisticated, demanding on-par test and evaluation capabilities, tools, methods, and processes. In April of this year, we issued the DOT&E Strategy Implementation Plan – 2023. This plan is designed to capitalize on the latest advances in science and technology to modernize our craft, enable our agility and efficiency, and continue to inspire trust and confidence in system performance under wartime conditions.

ENHANCING OPERATIONAL EVALUATIONS

To enable adequate representation of the operational environment in test and support the evaluation of the operational performance of DoD systems and capabilities in multi-domain operations, operational and live fire test and evaluation must lean more aggressively on automation, digital tools, and technologies. This includes evaluations throughout operations and sustainment as our systems and those of our adversaries as they both continue to evolve more dynamically over time. DOT&E's advocacy for multi-domain, realistic threat environments – live, virtual, and constructive – to support adequate operational and live fire test and evaluation continues to be a priority.

Digital tools were effectively used to inject combat-realistic target scenes into the live Patriot batteries to support operational testing of the Army's Patriot missile defense system. The fully accredited digital tool suite immersed the system and its operators into simulated, full-scale conflict; this enabled us to understand the Patriot system's performance under a wide variety of combat conditions, including simultaneous missile, cyber, and electronic warfare attacks. Similarly, operational testing of the most recent variants of the Aegis Weapon System relied on a simultaneous anti-air warfare and ballistic missile defense scenario with challenging digital threat surrogates, advancing the warfighter's confidence in Aegis under today's combat conditions.

The Joint Simulation Environment (JSE) – which provides a digital representation of test environments and integrates additional modern threat types, in greater densities, with threat capabilities not available on the open-air ranges – was critical to completing the F-35 initial operational test and evaluation (IOT&E), culminating in the final 42 percent of the required mission trial events. Testing in the JSE was accomplished after a thorough verification, validation, and accreditation (VV&A) process, setting a baseline that must continue to be updated as new F-35 capabilities and other weapons platforms such as the Navy's F/A-18E/F Super Hornets, the Air Force's F-22 Raptors, and the Air Force's Next Generation Air Dominance (NGAD) system are delivered to the warfighter.

ADDRESSING ADVANCED, PERSISTENT THREATS

Operational and live fire test and evaluation of DoD systems and warfighting capabilities in contested, congested, and constrained operations is key to enabling the *operational effectiveness, suitability, survivability, and lethality* of our joint force. Operational and live fire testing identifies problems prior to fielding and supports improvements in systems to avoid operational failures in battle.

The Russia-Ukraine war, while tragic, is a real-world validation of the value of operational and live fire test and evaluation. U.S. systems such as the Javelin Anti-Tank Weapon System and the HIMARS M142 High Mobility Artillery Rocket System have proven themselves on the world-stage by providing force protection and bringing overwhelming firepower and mobility. The operational performance observed in this conflict is a testament to our acquisition process and the significance of adequate operational and live fire test and evaluation. This data, collected against the operationally representative and relevant advanced and persistent threats, provide the DoD's leadership, Congress, our Service members, and the public with direct insight into whether our systems and capabilities can deter wars and ensure national security.

PRIORITIZING CHINA AS THE PACING CHALLENGE

As the 2022 National Defense Strategy states, "China will remain our most consequential strategic competitor," for decades to come. FY23 marked the re-establishment of DOT&E's Joint Test and Evaluation (JT&E) Program critical to the support of joint warfighting concepts, mission engineering, and development and validation of new data-based tactics, techniques, and procedures. JT&E is committed to identifying innovative joint test concepts and approaches intended to accelerate and advance the support to U.S. Indo-Pacific Command's (USINDOPACOM) *Blind, See, Kill* initiatives.

Our Joint Technical Coordinating Group for Munition Effectiveness (JTCG/ME) program reached a major achievement this year. JTCG/ME was invited to support the Department-wide Joint Targeting Intelligence Modernization initiative to accelerate and optimize the selection, analysis, and prioritization of targets while enabling targeting at scale and integration of kinetic and non-kinetic fires across all domains. This not only supports USINDOPACOM but other combatant commands as well.

Our Cyber Assessment Program (CAP) continued the support to USINDOPACOM and the other combatant commands by increasing the threat realism of their exercises, affording warfighters and defenders with excellent opportunities to fight through realistic contested environments. These assessments also underscore the importance of Zero Trust best practices, and the survivability of cross domain solutions needed to counter the escalating offensive capabilities of our potential adversaries.

TAKING CARE OF OUR PEOPLE

Rapid technological changes are shifting the skills and scale required to conduct operational and live fire test and evaluation. To build resilience and readiness, we must update and maintain the workforce competencies, establish a complementary continuous learning campaign, and enhance the talent

management and talent acquisition initiatives to meet future mission demands. We look forward to teaming with USD(P&R) to leverage their Advanced Distributed Learning platform and USD(A&S) to leverage their Defense Civilian Training Corps.

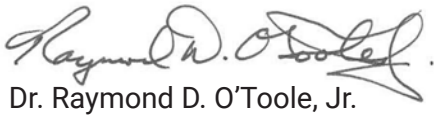
SUCCEEDING THROUGH TEAMWORK

I want to thank our partners within DoD and across industry, academia, national laboratories, and federally funded research and development centers for supporting our strategic initiatives and actions. While there is still work to be done, we have made significant progress this year towards meeting our strategic objectives. I also want to thank Congress for their continued support, and for encouraging us to innovate. Our global allies and partners who join us on the test and evaluation transformation journey deserve our gratitude as well. Finally, thank you to my staff and our warfighters for working as a formidable team to serve and defend our Nation.

WAY AHEAD

In December of 2023, I was honored to start serving as the Acting Director of DOT&E when the former Director of DOT&E, HON Nickolas Guertin, transitioned to become Assistant Secretary of the Navy for Research, Development, and Acquisition. On behalf of DOT&E and the larger Operational and Live Fire Test and Evaluation community, we applaud the numerous exemplary accomplishments of HON Guertin during his two years leading DOT&E.

I will serve in my new role until a new DOT&E Director is appointed by the President following Senate confirmation. In the meantime, I am confident DOT&E will continue to serve the Department of Defense and Congress, and my staff will give me their best efforts as we embrace the opportunities ahead.



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

This page intentionally left blank.

CONTENTS

Introduction	i
Mission	1
Executive Summary	3
DOT&E Strategy Implementation Plan	13
Test and Evaluation Resources	21
DoD Programs	27
Department of the Army Programs	81
Department of the Navy Programs	141
Department of the Air Force Programs	259
USSOCOM Programs	327
Missile Defense System	331
DOT&E-Managed Activities	343
Appendix	399

CONTENTS

Introduction i

Mission 1

Executive Summary 3

DOT&E Strategy Implementation Plan (I-Plan) 13

Test and Evaluation Resources 21

DoD Programs 27

Aerosol and Vapor Chemical Agent Detector (AVCAD) 29

Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives 32

DoD Healthcare Management System Modernization (DHMSM®). 37

F-35 Joint Strike Fighter (JSF) 40

Global Command & Control System – Joint (GCCS-J). 56

Joint Biological Tactical Detection System (JBTDS) 59

Joint Cyber Warfighting Architecture (JCWA) 62

Joint Operational Medicine Information Systems (JOMIS) 65

Joint Planning and Execution System (JPES) 68

Key Management Infrastructure (KMI) 71

National Background Investigation Services (NBIS) 74

Public Key Infrastructure (PKI) Increment 2 77

Department of the Army Programs 81

120mm Advanced Multi-Purpose (AMP) Cartridge, High Explosive Multi-Purpose with Tracer, M1147 83

Abrams M1A2 System Enhancement Packages (SEPs) and Active Protection System (APS) 85

Armored Multi-Purpose Vehicle (AMPV) 88

Army Integrated Air and Missile Defense (AIAMD) 91

Dismounted Assured, Positioning, Navigation, and Timing System (DAPS) 94

Distributed Common Ground System – Army (DCGS-A) Capability Drop 2 (CD2). 97

Family of Medium Tactical Vehicles A2 (FMTV A2) 100

Infantry Squad Vehicle (ISV) 104

Integrated Personnel and Pay System – Army (IPPS-A) Increment 2 106
Integrated Tactical Network (ITN) 109
Integrated Visual Augmentation System (IVAS) 112
Javelin Antitank Missile System – Medium 115
Joint Air-to-Ground Missile (JAGM) 119
Long Range Hypersonic Weapon (LRHW) – Dark Eagle 122
Mounted Mission Command – Software (MMC-S) 125
Next Generation Squad Weapons (NGSW) Weapons and Ammunition (W&A) 129
Sentinel A4 Radar 132
Soldier Protection System (SPS) 135
UH-60V Black Hawk Digital Cockpit 138

Department of the Navy Programs 141

Navy Progams 143

Advanced Anti-Radiation Guided Missile – Extended Range (AARGM-ER) 145
Aegis Modernization Program 148
AIM-9X Block II Sidewinder 152
Air and Missile Defense Radar (AMDR) / AN/SPY-6 154
AN/AQS-20X Minehunting Sonar and Tow Vehicle (all variants) 157
CH-53K® King Stallion® 159
CMV-22B Joint Services Advanced Vertical Lift Aircraft – Osprey – Carrier Onboard Delivery 162
Consolidated Afloat Networks and Enterprise Services (CANES) 165
Conventional Prompt Strike (CPS) 168
Cooperative Engagement Capability (CEC) 172
CVN 78 *Gerald R. Ford*-Class Nuclear Aircraft Carrier 175
DDG 1000 *Zumwalt*-Class Destroyer 183
Distributed Common Ground System – Navy (DCGS-N) 186
E-2D Advanced Hawkeye 189
F/A-18 Infrared Search and Track (IRST) Block II 192
F/A-18E/F Super Hornet and EA-18G Growler 195
FFG 62 *Constellation*-Class Guided-Missile Frigate 199
LHA 6 Flight 0/Flight 1 Amphibious Assault Ship 202

Littoral Combat Ship (LCS) 205
Mk 48 Torpedo Modifications 208
Mk 54 Lightweight Torpedo Upgrades Including the High Altitude Anti-Submarine Warfare Weapon Capability (HAAWC) 212
MQ-25 Stingray Carrier Based Unmanned Aerial System (CBUAS) 215
MQ-4C Triton 218
MQ-8C Fire Scout 221
Next Generation Jammer Mid-Band (NGJ-MB) 224
Offensive Anti-Surface Warfare (OASuW) Increment 1 227
Ship Self-Defense System (SSDS) Mk 2 Integrated Combat Systems 230
Ship to Shore Connector (SSC) 234
Standard Missile 2 (SM-2) Block IIIC and Block IIICU 237
Surface Electronic Warfare Improvement Program (SEWIP) Block 2 240
T-AO 205 *John Lewis*-Class Fleet Replenishment Oiler 243
Tomahawk Weapon System (TWS) 246
Trident II (D-5) Sea-Launched Ballistic Missile – Life Extension Program Variant 249
VH-92A® Patriot® Presidential Helicopter 251

Marine Corps Programs 255

Long Range Unmanned Surface Vessel (LRUSV) 257

Department of the Air Force Programs 259

Air Force Programs 261

AGM-183A Air-Launched Rapid Response Weapon (ARRW) 263
AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM) 266
Air Operations Center – Weapon System (AOC-WS) 268
B-52 Radar Modernization Program (RMP) 272
B-52J Commercial Engine Replacement Program (CERP) 275
Defense Enterprise Accounting and Management System (DEAMS) 278
F-15 Eagle Passive Active Warning and Survivability System (EPAWSS) 281
F-15EX Eagle II 284
F-16 Radar Modernization Program (RMP) 288
F-22A – Raptor Advanced Tactical Fighter Aircraft 291

HH-60W Jolly Green II. 294
KC-46A Pegasus 297
Massive Ordnance Penetrator (MOP) Modification 301
MH-139A Grey Wolf 303
Small Diameter Bomb Increment II (SDB II) 307
T-7A Advanced Pilot Training (APT) 310
Three-Dimensional Expeditionary Long-Range Radar (3DELRR) 313

Space Force Programs. 315

Global Positioning System (GPS) Enterprise 317
Space Command and Control System (Space C2) 323

USSOCOM Programs 327

Dry Combat Submersible (DCS). 329

Missile Defense System. 331

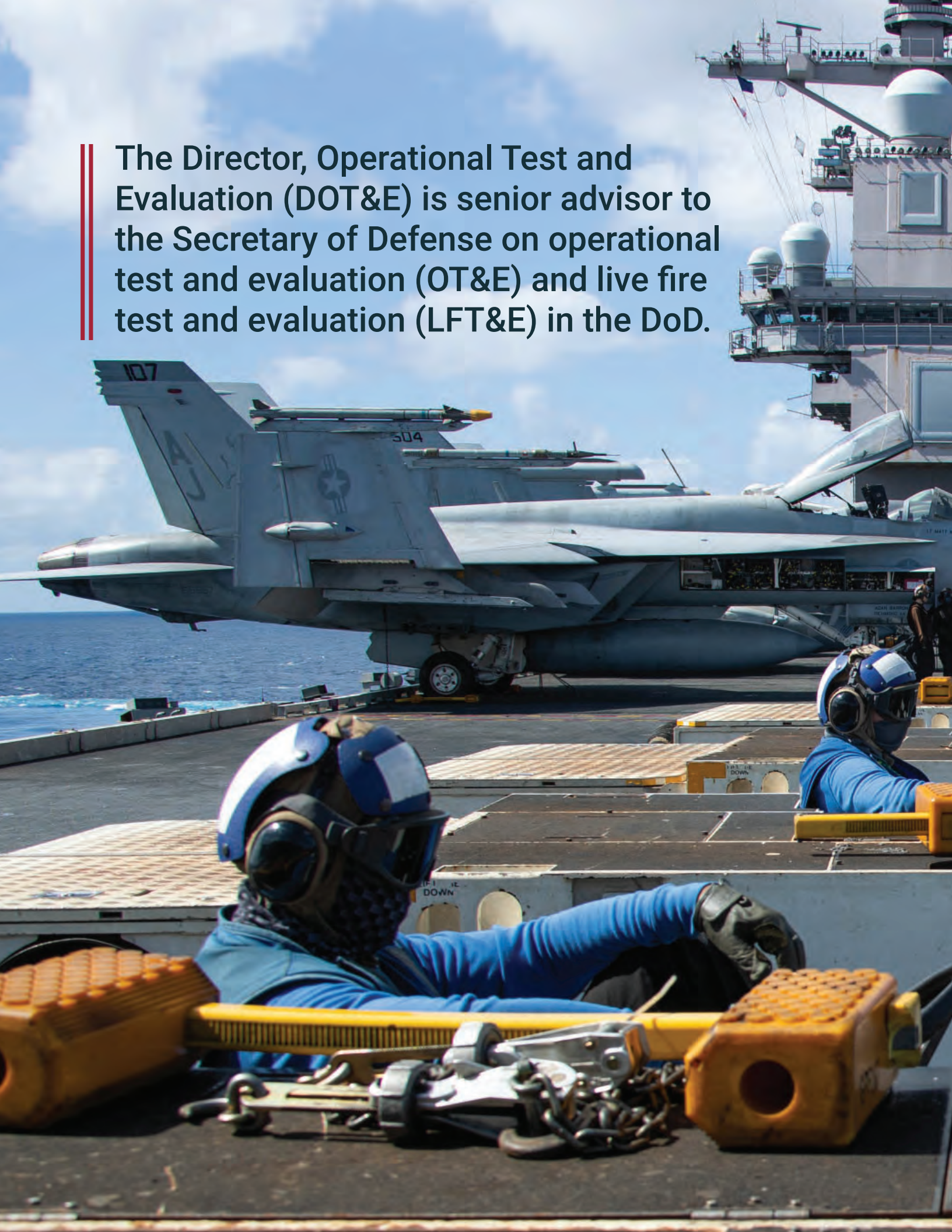
DOT&E-Managed Activities 343

Center for Countermeasures (CCM) 345
Cyber Assessment Program (CAP) 351
International Test and Evaluation Program (ITEP) 360
Joint Aircraft Survivability Program (JASP) 370
Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) Program 376
Joint Test and Evaluation (JT&E). 389
Test and Evaluation Threat Resource Activity (TETRA) 395

Appendix 399

Oversight List 401
DOT&E Activities 409
Service Secretary Comments. 419
Index of Programs. 427

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:

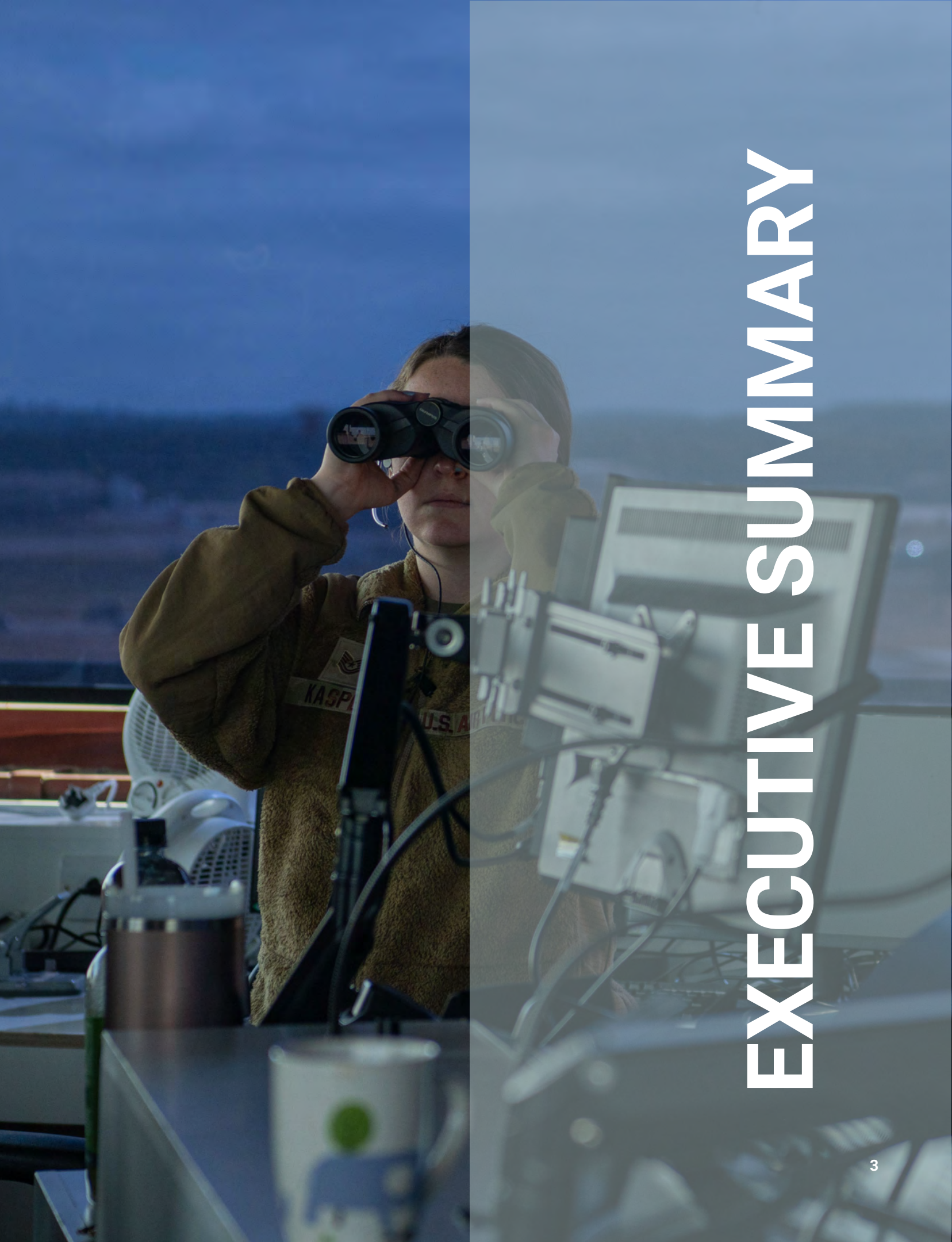
- Enable adequate OT&E and LFT&E of DoD weapon systems in operationally representative and relevant conditions to support credible evaluation of the operational effectiveness, suitability, survivability, and lethality of DoD weapon systems in combat. Adequate T&E enables the delivery and fielding of 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.

This page intentionally left blank.



EXECUTIVE SUMMARY

This page intentionally left blank.

MAJOR PRODUCTS

In FY23, DOT&E designated 45 new DoD systems for OT&E and LFT&E oversight and removed 22 systems from the T&E Oversight List. As of September 2023, DOT&E had 266 DoD systems on the T&E Oversight List for OT&E and/or LFT&E. In FY23, DOT&E:

- Reviewed and approved 32 T&E strategies/ Test and Evaluation Master Plans (TEMPs) and disapproved 1 TEMP.
- Approved 59 individual test plans and disapproved 1 test plan.
- Published 46 reports, including 34 reports on the independent evaluation of test adequacy and operational performance of DoD systems and 12 reports on cyber assessments or response to congressional taskers.

DOT&E completed 4 of the 14 assigned congressional taskers and is on track to complete the remaining tasks summarized in Table 1 in accordance with the agreed-upon timelines between DOT&E and Congress.

Table 1. Summary of DOT&E Congressional Activities

Source	Title	Status
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	Complete
Sec. 1529	Demonstration program for automated security validation tools	Ongoing
Other FY22 Congressional Taskers		
SASC Report pg. 191-192	Electronic Health Record interoperability between DoD and Veterans Affairs	Ongoing
FY23 NDAA		
Sec 217	Competitively awarded demonstrations and tests of electromagnetic warfare technology	Ongoing
Sec 242	Study and report on sufficiency of operational test and evaluation resources supporting major defense acquisition programs	Ongoing
Sec 1514	Operational testing for commercial cybersecurity capabilities	Ongoing
Sec 1656	Persistent cybersecurity operations for ballistic missile defense systems and networks	Ongoing
Other FY23 Congressional Taskers		
*Omnibus	Certification of funding for test infrastructure and test event resources	Complete
*Omnibus	Certification of test strategies on Middle-Tier Acquisition and Rapid Prototyping programs	Complete
HASC Report pg. 77	Assessment of contractor-provided test and evaluation capabilities	Ongoing
HASC Report pg. 77	Battery testing infrastructure	Ongoing
HASC Report pg. 77	Development and testing of body-worn equipment	Ongoing
HASC Report pg. 78	Equipment shortfalls within the test and evaluation community	Ongoing

Acronyms: 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 in FY23 which are reflected in the Appendix.

DOT&E published a DOT&E Strategy Implementation Plan (I-Plan) formally endorsed by the Under Secretary of Defense for Research and Engineering, the Under Secretary of Defense for Acquisition and Sustainment, and the Military Service Secretaries. The I-Plan outlines key actions and deliverables intended to contribute to the transformation of T&E infrastructure, tools, processes, and workforce in response to emerging changes in acquisition, technology, and warfighting.

DOT&E drafted the DoD Instruction for OT&E and LFT&E and the following DoD Manuals: (1) TEMP/ T&E Strategy; (2) Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A) for OT&E and LFT&E; (3) OT&E and LFT&E of Software; (4) OT&E and LFT&E of Artificial Intelligence (AI)-Enabled and Autonomous Systems; and (5) Full-Spectrum Survivability and Lethality T&E. These policies are intended to: (1) enable OT&E and LFT&E stakeholders to inform acquisition contracts; (2) optimize the use of all data, intelligence, and program artifacts across the acquisition life cycle; and (3) increase OT&E and LFT&E efficiency and agility by increasing the use of digital engineering, digital tools, and technologies (e.g., M&S, model-based engineering, smart documentation, data repositories, data analytics, modern predictive analytics tools using AI and machine learning).

OT&E AND LFT&E OVERSIGHT OF DoD SYSTEMS

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

In FY23, DOT&E evaluated the adequacy of the TEMPs or T&E strategies, and OT&E and LFT&E plans based on the degree that they will provide: (1) data to support credible evaluation of operational effectiveness and suitability; (2) coverage of the battlespace and threats; (3) adequate verification and validation of M&S; (4) complete assessments of system survivability and lethality against mission-relevant kinetic and non-kinetic threats; (5) production-representative test articles; (6) operational realism; and (7) sufficient funding required to support test execution.

In FY23, DOT&E approved all but one TEMP and all but one test plan. Common DOT&E pre-requisites for approval included improving: (1) testing of the supply chain and inclusion of all potential attack vectors in contested cyberspace; (2) coverage of the operational environment and threats; (3) testing of all possible system variants; (4) M&S verification and validation (V&V); (5) use of latest software versions; and (6) data collection processes or equipment to support an evaluation of operational effectiveness, suitability, survivability, and lethality (as applicable).

In FY23, for the 34 programs that executed OT&E and/or LFT&E, DOT&E assessed 70.5 percent (24 of 34) as adequate, 20.5 percent (7 of 34) as partially adequate, and 9 percent (3 of 34) as not adequate, as shown in Figure 1. By comparison, over the last 7 years (FY16-22), DOT&E assessed 66.5 percent (143 of 218) of the executed OT&E and LFT&E as adequate, 25 percent (54 of 218) as partially adequate, and 9.5 percent as not adequate. The inadequacy or partial adequacy of OT&E and LFT&E were caused by: (1) lack of operational testing prior to early fielding, (2) delays in testing and early test termination, (3) lack of production-representative hardware or software, (4) data collection shortfalls, and/or (5) lack of testing under all pertinent threats and conditions. For the 34 programs that executed OT&E and/or LFT&E, DOT&E highlighted at least one test limitation in 26 of them, including but not limited to:

- Lack of assessment of all relevant cyberattack vectors or paths due to limitations imposed to protect the system from damage and ensure operator safety.
- Lack of access to production-representative hardware, software, supporting systems, and relevant documentation during early tests.
- Lack of an available threat simulator or surrogate.
- Lack of an environment that replicates the most challenging scenarios and limited or no testing in a contested electromagnetic environment.
- Inadequately validated or accredited M&S, or M&S results that did not capture all operationally

relevant conditions or did not model all important interactions.

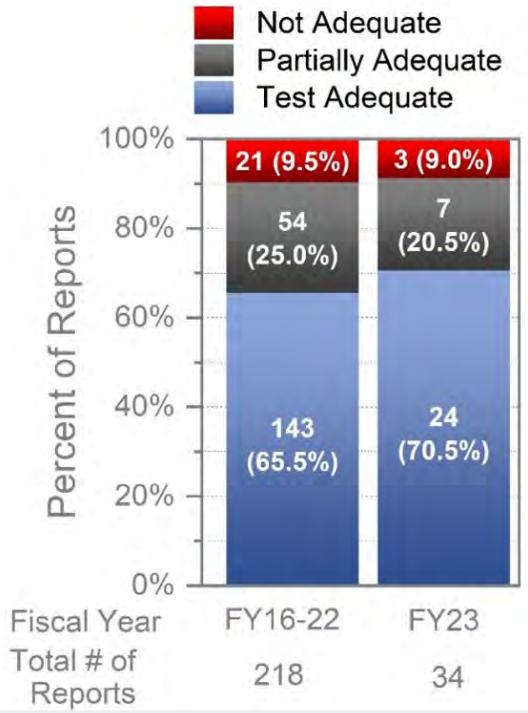


Figure 1. Test Adequacy in FY23 and Prior Years

Test Adequacy Recommendation Trends

DOT&E reports included recommendations for improving test adequacy including but not limited to:

- Completing testing with production-representative assets before fielding. A large fraction of test adequacy problems result from incomplete testing prior to fielding.
- Conducting operational testing across the relevant missions sets, operating conditions, and threats. Execution of robust testing continues to reveal important shortfalls that can be addressed prior to fielding.
- Testing all relevant cyberattack paths.
- Evaluating system suitability and cyber survivability early in the design to increase test efficiency, discover problems early, and improve outcomes in OT&E and LFT&E.
- Developing robust and independent V&V for all M&S to be used in OT&E and LFT&E.

Programs Pursuing the Middle Tier of Acquisition Pathway

In FY23, for the 97 programs approved by the Service Acquisition Executives to pursue Middle Tier of Acquisition pathways, DOT&E received and reviewed 55 test strategies and certified 43 of those to be appropriate. Test strategies were not certified as appropriate primarily due to inadequate resources for OT&E and/or LFT&E to evaluate the required capability in an operationally representative contested cyberspace and contested, congested, and constrained electromagnetic spectrum environments.

Adequacy of Resources for Programs with Approved TEMPs or T&E Strategies

In FY23, DOT&E assessed the adequacy of OT&E and LFT&E resources required to execute the agreed upon OT&E and LFT&E, scheduled in the current year and future years defense planning. This assessment could only be made for those programs on the DOT&E oversight that had approved TEMPs or T&E strategies.

- Fifty-five percent (72 of 131) of the eligible programs were assessed to have adequate funding to support the remainder of the planned test execution. Five percent (7 programs) were identified as having funding shortfalls, while 17 percent (22 programs) required updated TEMPs or T&E strategies due to program changes that may require new or altered testing or resource requirements. Eleven percent (15 programs) have fully executed all required testing and require no current or Future Year Defense Program funding. Fifteen additional programs were not assessed despite being eligible for this assessment because funding data were not provided by the Services.
- The identified OT&E and LFT&E resource shortfalls required to support adequate testing were primarily related to: (1) threat and target representation in contested environments; (2) representative digital representation of DoD systems; (3) physical and virtual range capabilities required to support testing of hypersonic weapons, integrated fires, and force-on-force operational performance; and (4) workforce skills

and capacity to accelerate the use of credible digital tools, automation, space-based OT&E and LFT&E and increase the availability of cyber and software scientists and engineers to include National Security Agency-certified Red Teams.

» PROVIDED INDEPENDENT EVALUATION OF OPERATIONAL PERFORMANCE

In FY23, DOT&E published 34 reports summarizing the adequacy of OT&E and LFT&E and a preliminary evaluation or final evaluation of the operational performance of the system. Of the 34 system reports, all included an assessment of test adequacy, 17 provided a final evaluation of operational effectiveness, 16 provided a final evaluation of operational suitability, and 12 provided a final evaluation of survivability. The remaining reports included a preliminary evaluation of operational performance not included in the operational performance trends discussed below and in Figure 2.

Operational Effectiveness Trends

In FY23, DOT&E reported 65 percent (11 of 17) of the evaluated programs to be operationally effective. By comparison, over the last 7 years (FY16-22), DOT&E reported 52 percent (71 of 137) to be operationally effective. DOT&E assessed two FY23 programs as not operationally effective and four programs as being partially effective because the system could either not complete one or more of its primary missions or had poor operational effectiveness in some operationally relevant conditions. For example, one system was able to complete missions in a permissive environment but could not complete missions in a contested environment because of poor survivability.

Operational Suitability Trends

In FY23, DOT&E reported 56 percent (9 of 16) of the evaluated programs to be operationally suitable. By comparison, over the last 7 years, DOT&E reported 52 percent (61 of 131) to be operationally suitable. DOT&E assessed six programs as not operationally suitable and one program as being partially operationally suitable. These seven programs, without exception, experienced shortfalls in reliability, availability, and/or maintainability. Other common suitability limitations included human systems integration challenges related to workload, usability, or training; transportability challenges; and immaturity of the logistical supply system.

Survivability Trends

In FY23, DOT&E reported 25 percent (3 of 12) of the programs to be survivable and 33 percent (4 of 12) to be partially survivable. By comparison, over the last 7 years, DOT&E assessed 31 percent (34 of 109) as survivable and 27 percent (29 of 109) as partially survivable, primarily due to a significant number of mission critical vulnerabilities in contested

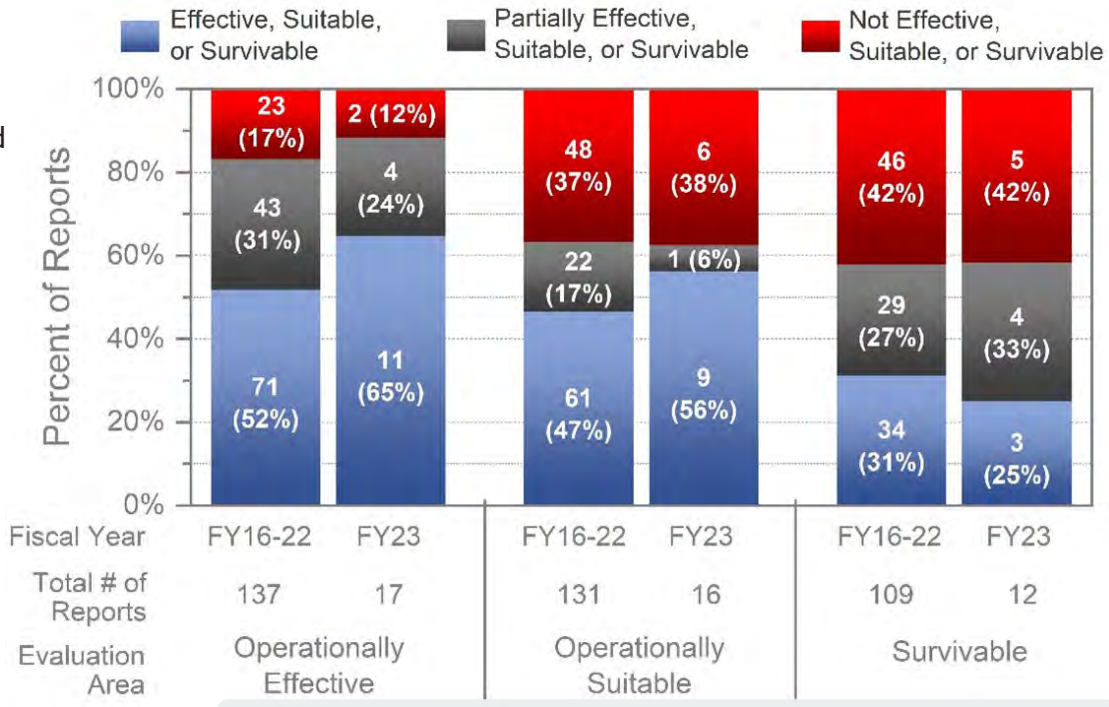


Figure 2. Operational Performance Trends in FY23 and Prior Years

cyberspace. Some systems also demonstrated unexpected vulnerabilities to kinetic threats and while operating in a contested electromagnetic spectrum environment.

Recommendation Trends

DOT&E reports include practical recommendations to fix the identified deficiencies, improve the operational performance of the DoD systems in expected operational scenarios, identify conditions to minimize risk to warfighters, and maximize probability of mission success. Examples of common recommendations are related to immature software, poor reliability, not survivable against cyberattacks, poor system performance, deficient human systems integration, and insufficient training and technical manuals.

RESPONDED TO WARFIGHTER REQUIREMENTS AND ADVANCED OT&E AND LFT&E PRACTICES

In FY23, DOT&E managed the Cyber Assessment Program (CAP) and the following field activities: (1) Center for Countermeasures (CCM), (2) Joint Aircraft Survivability Program (JASP), (3) Joint Technical Coordinating Group for Munition Effectiveness (JTCG/ME) that includes the Joint Live Fire (JLF) program, (4) Joint Test and Evaluation (JT&E), and (5) T&E Threat Resources Activity (TETRA). DOT&E also initiated the execution of the DOT&E Strategy Implementation Plan. Collectively, these activities made progress in responding to urgent warfighting requirements and transforming the DoD T&E infrastructure, tools, processes, and workforce in response to emerging changes in acquisition, technology, and warfighting. Details can be found in the DOT&E-Managed Activities and the Strategy Implementation Plan Update sections of this Annual Report. In summary, these activities:

- Improved the threats and operational realism in test. As an example, TETRA continued the development, validation, and delivery of 10 radio frequency and 10 infrared high-priority threat models, as well as over 25 high-fidelity, closed-loop, electronic-warfare-capable, emulative threat models needed for OT&E and LFT&E. JASP supported the delivery of new electronic attack techniques against advanced radar threats and improved hardware-in-the-loop capabilities for man-portable air-defense systems. CAP worked with the combatant commands to improve the operational realism of cyber assessments and emulate advanced threats.
- Advanced the use of credible digital tools in OT&E and LFT&E. For example, JTCG/ME continued to develop new digital tools (e.g., the Next Generation Enterprise Maritime Lethality Tool) and reduce the uncertainty in existing tools (e.g., Submarine Vulnerable Effects Model, Navy Enhanced Sierra Mechanics, and Dynamic System Mechanics Advanced Simulation) required to support the delivery and fielding of weaponeering tools against maritime targets while also supporting the survivability and lethality evaluations of U.S. Navy ships and submarines in contested environments. JTCG/ME also continued the critical VV&A and uncertainty quantification advancement efforts in coordination with the U.S. Army, U.S. Air Force, U.S. Navy, and Lawrence Livermore National Laboratory representatives.
- Supported the advancement of efficiency and agility of OT&E and LFT&E. For example, DOT&E supported the development of a prototype software application to optimize test sizing in a dynamic way using modern statistical inference methods to enable adaptive, integrated testing. DOT&E also supported the development of a prototype of a smart word processing and content management application intended to expedite the development and review of acquisition program (model-based) documents.
- Responded to urgent warfighter requirements. For example, JT&E supported new, data-based concepts of employment for long-range hypersonic weapons, nuclear command and control operations, and improved cyber survivability. JTCG/ME generated 13 reach-back packages for weaponeering, collateral damage estimates in support of current operations.

- Helped address the workforce challenges. For example, DOT&E supported an internship program – in partnership with the Army's Program Executive Office for Simulation, Training, and Instrumentation – resulting in 20 cyber experts poised to earn 20 Security+ certifications and 9 Certified Ethical Hacker certifications and join the T&E workforce.

CONTINUED TO SUPPORT GLOBAL T&E PARTNERSHIPS

In FY23, DOT&E continued to maintain multiple bilateral and multilateral agreements with international partners through the International T&E Program (ITEP) expediting the development and fielding of advanced warfighting technologies and supporting T&E infrastructure. Through ITEP, DOT&E finalized 12 new project agreements and is monitoring 24 ongoing projects. These projects are intended to improve capabilities and instrumentation among U.S. allies in areas including electronic warfare, autonomy, and survivability.

This page intentionally left blank.

DOT&E STRATEGY IMPLENTATION PLAN

This page intentionally left blank.

DOT&E Strategy Implementation Plan (I-Plan)

In April 2023, DOT&E, in coordination with USD(R&E), USD(A&S) and the Military Service Secretaries, published a DOT&E Strategy Implementation Plan (I-Plan) to collaboratively and cooperatively transform the DoD T&E infrastructure, tools, processes, and workforce in response to emerging changes in acquisition, technology, and warfighting. DOT&E's Strategy I-Plan is built on 5 strategic pillars and 12 lines of efforts summarized below.

1. Test the way we fight

- Standardize the development of a scalable and adaptive representation of the multi-domain operating environment
- Implement measures, tools, and processes to efficiently evaluate kill webs and system-of-systems performance

2. Accelerate delivery of weapons that work

- Develop and implement an enterprise-level T&E data management solution
- Integrate T&E in model-based engineering to operationalize and optimize the Shift Left approach

3. Improve the survivability of DoD in a contested environment

- Standardize and automate mission-based risk assessments
- Emphasize cyber and electromagnetic spectrum survivability
- Evaluate operational performance in a contested space environment

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

- Increase the use of credible digital twins in T&E
- Evaluate the operational and ethical performance of AI-based systems
- Advance the evaluation of software-reliant systems' operational performance

5. Foster an agile and enduring T&E enterprise workforce

- Identify and track T&E workforce competencies and capabilities
- Assess and address critical T&E workforce professional development needs

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

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

As documented in the DOT&E Strategy I-Plan, DOT&E recognizes the critical role of T&E within the wider DoD enterprise including acquisition, requirements, warfighting, and intelligence communities. DOT&E also recognizes the critical role of industry, academia, federally funded research and development centers, university affiliated research centers, and international partners to help DoD accelerate innovation and support the delivery of the world's most capable warfighting capability at the speed of need. To align this T&E enterprise against common objectives, the DOT&E Strategy I-Plan identifies the desired end-state for each of the five pillars, as summarized in Table 1. DOT&E looks forward to collaborating with the T&E enterprise to refine and accomplish the T&E initiatives listed for each of the 5 strategic pillars.

Pillar 1 – Test the Way We Fight

Pillar 1 – "Test the way we fight" – is designed to architect T&E around validated joint force mission threads and kill webs (including multiple systems under test) to demonstrate their operational effectiveness, suitability, survivability, lethality, agility, and responsiveness in multi-domain operations.

Measuring the operational performance of such mission threads and kill webs may be advanced by establishing:

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

To contribute to the Pillar 1 end-state, in FY23, DOT&E:

- Initiated a "range of the future" analysis, which is intended to inform the OT&E and LFT&E range capability needs of the future based on known and emerging technology and threat trends and gaps.
- Supported the development of a prototype for the range capabilities dashboard that will identify, prioritize, and digitally track the status of current and emerging OT&E and LFT&E range capability, capacity, and availability shortfalls.
- Developed a preliminary concept for a data-backed, all-domain modeling and simulation (M&S) environment to integrate with live, multi-

domain operational testing, and maintained an M&S for T&E working group.

- Demonstrated there is value to be added using model-based engineering for intelligence analytical activities to interoperate with the acquisition community's digital transition.
- Developed a joint test concept determining the preliminary plan for what needs to be changed, including policy, tools, and training, and how to ensure timely and rigorous T&E of joint operations.

Pillar 2 – Accelerate the Delivery of Weapons that Work

Pillar 2 – "Accelerate the delivery of weapons that work" – is designed to accelerate acquisition and T&E by adopting digital technologies and workflows to speed up the delivery of capabilities to the warfighter. T&E workload and process optimization that enables data-driven T&E at scale and machine speed may be accomplished by:

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

To contribute to the Pillar 2 end-state, in FY23, DOT&E:

- Prototyped a software application to optimize test sizing in a dynamic way using modern statistical inference methods to enable adaptive, integrated testing including the ability that is fully informed by prior live data and digital tool results as T&E is conducted across the acquisition life cycle.
- Developed examples of model-based T&E Master Plans to enable more adaptive and dynamic development, review and approval of such critical acquisition decision artifacts using SysML, and Structured Query Language relational databases.
- Supported the development of a prototype of a smart word processing and content management application intended to expedite the development and review of acquisition program (model-based) documents including the Test and Evaluation Master Plans and system performance reports that are native to Microsoft Word.
- Initiated the development of an enterprise-level automated data analysis suite for the T&E community implementing modern quantitative and computing methods to remix live data collected with M&S, and physics to create "digital arenas" for gleaning the emergent high-level mission effects characteristic of complex multi-domain scenarios and future joint warfighting concepts.
- Initiated analysis campaigns that characterize the high-level effects of specific multi-domain mission threads.

Pillar 3 – Improve DoD Survivability in Contested Environments

Pillar 3 – "Improve DoD survivability in contested environments" – is designed to enable dynamic assessments and improvements of system's ability to effectively operate and survive in a hostile full spectrum threat environment while maintaining mission effectiveness. Minimizing mission-critical vulnerabilities and maximizing defenses against full spectrum threats may be enhanced by:

- Standardizing and automating mission-based assessments to optimize the evaluation of kinetic and non-kinetic threats, and their combined effects. This includes efficient: (1) characterization of system designs, (2) identification and prioritization of vulnerabilities, (3) identification of potential attack conditions, and (4) evaluation of threats effects on the mission.

- Providing automated and integrated processes, tools, and representative threats scenarios with emphasis on cyber and electromagnetic spectrum (EMS) survivability.
- Enabling adequate evaluation of operational performance in a contested space environment by delivering: (1) space environment modeling, system modeling and analytic tools, (2) space T&E process, policy, and guidance, and (3) space test infrastructure to support testing space systems or subsystems ground-testing and combined effects at scale.

To contribute to the Pillar 3 end-state, in FY23, DOT&E:

- Conducted a full spectrum survivability and lethality proof-of-concept tool based on an envisioned cloud-hosted, full-spectrum threat effects as-a-service architecture. The proof of concept is designed to standardize inputs and outputs both within and across kinetic and non-kinetic threat effects to enable the evaluation of survivability and lethality in multi-domain operations to include throughout operations and sustainment.
- At the request of Deputy Secretary of Defense, hosted a DoD Cyber Survivability Human-Centered Design Study Group that published a report in June 2023. The report summarized key DoD cyber survivability challenges and four proposed courses of action to improve the DoD's warfighting survivability posture in contested cyberspace. The courses of action include: (1) integrate cyber survivability across a system's life cycle, including the operations and sustainment phases, (2) cultivate responsive cyber-focused industrial support, (3) conduct mission-based system of systems tests and exercises, and (4) go beyond cyber compliance to operational performance. The DoD is standing up cross-DoD working groups to support the planning and execution of these actions.
- Partnered with the Test Resource Management Center to provide the Cyberspace Live-Fire Evaluation Framework. This quantification framework is a collection of software, test data and automated tools constructed to rapidly test and analyze cyber capability under different environments.
- Supported the development of automated tools necessary to accurately evaluate the ability to detect and recover from cyber threats.
- Leveraged AI Natural Language Processing to support the development of a prototype tool that automatically extracts and properly formats a system's software data for vulnerability analysis.

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

Pillar 4 – "Pioneer T&E of weapon systems built to change over time" – is designed to respond to new warfighting capabilities that will be upgraded and changed throughout the life cycle. This includes things like aircraft mission systems, AI and machine learning (ML), test automation, and digital engineering requiring the development of tools and processes to determine the uniquely contextual operational and responsible performance of these capabilities, especially as they change during real operational use. The T&E community may evolve its processes by:

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

To contribute to the Pillar 4 end-state, in FY23, DOT&E:

- Initiated a pilot to support the development of an architecture for calibrating digital twins based on real, operational data.
- Conducted a pilot using AI/ML to glean differences between digital twins and the physical systems they represent.
- Completed a literature review on the current state of T&E of AI-based systems, discovering that industry and academia have been focused on collecting data to train algorithms and produce models. While numerous tools exist for model monitoring and drift detection, adversarial attacks, hyperparameter optimization, reproducibility, explainability, labeling and annotation, model evaluations, and privacy, there is still an insufficient amount of information to adequately evaluate the operational and ethical performance of AI-enabled and autonomous systems as a T&E enterprise.
- Developed a "best practices" guide to T&E of AI-enabled systems. Completed AI T&E research projects covering: intellectual property implications, using model-based engineering for test case generation, and design of experiments of AI-enabled systems; methods for assessing adversarial effects in computer vision applications; and hierarchical scoring for operational missions.
- Sponsored the development of a prototype application in coordination with DoD CIO and USD(R&E) that measures the maturity of a software factory and helps T&E practitioners understand the effectiveness and overall security of the software factory.
- Investigated the effectiveness rates of static and dynamic code analysis tools and how they can be leveraged for test design.
- Developed a pathfinder effort for model-based testing, demonstrating that a system model can automatically generate and simulate test cases within the model. This capability, if leveraged correctly, may accelerate T&E capabilities through automated test generation and execution.

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

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

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

To contribute to the Pillar 5 end-state, in FY23, DOT&E:

- Enhanced the DOT&E Action Officer (AO) professional development program by redesigning its annual AO course to provide AOs and the larger T&E enterprise with interactive and relevant case simulations that moved beyond traditional lecture-based methods. The course was based on highly interactive, human-centered design learning principles, and engaged attendees in scenario-based exercises, panel discussions, cohort collaboration, and teambuilding while also ensuring a standardized and effective learning experience for new DOT&E AOs and participants from the Service operational test agencies.
- Developed new training materials to respond to emerging changes in DOT&E policy and guidance. Tangentially, coordinated with the Defense Acquisition University and their Software T&E Credential and Cyber T&E Credential teams to support and accelerate the development of their courseware to offset training gaps in software and cyber OT&E and LFT&E training.
- Executed a Learning Needs Assessment of the DOT&E workforce to identify and evaluate T&E campaign of learning and course curriculum to meet future workforce demands. This included

updates to the DOT&E competency model to account for changing job demands in response to a continuously changing and dynamic operating environment and to mirror the Defense Acquisition University's T&E competency model to facilitate a "T&E Enterprise Mindset."

- Continued with the implementation of T&E collaboration and innovation partnership to meet the congressional intent to address the unmet demand for qualified, certified cyber and software T&E talent. In partnership with the Army's Program Executive Office for Simulation, Training, and Instrumentation, DOT&E hosted the 2023 Summer Pathfinder Internship Program. A diverse class of 29 students from 11 universities across the country graduated from the program, resulting in 20 cyber experts poised to earn 20 Security+ certifications and 9 Certified Ethical Hacker certifications and join the T&E workforce. These internships resulted in prototype capabilities for close access teams, adversarial social media tactics, techniques, and procedures, and new command and control techniques for network protocols. All projects ended in a state where DoD cyber Red Teams can mature the prototypes.

TEST AND EVALUATION RESOURCES

This page intentionally left blank.

Test and Evaluation Resources

Key Takeaways	
Department of the Army	• Continued investment in **distributed range capabilities** will support efficient and scalable testing of networked sensor-to-shooter kill chains. • **Availability of advanced threat surrogates** (e.g., armor, electronic warfare threat emulators) will enable representative testing of land warfare systems. • **Advanced open-air and digital range capabilities** will enable dynamic and efficient testing of networks and system-of-systems events. • Developers and technical subject matter experts will improve the use of **digital environments** in test planning and execution.
Department of the Navy	• Availability of **accurate test surrogates** (e.g., threat submarines, ships, and aircraft; modern threat jammers; threat missiles and torpedoes, digital threat simulators) will enable representative testing of naval warfare systems. • **Integration of digital threat representation within test ranges** will provide adequate support of live-virtual-constructive end-to-end system evaluation (e.g., electromagnetic spectrum offensive and defensive capabilities). • **Continuous updates and associated continuous verification, validation, and accreditation (VV&A)** of the Joint Simulation Environment (JSE)[1] will support effective T&E of new air warfare systems.
Department of the Air Force	• New and updated live data will enable accurate **VV&A of high-fidelity digital tools** of blue and red platforms, sensors, and weapon systems including space-based capabilities. • **Updates to range threats, instrumentation, and connectivity** will improve the development and testing of emerging technologies including space-based systems (i.e., open air ranges require high fidelity class of capability emulators, and hardware-in-the-loop facilities lack dynamic, direct-inject simulation of threat infrared (IR) signatures). • **Continuous updates and associated continuous VV&A** of the JSE will support effective T&E of new air warfare systems.
Multi-Service	• **Improved throughput, capacity, and capabilities of test ranges** including advanced data collection will enable the evaluation of emerging technologies including long-range weapons, autonomous, and artificial intelligence (AI)-enabled systems, and against **realistic electronic warfare threats**. • **Big data centers, data management infrastructure, and appropriate classified networks and workstations** in Sensitive Compartmented Information Facilities (SCIFs) will increase efficiencies across the T&E enterprise including DOT&E. • **Automated test tools** including those for software, **cyber**, AI, and integrated T&E will enable testing of complex weapon systems at scale and speed. • **A qualified workforce** including NSA-certified Red Teams and personnel with expertise in digital engineering, software, electronic warfare, AI, big data science, space operations, will help the T&E enterprise meet emerging T&E needs.

1 JSE is a multi-service, scalable, expandible, high-fidelity, government-owned, non-proprietary modeling and simulation (M&S) environment to conduct testing on fifth-plus generation aircraft and systems as a supplement to open-air testing.

DEPARTMENT OF THE ARMY

DOT&E oversees a subset of DoD systems and services intended to support land and expeditionary warfare including the newest military vehicles, ground weapons systems, rotary wing aircraft, communications systems, and missile systems to include hypersonics. To support adequate evaluation of such systems, DOT&E has identified the following T&E resources requirements.[1]

» REQUIRED RESOURCES

- Increased production of Intelligence Community-based threat models of contemporary Russian and Chinese electronic warfare systems, and radio-based communication systems to test emerging Army sensors and offensive capabilities.
- Advanced adversary armor systems to assist in the development of armor surrogates and models.
- Adversary active protection systems to support the evaluation of operational effectiveness and lethality of Army weapon systems.
- Accredited digital environments and tools to support testing of mission threads and other system-of-systems architectures.
- Real-time casualty assessment capability to support evaluation of casualties due to blast effects on walls and bunkers.
- Equipment updates to capture and distribute audio-visual test data.
- An open-air range to support short- to long-range artillery engagements, in representative contested environments, with various munitions.
- Test ranges authorized to conduct open-air end-to-end lethality tests using depleted uranium rounds.
- Upgraded test fixtures and chemical testing referee systems to provide near real-time continuous air monitoring.
- Initiatives in test capabilities to support the testing of the new chemical, biological, nuclear, and radiological warfare protective suit.

DEPARTMENT OF THE NAVY

DOT&E oversees a subset of DoD systems and services intended to support naval warfare including amphibious systems, the newest surface and undersea naval warfare systems, naval airborne platforms, uncrewed systems, and missiles to include hypersonics. To support adequate evaluation of such systems, DOT&E has identified the following T&E resources requirements:

» REQUIRED RESOURCES

- Accurate test surrogates representing threat submarines, ships, and aircraft; modern threat jammers; and threat missiles and torpedoes.
- Threat surrogates for multi-stage anti-ship cruise missiles and large tactical aircraft.
- Additional aerial targets that respond to soft-kill defenses, multi-stage supersonic target, and standoff jammer aircraft.
- Submarine-representative set-to-hit torpedo target surrogate.
- Additional mobile ship targets to support the capacity of anti-ship missile testing.
- Synthetic undersea environment for unmanned undersea vehicles (UUVs) interoperable with other environments for multi-domain testing.
- Undersea threat emulators including countermeasures, torpedoes, and small (coastal/midget) submarines.
- Test ranges capable of testing the vulnerability of systems to emerging threats (i.e., hypersonics, UUVs).
- Digital threat representation integrated within test ranges supporting live-virtual-constructive end-

1 T&E resources include test facilities; instrumentation; equipment; ranges; tools; threats; targets; test assets; interfacing systems; digital tools and their VV&A; test teams; related support (e.g., friendly and threat operational forces, data collectors, analysts, subject matter experts); digital technologies (e.g., data repository); training materials; Federal, State, and local requirements; funding needed to plan, execute, and report on OT&E and LFT&E.

to-end system evaluation (e.g., electromagnetic spectrum offensive and defensive capability, scalable threat cruise missile representation, threat kinetic and non-kinetic self-defense systems including emerging capabilities).

- Representative naval topside electronics, emitters, and weapons systems for destructive testing.
- Increased capability and capacity in support of shock-hardened equipment testing.
- Faster small boat threat surrogates for destructive live fire test events.

DEPARTMENT OF THE AIR FORCE

DOT&E oversees a subset of DoD systems and services intended to support air warfare including fighters, bombers, mobility aircraft, rotary wing aircraft, airspace battle management, air-to-air, air-to-ground, and hypersonic weapons. To support adequate evaluation of such systems, DOT&E has identified the following T&E resources requirements:

» REQUIRED RESOURCES

- Advanced threat environments at ranges (including but not limited to, Nevada Test and Training Range, Point Mugu Sea Range) and enough throughput and connectivity to support testing and evaluation of complex mission scenarios, hypersonic, and force-on-force testing with Open-Air Battle Shaping (OABS), which integrates USAF and USN instrumentation systems.
- A dedicated Space Force range for electronic warfare testing with additional space-specific testing capabilities.
- Enhanced virtual environments and M&S capabilities to test on-orbit threats.
- Availability of operational terminals and systems.
- Capabilities (e.g., blue unmanned aircraft systems) to enable live testing of infrared missile warning systems and directed countermeasures.
- Qualified, specialized personnel to operate the test assets, analyze, and conduct tests on new space systems and technologies.

MULTI-SERVICE T&E RESOURCES

Common to systems and services across all Services, DOT&E has identified the following T&E resources requirements:

» REQUIRED RESOURCES

- Test ranges with enough throughput and capability of supporting the testing of several long-range missiles with telemetry and flight termination packages (e.g., Stand-in Attack Weapon, long-range fires, hypersonic weapons).
- Rapid and agile delivery of new and updated threat models informed by the intelligence community including class-of-capability radar and electronic attack emulator systems that can be programmed to stay ahead of the emerging threat and be tied into the range with OABS.
- Modern aerial targets (e.g., fourth- and fifth-generation fighter aircraft, large bomber and mobility aircraft, helicopters, electronic warfare, ground-based radars, airborne threat, software-defined radars, radio frequency and physical decoys, surface-to-air missiles, hypersonic missiles, and other emerging technologies and threat weapons).
- Capability to test representative densities and complex scenarios in anechoic chambers, hardware-in-the-loop labs, hybrid (digital range) environments, and open air test ranges.
- A facility to emulate modern radio frequency threats.
- High-fidelity cockpit, avionics, and weapons simulations of current and emerging red and blue aircraft delivered in time for integration into the Joint Simulation Environment (JSE) with full verification, validation, and accreditation (VV&A).

- A continuous VV&A process that enables the high-fidelity JSE to keep up with constant changes to platform, weapon, and battlespace entities.
- Additional, higher-fidelity and accredited live virtual constructive test environments.
- Multi-domain red and blue platforms, sensors, weapons modeling and simulation (M&S), and constructive effects that are tied into OABS via multi-level secure networks for testing of complex scenarios with representative long- and short-range kill chains.
- Capacity and certification to conduct frequent and simultaneous GPS jamming and spoofing across multiple test ranges.
- Missile defense capabilities including jamming equipment found on adversary ballistic missiles.
- Automated test tools including those for software, cyber, artificial intelligence (AI), and integrated T&E.
- Ability to conduct complex AI data collection and reduction, including infrastructure, tools, and personnel. AI software development tools and services to load, build, and test the various AI models.
- Improved capability to network open-air and ground test facilities to mirror an operational Combined Joint All-Domain Command and Control (C-JADC2) environment.
- Big data centers, data management infrastructure, and appropriate classified networks and workstations in SCI facilities across the T&E enterprise, including DOT&E.
- High-performance computing and high bandwidth and low-latency data transfer network architectures to support T&E data management challenges, compliance with the DoD Data Management Strategy, and the implementation of emerging digital tool capabilities for high-level mission effects analyses.
- Integrated data analytics to conduct data fusion and create a common operating picture from multiple sensors or ranges.
- Model-based engineering baseline for future digital T&E campaigns informed by live, virtual, and constructive testing.
- Capability to test and analyze 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.
- Electromagnetic pulse test capabilities for survivability and lethality evaluations.
- Range sustainability related to mitigation of any adverse effects due to off-shore wind-turbine generation impacting test ranges and T&E activities.
- Range sustainability related to detailed transition plans to address decreases in spectrum availability for test and training due to recent 5G-related sell-offs (including S- and L-bands) to commercial industry.
- A cyber-qualified workforce – including NSA-certified Red Teams – to keep pace with the increasing complexity and scale of cyber survivability testing. Increased cyber expertise in aggressing non-Internet Protocol networks and systems, identifying unauthorized users and spoofing attempts, assessing radio frequency data links, and supporting convergence of cyber and electromagnetic spectrum operations.
- Personnel across the OT&E and LFT&E enterprise with expertise in M&S, digital engineering, model-based systems engineering, electronic warfare, software, AI, and machine learning.

DOD PROGRAMS

This page intentionally left blank.

Aerosol and Vapor Chemical Agent Detector (AVCAD)

In April 2023, DOT&E published an operational assessment (OA) report that states, the Aerosol and Vapor Chemical Agent Detector (AVCAD) demonstrated the ability to detect chemical agents during testing, but in most cases did not meet detection requirements. AVCAD provides a new capability to detect aerosol agents that is not possible using the currently fielded Joint Chemical Agent Detector. AVCAD demonstrated reliability is substantially below the required level. The program office must mitigate several vulnerabilities to be survivable in contested cyberspace. DOT&E approved the Milestone C (MS C) Test and Evaluation Master Plan (TEMP) in June 2023, which requires additional development and operational testing on low-rate initial production systems to address deficiencies reported in the DOT&E OA.

SYSTEM DESCRIPTION

The AVCAD is an aerosol and vapor chemical warfare agent (CWA) and non-traditional agent detector. The Joint Services, without the Air Force, 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 warfare agents and support force-protection decisions. The AVCAD is designed to be powered by shore power, 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

AVCAD is a joint Acquisition Category III program which was authorized in June 2023 to enter the production and deployment phase. AVCAD provides a new capability to detect aerosol agents that is not possible using the currently fielded Joint Chemical Agent Detector. DOT&E approved the MS C TEMP to support the low-rate initial production decision in June 2023. The production and deployment phase of testing will begin in December 2023. The full-rate production decision is targeted for February 2025.

» MAJOR CONTRACTOR

- Smiths Detection, Inc. – Edgewood, Maryland

TEST ADEQUACY

DOT&E published an OA in April 2023. This assessment was based on a series of test events, as reported in the FY22 annual report, to include developmental test (DT), an OA, chamber testing, a DT Soldier Touch Point, and combined DT/operational test (OT) in FY22. Operational and chamber testing was conducted in accordance with DOT&E-approved plans. DOT&E observed all operational events. There were four different hardware and software configuration changes preventing a full dataset on the last configuration. Full retesting on the last configuration did not occur because it was known that the Materiel Developer wanted to continue to implement more changes such as software algorithm updates, hardware updates, and preventative maintenance updates. DOT&E supported the decision to enter the production and deployment phase of testing under the condition that regression testing on software and testing of hardware changes be performed on the production-representative version. Ship shock deficiencies were addressed, but still need to be re-tested. DOT&E coordinated with Service operational test agencies on the scope and scale of retesting detailed in the DOT&E-approved MS C TEMP.

PERFORMANCE

» EFFECTIVENESS

AVCAD demonstrated the ability to detect and identify aerosol and vapor CWAs, but in most cases, the system did not meet detection requirements. AVCAD detected CWAs at higher concentrations than required in the Capability Development Document. Performance results for aerosol agents varied significantly between systems with the same software and hardware configuration. AVCAD did not meet its false alarm rate requirement during the OA and demonstrated a propensity to false alarm in various operationally relevant environments.

AVCAD must overcome several challenges to be operationally effective. AVCAD demonstrated the ability to detect chemical agents, but in most cases, the system did not meet detection requirements. During chamber testing, AVCAD demonstrated the capability to detect agents in a majority of environmental conditions tested, including aerosolized agents that cannot be detected by the currently fielded system. However, AVCAD detected chemical agent at the required level in only 22 percent of the test cases. Despite this increased capability, the AVCAD would not provide sufficient early

warning time for unprotected forces. AVCAD detection performance varied significantly by individual detector. Early in testing, the AVCAD false alarm rate was meeting requirements in a variety of environments but did not meet the requirement after a software version change. The Materiel Developer expects this to be fixed for the next round of testing.

» SUITABILITY

AVCAD must overcome several challenges to be operationally suitable. AVCAD reliability was well below the required levels in all environments tested and did not improve during engineering and manufacturing development testing. AVCAD usability needs improvement due to reliability and communication challenges. AVCAD Operator training and the system technical manual should be updated to include step-by-step troubleshooting and maintenance instructions. The Air Force dropped out of the program because the reliability levels for their mission were insufficient. As noted in the FY22 Annual Report, the Joint Requirements Office was going to revisit the operational requirements after the Air Force left the program. This is currently ongoing.

» SURVIVABILITY

Testing identified AVCAD cyber vulnerabilities in electromagnetic environments and are detailed in the classified annex of the AVCAD OA, dated April 2023.

RECOMMENDATIONS

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

1. Improve the AVCAD probability of detection.
2. Reduce the AVCAD propensity to false alarm.
3. Improve AVCAD operational reliability, system-to-system variation, and usability.
4. Improve AVCAD technical manuals to aid in trouble shooting.
5. Mitigate the identified cyber vulnerabilities.
6. Continue to 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.

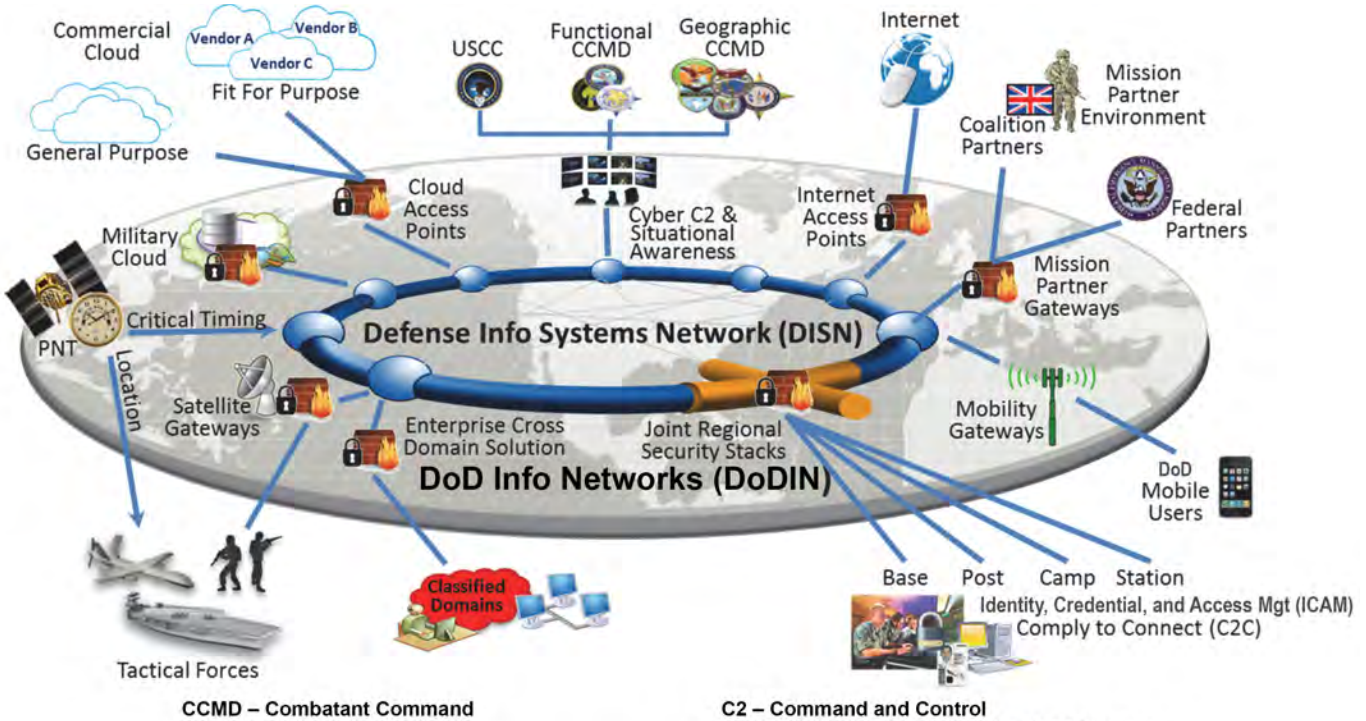
Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives

In March 2023, the DoD Chief Information Officer (CIO) established the DoD Information Enterprise Portfolio Management, Modernization and Capabilities (PM2C) Council, which it chairs, to govern aspects of the Department's information enterprise to include the Joint Warfighter Cloud Capability (JWCC) oversight and cloud rationalization initiative. This Council superseded the Digital Modernization Infrastructure (DMI) Executive Committee (EXCOM). The DoD CIO, Defense Information Systems Agency (DISA), and Services have been implementing programs, projects, and initiatives intended to achieve DoD Digital Moderation Strategy (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 if not adequately protected. Current DoD DMS efforts are intended to:

- Deliver a DoD enterprise cloud environment that leverages commercial technology and innovations
- Optimize DoD office productivity and collaboration capabilities, e.g., Enterprise Collaboration and Productivity Services (ECAPS) Capability Set 1 - Defense Enterprise Office Solution (DEOS) via Microsoft Office 365 (O365) on NIPRNet, SIPRNet, tactical, and training networks; Capability Set 2 - Business Voice and Video; and Capability Set 3 - Assured Command and Control Voice
- 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)



CCMD – Combatant Command
C2C – Comply to Connect
DoD – Department of Defense
ICAM – Identity, Credential, and Access Management
USCC – United States Cyber Command

C2 – Command and Control
DISN – Defense Information Systems Network
DoDIN – DoD Information Networks
PNT – Positioning, Navigation and Timing

PROGRAMS, PROJECTS, AND INITIATIVES

In March 2023, the DoD CIO established the DoD Information Enterprise PM2C Council, which it chairs, to govern aspects of the Department's information enterprise to include JWCC oversight and cloud rationalization initiative. Cloud rationalization is the DoD CIO effort to consolidate the Department's disparate cloud contracts under a single DoD umbrella contract. The PM2C Council convened its first meeting in August 2023. This Council superseded the previous DMS governance structure established in FY20 that consisted of the DMI EXCOM chaired by the DoD CIO, U.S. Cyber Command, and Joint Staff J6. The former Deputy SECDEF approved the DoD DMS in FY19.

DISA is the principal integrator for DoD Information Network enterprise capabilities, enabling initiatives, and testing. The DoD CIO, DISA, and Services intend to achieve DMS objectives by implementing programs, projects, and initiatives. The current funded programs, projects, and initiatives include:

- **Enterprise Collaboration and Productivity Services (ECAPS)** –The DEOS Program Office continued 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). In the future, the DEOS Program Office intends to work with the Services to implement solutions for tactical and training networks. In FY23, the DoD CIO and DISA began fielding DoD365 Integrated Phone System (DIPS) to support ECAPS Capability Set 2 (Business Voice and Video) by FY25. In FY21, the DoD CIO and DISA determined the solution for Capability Set 3 (Assured Command and Control Voice) to be the DISA-managed Enterprise Classified Voice over Internet Protocol (ECVoIP) service.
- **Identity, Credential, and Access Management (ICAM)** – The DoD CIO is the lead for ICAM governance to manage Enterprise ICAM efforts. In May 2023, the DoD CIO published the ICAM Governance Structure and Services memoranda. Enterprise ICAM is made up of three capability pillars: Identity Provider (IdP), Automated Account Provisioning (AAP), and Master User Record (MUR). In FY23, DISA continued integrating financial and other applications with the Enterprise ICAM capabilities on NIPRNet, deployed the Enterprise ICAM IdP on SIPRNet, and piloted Privilege Access Management (PAM) on NIPRNet. A major ICAM acquisition effort is the Public Key Infrastructure, detailed in this Annual Report.
- **Zero Trust** – The DoD intends to adopt a Zero Trust 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. The DoD CIO published an updated Zero Trust Strategy in September 2022. In 2QFY23, DISA completed development of the Thunderdome prototype, a suite of Zero Trust enabling capabilities that work in concert with existing identity management and cybersecurity tools. DISA awarded a Thunderdome production agreement in 4QFY23 and is implementing Thunderdome on NIPRNet and SIPRNet at DISA and other Defense agencies.
- **Joint Regional Security Stack (JRSS)** – In FY21, the DoD CIO began efforts to phase out JRSS and to transition to a new Zero Trust security and network architecture. The DoD intends to decommission JRSS by the end of FY27.
- **Mission Partner Environment (MPE)** – In support of DoD Directive 5101.22E, the Air Force is developing enterprise MPE services tailored to meet DoD mission partner information sharing needs, while supporting rationalization of combatant command existing MPE capabilities, such as Combined Enterprise Regional Information Exchange Systems (CENTRIXS). The Air Force is developing the Secret and Below Releasable Environment (SABRE) as the first modernized MPE capability platform. In May

2023, JITC accepted lead operational test agency (OTA) responsibilities and will work with the Air Force to develop an MPE SABRE test and evaluation strategy (TES). In FY23, the Air Force continued to integrate 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 employed SABRE as the U.S. enterprise capability for the MPE Interoperability Initiative 3.0 conducted during Bold Quest 23.2 in September 2023.

- **Enterprise Cloud Efforts** – The DoD continues to leverage commercial cloud innovations to deliver infrastructure and services for the DoD enterprise. In December 2022, the DoD awarded the JWCC multi-vendor contract designed to meet DoD enterprise cloud requirements. Congress directed the DoD in the FY23 National Defense Authorization Act (NDAA), Section 1553 to conduct cyber testing of secure DoD commercial clouds.

TEST ADEQUACY

- **ECAPS:** JITC intends to conduct an early operational assessment (EOA) on DoD365-Sec in 2QFY24. JITC intends to conduct a cyber assessment of DoD365-Sec and Global Federated User Domain (GFUD) for SIPRNet IdP in 1QFY24, per a DOT&E-approved cyber test plan. JITC supported initial developmental testing on DIPS in FY23. JITC has not been funded to conduct OT&E of ECAPS Capability Sets 2 and 3. In contrast to the FY22 annual report, DISA and JITC are no longer preparing a TES for ECAPS.
- **ICAM:** JITC conducted a developmental cyber assessment on MUR and AAP in a non-production infrastructure in November and December 2022. DISA did not fund JITC to conduct operational ICAM capability testing in FY23 and does not intend to fund JITC in FY24. There is no overarching Program Office or OTA supporting the various ICAM-related initiatives, which has made planning for tests to characterize the overall value and mission impact of the disparate initiatives difficult.
- **Zero Trust:** In January 2023, JITC conducted a limited EOA to assess NIPRNet Thunderdome prototype status toward achieving an operationally effective and suitable determination to inform a DISA fielding decision. The NIPRNet Thunderdome covers four of the seven DoD Zero Trust pillars. In 1QFY24, JITC plans to conduct a cyber assessment of the NIPRNet Thunderdome capabilities. DISA did not fund JITC to conduct operational SIPRNet Thunderdome capabilities testing in FY23 and does not plan to fund JITC in FY24; however, DISA intends to work with JITC to design a future operational test of the Thunderdome capabilities.
- **JRSS:** In May 2023, JITC completed a limited cyber assessment of the final JRSS capability upgrades per a JITC-approved test plan and has no plans for future JRSS testing.
- **MPE:** In January 2023, the Air Force conducted MPE developmental interoperability testing at an Air Force-contracted facility with mission partners.
- **Enterprise Cloud Efforts:** In 1QFY24, JITC plans to conduct threat-representative cyber-OT&E of the DoD365-Sec cloud infrastructure. This is the first cyber-OT&E of a DoD secure commercial cloud per the FY23 NDAA, Section 1553, which required such testing of DoD commercial clouds containing classified data. DOT&E intends to report the cloud-related cyber test findings in FY24.

PERFORMANCE

In FY23, the DoD CIO's decision to eliminate the DMI EXCOM as the DoD enterprise governance forum for aspects of DMS coordination resulted in less transparency, information sharing, and monitoring of DMS capability dependencies. There has been little operationally realistic testing performed to date 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.

RECOMMENDATIONS

The DoD CIO, Services, Director of DISA, and various DMS governance forums 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. Complete an MPE SABRE TES, and more generally develop a TEMP or TES for each funded DMS enterprise IT initiative.
4. Fund JITC to fully support DMS enterprise IT initiatives, testing, and test-related forums.
5. Perform threat representative cyber survivability testing of all DMS enterprise IT programs, projects, and initiatives in accordance with current DoD and DOT&E cyber survivability T&E guidance and policy, and use operational test data, analyses, and reporting to inform DMS governance decisions.
6. Conduct comprehensive cyber survivability testing of secure cloud environments per the FY23 NDAA, Section 1553.

DoD Healthcare Management System Modernization (DHMSM®)

In May 2023, the Joint Interoperability Test Command (JITC) conducted an FOT&E of the DoD Healthcare Management System Modernization (DHMSM) expanded revenue capabilities. The DHMSM Program Management Office (PMO) will begin fielding the MHS GENESIS to medical treatment facilities outside of the continental United States in September 2023 and anticipates completion of these fielding activities before the end of FY24. DHMSM® and MHS GENESIS® are registered trademarks of the DHMSM PMO.

SYSTEM DESCRIPTION

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

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

The DHMSM PMO began deploying the Revenue Cycle Expansion (RevX) component of MHS GENESIS in April 2022. RevX covers all revenue features, to include patient scheduling, registration, pre-authorization, medical coding, claims submission, billing, and payment processing. It introduces new capabilities and workflows to support patient accounting and billing.

MISSION

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

PROGRAM

DHMSM is an Acquisition Category ID program. DOT&E approved the Test and Evaluation Master Plan in October 2017, which describes testing to support the full deployment review and how T&E applies to the types of releases throughout the program life cycle.

In FY22, in response to DOT&E's FY21 recommendation, the program conducted an event to verify remediation of incident reports identified during previous operational testing. In August 2022, JITC conducted an operational assessment of RevX in Bremerton, Washington, at the request of the PMO, in order to identify potential critical risks prior to conducting an FOT&E event. In May 2023, JITC conducted the FOT&E of RevX in San Antonio, Texas, to evaluate operational effectiveness and suitability. This is the second FOT&E event, following the completion of the IOT&E in July 2018.

As of September 2023, the PMO reported that MHS GENESIS is deployed to 86 percent of healthcare facilities throughout the Defense Health Agency. The PMO continues to deploy RevX to new sites in conjunction with the initial Go-Live deployments of MHS GENESIS. RevX has also completed deployment to sites where MHS GENESIS had previously been deployed. MHS GENESIS is not currently capable of operating in a denied or disconnected communications environment. The MHS GENESIS Theater (MHSG-T) capability, currently being jointly developed by the DHMSM and Joint Operational Medicine Information Systems (JOMIS) PMO, is intended to be interoperable with MHS GENESIS while operating in a denied, degraded, intermittent, or limited communications (DDIL) environment. However, MHSG-T is not currently intended to be a backup to MHS GENESIS across all MHS GENESIS sites.

» MAJOR CONTRACTORS

- Leidos – Reston, Virginia
- Oracle Health – Austin, Texas (Millennium suite)
- Henry Schein ONE – American Fork, Utah (Dentrix Enterprise)
- Accenture Federal Services – Arlington, Virginia

TEST ADEQUACY

JITC conducted an OT&E of the RevX capabilities in May 2023 at Joint Base San Antonio medical treatment facilities in accordance with the DOT&E-approved test plan and observed by DOT&E. As planned, JITC did not conduct cybersecurity testing of MHS GENESIS during this test event; the DHMSM PMO is conducting ongoing persistent cyber operations of the system to help maintain and improve its cyber survivability.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E has not yet determined the operational effectiveness and suitability of RevX based on the FY23 operational testing but plans to release a report on its findings in 1QFY24.

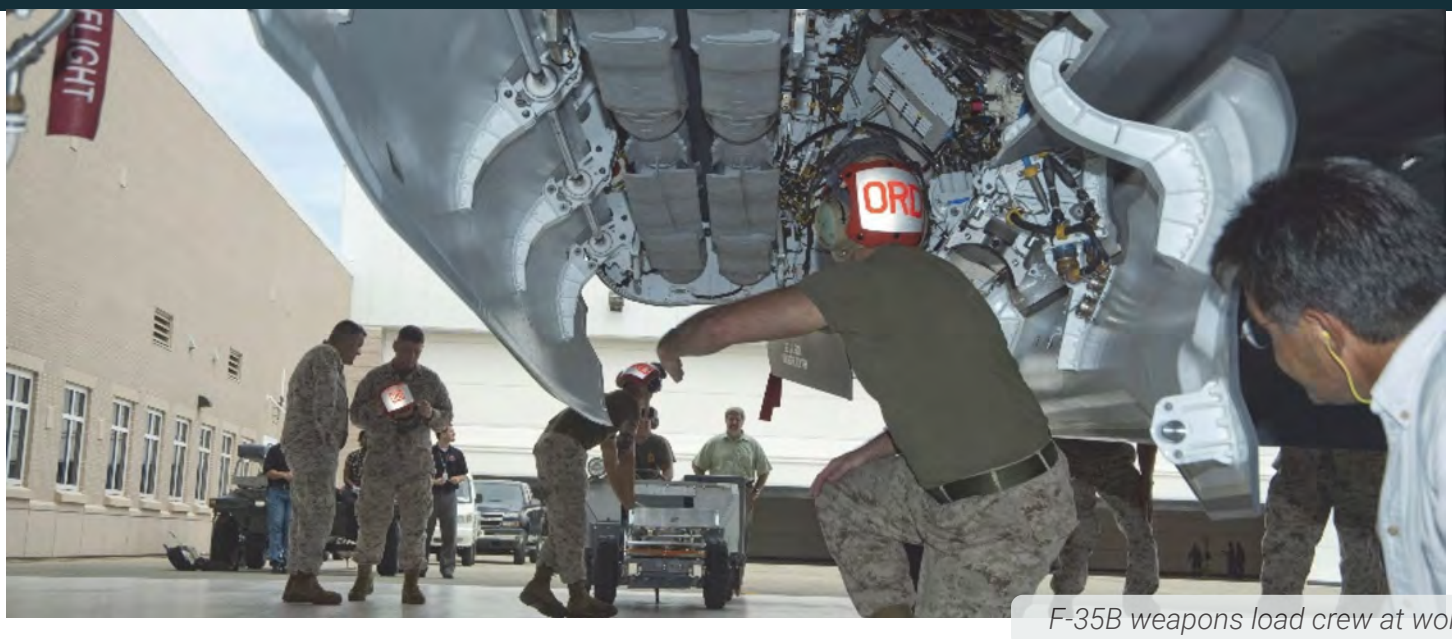
DOT&E will determine the cyber survivability of RevX during a future FOT&E.

RECOMMENDATIONS

The DHMSM PMO should:

1. Continue to work with JITC to verify the remediation of incident reports identified during previous operational test events.
2. Engage with the JOMIS PMO to explore the feasibility of using MHSG-T as a backup capability for MHS GENESIS at all MHS GENESIS facilities, to ensure continuity of care in a DDIL environment.

F-35 Joint Strike Fighter (JSF)



F-35B weapons load crew at work

During the period of this report, the F-35 program concluded preparations of the Joint Simulation Environment (JSE) for the 64 JSE test trials required to complete IOT&E. Test trials began and were completed in September 2023, three months later than the program's estimate reported in the FY22 Annual Report. As cited in last year's report, additional discoveries of deficiencies continued to delay readiness. The program certified the JSE as ready for operational test (OT) in September 2023 based on the Operational Test Agency (OTA) accreditation recommendation, with 65 remaining deficiencies against requirements carried into testing. The program plans to correct these deficiencies prior to and concurrent with using the JSE for Block 4 OT.

The F-35 program development cycle continues to experience delays due to immature and deficient Block 4 mission systems software and avionics stability problems with the new Technology Refresh 3 (TR-3) hardware going into Lot 15 production aircraft. As a result, deliveries of production Lot 15 aircraft in the TR-3 configuration are on hold until more testing can be completed and the avionics issues resolved. Additionally, these delays prevented the F-35 Joint Program Office (JPO) from adequately planning and programming for hardware modifications for OT of the upgraded hardware configuration. Furthermore, the necessary flight test instrumentation (FTI), including both aircraft and Open-Air Battle Shaping (OABS) instrumentation, for both the remaining TR-2 and upgraded TR-3 OT aircraft, are not all on contract and will not be available in time. As a result, the F-35 JPO is contracting an interim FTI solution to allow OT squadrons to have some data recording capability until sufficient test aircraft with full data recording capability become available.

SYSTEM DESCRIPTION

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

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

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

MISSION

Combatant commanders 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, and in heavily defended areas.

PROGRAM

The F-35 JSF is an Acquisition Category ID program. DOT&E approved the fourth revision of the System Development and Demonstration (SDD) Test and Evaluation Master Plan (TEMP), which governs the conduct of IOT&E, in March 2013.

A separate F-35 Overarching Block 4 TEMP and associated annexes govern the conduct of FOT&E. DOT&E approved the F-35 Overarching Block 4 TEMP and Increment 1 Annex in May 2020. The Increment 1 Annex covered the Block 4 developmental and operational flight testing of software versions 30R03 through 30R06, which were completed in FY21. Increment 2 Annexes, which cover Block 4 software versions 30R07, 30R08, and 40R01, and their associated hardware enablers, including the transition from TR-2 to TR-3 equipped aircraft in the production line, were approved in October and December 2022. As reported in the FY22 Annual Report, Increment 3 Annexes, which cover Block 4 software versions 40R02, 41R01, and 42R01, and their associated hardware enablers are in coordination with the F-35 JPO, the Services, and DOT&E.

» MAJOR CONTRACTORS:

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

F-35A live air-to-air missile shot

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

F-35 Development Phase	Major Avionics Hardware	Capabilities	Mission Systems Software	Operational Testing*
SDD	TR-1	Block 2B	Block 2B Software	• Marine Corps Fielding Reports and F-35B IOC • Service and JOTT test events • Formal OUE canceled
	TR-2	Block 3i	Block 3i Software	• Air Force Fielding Reports and F-35A IOC • Service and JOTT test events
		Block 3F	Block 3F/ 3FR6**	**Pre-IOT&E Increment 1 (Jan – Feb 2018) Cold Weather Deployment** For-score testing to evaluate the suitability of the F-35 air system and alert launch timelines in an extreme cold weather environment
			Block 3F/ 30R00***	• Navy Service Fielding Reports • **Pre-IOT&E Increment 2 (Starting Mar 2018)** For-score testing of limited two-ship mission scenarios, F-35A deployment, F-35C deployment to a carrier, and weapons delivery events
C2D2		Block 4, 30 Series	30R02.04	**Portion of Formal IOT&E (Dec 2018 – Sep 2019)** 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 completed their evaluation of this series of software 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 approved four missile test events from the OT plan for 30R08; no other testing has been approved due to lack of readiness. No OT of 30R08 has been completed to date.
	TR-3	Block 4, 40 Series	40R0X	Dedicated OT events are planned for each release of capability in the series

Notes:

* **Bold** text highlights for-score IOT&E events.
** 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; IAW – in accordance with; IOC – Initial Operational Capability; JOTT – JSF Operational Test Team; OUE – Operational Utility Evaluation; OT – operational test; SDD – System Development and Demonstration; TR-X – Technology Refresh [version #], referring to the suite of various avionics and supporting subsystems; UOTT – U.S. Operational Test Team

TEST ADEQUACY

» IOT&E

Open-Air Testing

The F-35 program is nearing completion of a multi-year IOT&E which began in 2018. The JSF Operational Test Team (JOTT) completed, and DOT&E observed, a series of weapons trials (both bombs and missiles) and open-air test missions to evaluate the F-35 in multiple roles (i.e., offensive counter-air, defensive counter-air, 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 finished with completion of the final AIM-120 missile trial in June 2021 when the program delivered software version 30R06.042 with the fixes needed to complete the trial.

Modeling and Simulation - JSE

Throughout FY23, the JSE and OT teams focused on preparations to conduct runs for score in the JSE. The JPO completed the OT readiness review for JSE trials in September 2023, and certified it as ready for testing, despite 65 deficiencies against the baseline JSE requirements, including the F-35-in-a-box (FIAB) model, the battlespace environment, and other threat and friendly models used in the simulation. The JPO and JSE teams intend to address these deficiencies prior to or in conjunction with Block 4 testing in the JSE. The F-35 Executive Committee (EXCOM) accredited JSE, with limitations, for IOT&E on September 1st, 2023. DOT&E assessed the mitigations for the deficiencies, determined the testing would be adequate, and approved the remaining portion of the IOT&E plan to allow JSE testing to proceed. Test missions for score began and were completed in September 2023.

The remaining IOT&E events were completed in September and included 64 test trials in the JSE at Naval Air Station Patuxent River, Maryland. These trials included 11 defensive counter-air, 22 cruise missile defense, and 31 combined offensive counter-air/air interdiction/DEAD trials in operationally representative scenarios with modern threat systems that are not available on open-air ranges. All three F-35 variants were involved in the conduct of these trials.

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

» FOT&E

Block 4 Open-Air Testing

The U.S. Operational Test Team (UOTT) completed OT of software version 30R07 in June 2022 in accordance with the DOT&E-approved test plan. DOT&E observed the test. The UOTT submitted an OT plan for 30R08, but DOT&E only approved four weapon events in the plan in February 2023, due to the lack of readiness of key requirements

such as flight test instrumentation, aircraft modifications, and OABS, which are needed to conduct other testing in the plan. As reported in the FY22 Annual Report, no OT of 30R08 has been completed from the test plan.

Per the Block 4 TEMP and associated annexes, OT aircraft are required to support both developmental test (DT) and OT in various Block 4 configurations. Modifications to these aircraft must be funded, scheduled, and completed just after DT aircraft modifications to enable integrated DT/OT, DT assist, and mission-level OT of capabilities. Although the JPO has funded and contracted for some of the OT aircraft modifications, it does not yet have a scheduled and coordinated plan to ensure that all 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 the TR-3 configuration. Because of these issues, the UOTT has been unable to conduct OT events of the 30R08 capabilities as required in the test plan. The JPO and OT organizations plan to conduct an updated readiness review in 1QFY24.

The UOTT began making plans for OT of the first TR-3 production configuration, with aircraft software version 40R01, but the program's DT effort is significantly behind schedule. The UOTT will be providing two OT aircraft in a DT assist role in FY24 to accelerate the DT baseline plan and allow early OT exposure to TR-3 testing. Major hardware changes with the TR-3 transition include upgraded integrated core processors, aircraft memory system, next generation distributed aperture system, and a panoramic cockpit display. The program planned to deliver aircraft in the TR-3 configuration beginning in Lot 15, in July 2023, but DT schedule delays have pushed the U.S. Services' acceptance of these aircraft into FY24. In FY23, just 32 of 205 baseline DT flights were completed after the first DT flight in January 2023. Delays caused by aircraft modifications, software maturity, avionics architecture instabilities, and ongoing troubleshooting and debugging have all contributed to the slow progress in development. The JPO and the Services are not accepting deliveries of aircraft in the TR-3 configuration until the problems are resolved enough to complete DT.

Block 4 Modeling and Simulation Development - JSE

The extended delay in completing the necessary verification, validation, and accreditation of the F-35 JSE for conducting IOT&E test missions delayed preparations for OT of Block 4. Licensing issues associated with the FIAB have also contributed to the delayed JSE modernization efforts. To support OT requirements, the JPO needs to align updated FIAB deliveries with the Block 4 OT periods as soon as possible. This alignment is needed so that the OT teams can use the JSE to accomplish critical testing of future capabilities, beginning with the 30R08 release that is currently in developmental and operational flight test. In addition, the program must account for new capabilities in upgrades to the FIAB, the environment, blue and red weapons models, and red ground threat models, as well as correcting the 65 remaining deficiencies against JSE requirements carried over from the IOT&E configuration.

Suitability Testing

In August 2023, DOT&E approved the UOTT's limited Autonomic Logistics Information System (ALIS) disconnected operations test plan, which included the scenario of disconnecting the Standard Operating Unit (SOU) from flight line operations. The test plan did not cover other off-line conditions, so DOT&E directed that additional scenarios be tested later.

No other operational suitability test plan was approved by DOT&E in FY23.

Cyber Survivability Testing

In FY23, the UOTT cyber test teams conducted cyber survivability assessments of ALIS software version 35P21.Q4 and supporting functionality (both a cooperative vulnerability and penetration assessment and an adversarial assessment). Four additional cyber survivability tests were planned to be accomplished in

FY23, but were moved to FY24 due to test team readiness and asset availability issues.

AV test assets are made available to support AV tests, which are limited in scope based on the potentially disruptive nature of cyber tests. However, more robust and representative AV cyber tests are needed, which will involve Service and JPO programmatic investment in requisite hardware- and software-in-the-loop capabilities. Cyber survivability testing is also often limited by available trained and qualified test personnel, so Service OTAs should improve staffing levels.

PERFORMANCE

» IOT&E

Effectiveness, Suitability, and Survivability

The results of operational effectiveness, suitability, and survivability testing from IOT&E will be reported in the DOT&E IOT&E report, expected in 2QFY24.

» FOT&E

Effectiveness

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

Due to the lack of testing on the 30R08, DOT&E is unable to assess its operational effectiveness. The OT teams have flown with immature versions of the 30R08 software to support developmental and operational assessments of capabilities and have participated in large force exercises to assess integration and interoperability with other aircraft. However, this testing has not been adequate to evaluate effectiveness of the 30R08 capabilities in mission-level scenarios.

The OT teams have also conducted weapons integration and employment characterization testing to support the overall development effort, but these events have not been adequate to satisfy the DOT&E-approved weapons delivery events in the test plan.

Block 4, TR-3, 40 Series Development

The program began developmental flight testing of the TR-3 configuration in January 2023, with software version 40R01. This version of software was developed using the baseline capabilities provided in the 30R07 software, which completed development in 1QFY22. The ongoing avionics stability problems with the TR-3 configuration have delayed the integration of 30R08 software capabilities and 40R0X hardware and software.

Suitability

Reliability, Maintainability, and Availability

The operational suitability of the F-35 fleet remains below Service expectations and requirements. In FY23, aircraft availability was slightly below that in FY22, after declining for most of FY21 despite reaching a historic program high in January 2021.

As of the end of September 2023, 628 aircraft have been produced for the U.S. Services. These aircraft do not include any aircraft assigned to dedicated DT 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 2023. 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 OT) was 51 percent. The DOT&E assessment shows a relatively flat trend for the 12 months of data in FY23.

Availability tracks aircraft capable of performing at least one designated F-35 mission and may not represent the capability to execute desired missions for combat or for specific OTs. The Full Mission Capable (FMC) rate tracks what proportion of F-35s are capable of executing all assigned missions and provides a better evaluation of combat readiness. For the 12-month period ending September 2023, the FMC rate for the whole U.S.

fleet was 30 percent, and the rate for the OT fleet was 9 percent.

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 OT. The proportion of the fleet that is combat-coded has risen steadily over time and represents slightly more than half of the U.S. fleet over the 12 months ending in September 2023. 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. However, unlike in FY22, the combat-coded fleet did not achieve the 65 percent target for monthly average availability for the overall, combined 12 months ending in September 2023. Instead, the combat-coded fleet attained an average monthly availability of 61 percent, and only achieved or surpassed the 65 percent goal in one of the 12 months. The FMC rate of the combat-coded fleet over the same 12-month period was 48 percent, compared to 30 percent for the entire U.S. fleet.

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), or 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 FY23. For the 12 months ending in September 2023, the average monthly NMC-S rate was 27 percent, slightly worse than the overall rate in FY22. The average monthly NMC-M rate for the 12 months ending in September 2023 was 15 percent. 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, adhesive cure times for attaching hardware such as nutplates, and spares posture for those critical items most in demand. The program should also focus reliability improvements on the components most often not immediately available in supply.

As previously reported, the significant shortage of fully functional F135 engines had contributed to reduced aircraft availability, particularly for the F-35A variant. Aggressive program efforts to lay in additional depot resources, improve depot efficiencies, and ruggedize key engine components have reduced the number of aircraft without an engine and increased the number of spare modules ready for issue. However, despite those efforts, other degraders such as canopy and egress system issues have contributed to stagnant, or slightly declining, availability.

The F-35 fleet remains below JSF Operational Requirements Document (ORD) thresholds in some areas for overall reliability and maintainability. Maintenance data gathered through May 2023 from the U.S. fleet of all three variants show that the F-35C is not meeting any of the ORD reliability and maintainability requirements for mature aircraft. The F-35A meets two and the F-35B meets one of the three 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 through 5 show the values of the reliability metrics, and Tables 6 and 7 show the values of the maintainability metrics, respectively, based on data aggregated in three-month rolling windows, where monthly reports are generated based on the last three months of data. This process enables trends to be observed more clearly than reports generated by only a single month of data. The tables also show the metric values for the three-month period ending May 2022 for comparison, as well as the component or system drivers

most significantly degrading that metric's performance.[1]

In Table 2, Mean Flight Hours Between Critical Failure (MFHBCF) includes all failures that render the aircraft unsafe to fly, along with any equipment failures that would prevent the completion of a defined F-35 mission. It includes failures discovered in the air and on the ground. Historically, MFHBCF has fluctuated widely for the F-35, showing little year-to-year trends.

Table 2. Reliability Measure: Mean Flight Hours Between Critical Failures (MFHBCF)

F-35 Reliability: MFHBCF (hours)								
Variant	ORD Threshold		Values as of May 31, 2023			Values as of May 2022		Trend**
	Flight Hours	MFHBCF	Cumulative Flight Hours	Observed MFHBCF* (3 Months Rolling Window)	Observed Value as Percent of Requirement	Cumulative Flight Hours	Observed MFHBCF* (3 Months Rolling Window)	May 2023 Compared to May 2022
F-35A	75,000	20	288,926	10.5	53%	245,317	10.1	↑
F-35B	75,000	12	106,553	11.1	93%	89,469	8.8	↑
F-35C	50,000	14	62,192	9.6	69%	53,067	16.2	↓

Drivers (by frequency): troubleshooting (including software stability), attaching hardware (including nutplates), wires/tubes/ducts/fiber optics, throttle grip, aircraft memory device, LO repair, standby flight display, refueling door, position lights

Notes:
* Red = Does Not Meet Threshold Requirement; Green = Meets Threshold Requirement
** For Reliability Metrics, Trend ↑ = Improved; Trend ↓ = Worse; Trend ↔ = Flat

Acronyms: LO – Low Observable; ORD – Operational Requirements Document

1 All reliability metrics in this report are calculated as mean flight hours between events. DOT&E notes that these metrics are based on a fleet with a relatively low FMC rate, which means they are flying with many failed components awaiting resupply. The low FMC rate effectively skews the resulting metrics to look more reliable than a fleet that has failed components replaced quickly.

In Table 3, Mean Flight Hours Between Removal (MFHBR) indicates the degree of necessary logistical support and is frequently used in determining associated costs. It includes any removal of an item from the aircraft for replacement, except for consumables like fasteners. Not all removals are failures; some removed items are later determined to have not failed when tested at the repair site, and other components can be removed due to excessive signs of wear before a failure, such as worn tires.

Table 3. Reliability Measure: Mean Flight Hours Between Removal (MFHBR)

F-35 Reliability: MFHBR (hours)								
Variant	ORD Threshold		Values as of May 31, 2023			Values as of May 2022		Trend**
	Flight Hours	MFHBR	Cumulative Flight Hours	Observed MFHBR* (3 Months Rolling Window)	Observed Value as Percent of Requirement	Cumulative Flight Hours	Observed MFHBR* (3 Months Rolling Window)	May 2023 Compared to May 2022
F-35A	75,000	6.5	288,926	7.0	108%	245,317	6.8	↑
F-35B	75,000	6.0	106,553	4.7	78%	89,469	4.0	↑
F-35C	50,000	6.0	62,192	4.7	78%	53,067	5.6	↓

Drivers (by frequency): nose & main landing gear tires, ejection seat assembly, brake assembly, seat survival kit, crash survivable memory unit, throttle grip, divergent exhaust nozzle segments & seals, backup oxygen bottle, position lights

Notes:
* Red = Does Not Meet Threshold Requirement; Green = Meets Threshold Requirement
** For Reliability Metrics, Trend ↑ = Improved; Trend ↓ = Worse; Trend ↔ = Flat

Acronyms: ORD – Operational Requirements Document

Aviation Boatswain's Mate signals F-35B on USS America *(LHA 6)*

In Table 4, Mean Flight Hours Between Maintenance Events Unscheduled (MFHBME_Unsch) is a reliability metric for evaluating maintenance workload due to unplanned maintenance. Maintenance events are either scheduled (e.g., inspections or planned part replacements) or unscheduled (e.g., failure remedies, troubleshooting, replacing worn parts such as tires). MFHBME_Unsch is an indicator of aircraft reliability and must meet the ORD requirement.

Table 4. Reliability Measure: Mean Flight Hours Between Maintenance Events Unscheduled (MFHBME_Unsch)

F-35 Reliability: MFHBME_Unsch (hours)								
Variant	ORD Threshold		Values as of May 31, 2023			Values as of May 2022		Trend**
	Flight Hours	MFHBME_ Unsch	Cumulative Flight Hours	Observed MFHBME_ Unsch* (3 Months Rolling Window)	Observed Value as Percent of Requirement	Cumulative Flight Hours	Observed MFHBME_ Unsch* (3 Months Rolling Window)	May 2023 Compared to May 2022
F-35A	75,000	2.0	288,926	2.2	110%	245,317	2.1	↑
F-35B	75,000	1.5	106,553	1.8	120%	89,469	1.7	↑
F-35C	50,000	1.5	62,192	1.2	80%	53,067	1.5	↓

Drivers (by frequency): troubleshooting (including software stability), LO repair, attaching hardware (including nutplates), nose & main landing gear tires, wires/tubes/ducts/fiber optics, LO system seals, maintenance & refueling door, landing gear struts

Notes:
* Red = Does Not Meet Threshold Requirement; Green = Meets Threshold Requirement
** For Reliability Metrics, Trend ↑ = Improved; Trend ↓ = Worse; Trend ↔ = Flat

Acronyms: LO – Low Observable; ORD – Operational Requirements Document

F-35C lands on USS Carl Vinson *(CVN 70)*

In Table 5, Mean Flight Hours Between Failure, Design Controllable (MFHBF_DC) includes failures of components due to design flaws under the purview of the contractor, such as the inability to withstand loads encountered in normal operation.

Table 5. Reliability Measure: Mean Flight Hours Between Failure, Design Controllable (MFHBF_DC)

F-35 Reliability: MFHBF_DC (hours)								
Variant	JCS Threshold		Values as of May 31, 2023			Values as of May 2022		Trend**
	Flight Hours	MFHBF_DC	Cumulative Flight Hours	Observed MFHBF_DC* (3 Months Rolling Window)	Observed Value as Percent of Requirement	Cumulative Flight Hours	Observed MFHBF_DC* (3 Months Rolling Window)	May 2023 Compared to May 2022
F-35A	75,000	6.0	288,926	12.2	203%	245,317	10.6	↑
F-35B	75,000	4.0	106,553	6.7	168%	89,469	6.3	↑
F-35C	50,000	4.0	62,192	3.4	85%	53,067	8.8	↓

Drivers (by frequency): DAS sensor, EOTS window cover, throttle grip, fiber channel switch, canopy assembly, 80 kW inverter/converter/controller, divergent exhaust nozzle segments and seals, manifold filter, power and thermal management system

Notes:
* Red = Does Not Meet Threshold Requirement; Green = Meets Threshold Requirement
** For Reliability Metrics, Trend ↑ = Improved; Trend ↓ = Worse; Trend ↔ = Flat

Acronyms: DAS - Distributed Aperture System; EOTS - Electro Optical Targeting System; JCS – Joint Contract Specification

F-35A maintainer at work

In Table 6, Mean Time to Repair (MTTR) measures the average active maintenance time for all unscheduled maintenance actions. It is a general indicator of the ease and timeliness of repair.

Table 6. Maintainability Measure: Mean Time to Repair (MTTR)

F-35 Maintainability: MTTR (hours)					
Variant	ORD Threshold	Values as of May 31, 2023* (3 Months Rolling Window)	Observed Value as Percent of Threshold	Values as of May 2022* (3 Months Rolling Window)	Trend** May 2023 Compared to May 2022
F-35A	2.5	5.2	208%	5.2	↔
F-35B	3.0	6.7	223%	7.2	↓
F-35C	2.5	5.6	224%	5.9	↓

Drivers (by Sum Elapsed Maintenance Time): LO repair, attaching hardware (including nutplates), LO system seals, canopy assembly, wires/tubes/ducts/fiber optics, three-bearing swivel module, maintenance & refueling door, position lights

Notes:
* Red = Does Not Meet Threshold Requirement; Green = Meets Threshold Requirement
** For Maintainability Metrics, Trend ↑ = Worse; Trend ↓ = Improved; Trend ↔ = Flat

Acronyms: LO – Low Observable; ORD – Operational Requirements Document

F-35A pilot ground operations

In Table 7, Mean Corrective Maintenance Time for Critical Failures (MCMTCF) measures active maintenance time to correct only the subset of failures that prevent the F-35 from being able to perform a specific mission. It indicates the average time for maintainers to return an aircraft from Non-Mission Capable to Mission Capable status.

Table 7. Maintainability Measure: Mean Corrective Maintenance Time for Critical Failures (MCMTCF)

F-35 Maintainability: MCMTCF (hours)					
Variant	ORD Threshold	Values as of May 31, 2023* (3 Months Rolling Window)	Observed Value as Percent of Threshold	Values as of May 2022* (3 Months Rolling Window)	Trend** May 2023 Compared to May 2022
F-35A	4.0	8.0	200%	7.4	↑
F-35B	4.5	12.5	278%	11.5	↑
F-35C	4.0	9.3	233%	11.8	↓

Drivers (by Sum Elapsed Maintenance Time): attaching hardware (including nutplates), wires/tubes/ducts/fiber optics, LO repair, canopy assembly, position lights, engine assembly, radar, position lights, communication/navigation/identification system

Notes:
* Red = Does Not Meet Threshold Requirement; Green = Meets Threshold Requirement
** For Maintainability Metrics, Trend ↑ = Worse; Trend ↓ = Improved; Trend ↔ = Flat

Acronyms: LO – Low Observable; ORD – Operational Requirements Document

ALIS and Operational Data Integrated Network (ODIN)

ALIS is the 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. ODIN is the migration of ALIS applications into a cloud-based environment hosted on updated hardware. New ODIN applications are planned to add capabilities and improve cyber survivability.

In FY23, 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 SOU to the ODIN Base Kit (OBK), reached selected field units in FY22, but was delayed by contracting and production of the remainder of the legacy hardware-equipped units. Original plans were to have OBKs to the remaining squadrons by September 2023, but current projections place the complete transition from SOUs to OBKs in 2025.

The path to ODIN, which will be the software bundle ported from the legacy ALIS hardware systems into the OBKs to formalize the ODIN software and hardware system, follows three steps:

- Step one, referred to as ALIS 21.Q4, is the current release of ALIS software, which finished fielding in July 2023, representing a roughly 1.5-year delay from the originally planned release date laid out by the program in FY21.
- Step two, referred to as ALIS 22.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 releases.

ALIS 22.Q4 is now projected for release in sub-phases (dot releases) beginning 3QFY24. The first increment, 22.Q4.1, will focus on burning down identified cyber issues and TR-3 compatibility. Follow-on dot releases are being investigated to deliver needed capabilities to the field.

- The final step in the path to an ODIN Minimum Viable Capability Release occurs after a rehost of ALIS 22.Q4 into the ODIN format. This was to begin testing by the Integrated Test Force in July 2023 but is now projected to begin at some point in FY25.

ALIS provides units the ability to evaluate the Low Observable (LO) characteristics of their aircraft, given damages and repairs accumulated in service, via an LO Dedicated System Processor (DSP). Units require a functioning LO DSP to determine whether their aircraft have an adequate LO signature for missions relying on these characteristics. However, LO DSP reliability issues are hindering the fleet's ability to track the LO status of fielded F-35 aircraft. As an example, during FY23, two of the three OT squadrons were without a functional LO DSP for extended periods of time. When an LO DSP fails, the backorder time to receive a replacement is also significant.

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 capture AV software instability events in the Computerized Maintenance Management System (CMMS). While pilots can manually document instability events, they do so 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 events are not captured and reflected in the metrics, the effect of these events is clearly under-reported. Currently, only proprietary tools used by contractor field service engineers can identify pilot-initiated reset events. In order to improve F-35 aircraft mission systems stability, ODIN will need to have the capability to automatically document pilot-initiated resets of mission systems.

In August 2023, the UOTT conducted eight days of a formal test of F-35 aircraft operations and maintenance with the ALIS squadron kit offline. This partially satisfies the DOT&E adequacy requirement to test the ability of an F-35 unit to conduct operations with ALIS or ODIN disconnected from their supporting infrastructure, as required in the TEMP. Further testing in additional ALIS or ODIN degraded conditions must still be conducted to fully satisfy DOT&E adequacy of test requirements. Preliminary results of this test also highlight the need to formally test agile combat employment operations in which small detachments of F-35 aircraft may have to operate for significant periods of time without on-site access to an SOU or OBK.

Survivability

Twelve ALIS cyber survivability deficiency reports were verified as being fixed during FY23 testing; however, numerous cyber survivability deficiencies remain across the F-35 program. To address the deficiencies, the JPO invested in cyber mitigations associated with recent JOTT testing, and key test findings are being tracked to closure by the Authorizing Official for ALIS and ODIN. Lack of access to proprietary information for government support contractor cyber survivability testers, overall test team capacity constraints, and test asset availability impeded execution of several planned tests in FY23, requiring their rescheduling for FY24 or later. 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 cyber survivability testing on AV components and support systems.

The F-35 JPO is using Development Security Operations (DevSecOps) and Agile software methods to advance frequent software updates to the field in support of the ODIN path forward. The Block 4 30RXX and 40RXX software version development process is also providing more frequent operational flight profile software updates to the combat forces than during the SDD phase. An increased frequency of new software deployments is

stressing the capacity of cyber test teams to thoroughly evaluate each update and will continue to stress future capacity without appropriate mitigation.

In light of current cyber threats and vulnerabilities, along with peer and near-peer threats to operating bases and communications, DOT&E continues to require the F-35 program and Services conduct testing of aircraft operations without access to the ALIS SOU as required in the TEMP, which is also a suitability testing requirement. The program has yet to meet this requirement and is currently in the planning stages for complete testing of the ALIS Contingency Operations Plan, which will test standardized procedures for lack-of-connectivity scenarios and is intended to satisfy the requirement.

Emerging candidates for cyber survivability testing are continually assessed, updated, and incorporated into test plans, to include insights into prioritization from a Mission-Based Cyber Risk Assessment commencing in 1QFY24. Additionally, including emulation of cyber effects from actual testing into mission rehearsals in the JSE is key to assessing potential mission consequences from cyber exploits against the AV.

RECOMMENDATIONS

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

1. Expedite preparations for required F-35 follow on operational testing in the JSE beginning with the 30R08 capability release.
2. As recommended in the FY22 Annual Report, develop and begin executing detailed planning for upgrading the JSE in time 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 to ensure test adequacy.
3. In accordance with the DOT&E-approved Block 4 TEMP:
   - As recommended in the FY22 Annual Report, fully fund, develop, and update the detailed plan to modify all OT aircraft with the appropriate capabilities, life limit, and instrumentation, including OABS requirements.
   - As recommended in the FY22 Annual Report, continue work to 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. As recommended in the FY22 Annual Report, continue to pursue maintenance system improvements, especially for common processes distributed among Non-Mission Capable Maintenance drivers, such as low observable repairs, adhesive cure times for attaching hardware such as nutplates, and spares posture for those critical items most in demand.
5. As recommended in the FY22 Annual Report, 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.
6. As recommended in the FY22 Annual Report, 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.
7. As recommended in the FY22 Annual Report, ensure both DT and OT for ALIS and ODIN are adequately resourced to reduce the high risk associated with fielding an immature and inadequately tested replacement.
8. As recommended in the FY22 Annual Report, conduct more in-depth cyber survivability testing of the AV, ALIS/ODIN, training systems, and eventually JSE; provide dedicated hardware- and software-in-the-loop AV cyber-test assets that can be used for the full extent of cyber testing; introduce the ability for JSE to emulate cyber effects during mission rehearsals.
9. As recommended in the FY22 Annual Report, correct program-wide deficiencies

identified during cyber survivability testing in a timely manner and verify corrections within ALIS prior to rehosting ALIS software on ODIN.

10. As recommended in the FY22 Annual Report, develop and routinely report software sustainment and stability metrics that show how well the program's overall software development capability for the AV and logistics sustainment system is progressing. In particular, incorporate the ability of the aircraft's prognostics health management to detect pilot-initiated resets of mission critical systems in flight and produce records in CMMS to more accurately track AV system stability.
11. Since cyber survivability testing is often limited by available trained and qualified test personnel, Service OTAs should continue to work improve staffing levels.

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

The Global Command & Control System – Joint (GCCS-J) family of systems has been broken into two separate acquisition programs: GCCS-J and Joint Planning and Execution System, which is being reported on in a separate article. In FY23, GCCS-J fielded v6.1.0.0, providing a significant upgrade to the GCCS-J program. DOT&E is analyzing data collected during operational testing in FY23, plans to observe further testing in FY24, and will report on operational effectiveness, suitability, and cyber survivability in 3QFY24.

SYSTEM DESCRIPTION

GCCS-J is a software-based system with commercial off-the-shelf and government off-the-shelf software and is highly modular, allowing 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.

MISSION

GCCS-J enables joint commanders to accomplish command and control by:

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

PROGRAM

The GCCS-J Program Management Office (PMO) fielded version v6.1.0.0 as a significant upgrade to the existing fielded version of v6.0.1.x. During FY23 operational testing, users identified impactful upgrades that have been added for future development. As the PMO continues development of the v6.1.x baseline, GCCS-J will field user-identified capabilities through the Development, Security, and Operations (DevSecOps) process as part of their Agile software development framework.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

In FY23, the Joint Interoperability Test Command (JITC) conducted one operational test which was observed by DOT&E, for GCCS-J v6.1.0.x. The GCCS-J v6.1.0.0 Operational Test included representative hardware, software, real-world data, and operational end users that exercised system administration, COP, and intelligence user mission tasks. Testing focused on the capabilities and interfaces available at U.S Central Command (USCENTCOM) and U.S. Southern Command (USSOUTHCOM). Test cases were developed with direct input from users at both combatant commands. Additional combatant and lower echelon commands with site specific test cases will be tested as these commands migrate to v6.1.0.x.

The GCCS-J integrated test environment does not currently capture the mission configurations associated with each Combatant Command and other critical sites. As reported in the FY22 Annual Report, GCCS-J test strategies need to be developed to encompass the agile nature of the product and varying operational site configurations to inform the update to the Test and Evaluation Master Plan (TEMP) and the Agile Operational Master Test Plan (AOMTP). Additionally, the TEMP update for the GCCS-J program should detail operational cyber survivability tests that include cooperative vulnerability and penetration assessments (CVPAs) followed by adversarial assessments (AAs).

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

DOT&E is assessing the data from the GCCS-J operational testing in FY23 and will report on operational effectiveness, suitability, and cyber survivability in FY24 following completion of additional operational testing.

» SURVIVABILITY

DISA has not conducted operational cyber survivability testing of v6.1.x and should conduct a CVPA and an AA to complete the testing necessary to support an evaluation of cyber survivability.

RECOMMENDATIONS

DISA should:

1. Develop test strategies to encompass the agile nature and varying operational site configurations to inform the update to the TEMP and the AOMTP, as discussed in the FY22 Annual Report.
2. Conduct a CVPA and an AA to complete testing necessary to support an evaluation of cyber survivability.

Joint Biological Tactical Detection System (JBTDS)

In July 2023, DOT&E published an operational assessment (OA) report on the Joint Biological Tactical Detection System (JBTDS) to support the Milestone C (MS C) decision in August 2023. The JBTDS demonstrated satisfactory progress toward operational effectiveness in detecting and identifying some biological warfare agents (BWAs) to support timely force protection decisions. Additional development is required to optimize detection and identification performance against other agents. The JBTDS demonstrated operational suitability challenges that prevent it from currently meeting operational requirements.

SYSTEM DESCRIPTION

The JBTDS consists of an integrated man-portable BWA aerosol detector and sample collector, a base station, a meteorological station, a GPS receiver, a sample extraction kit, and a handheld BWA identifier with consumable assays. The detector and sample collector can be connected to the base station using a Service-provided, closed, or restricted local area wired or wireless network to enable remote monitoring and reporting.

MISSION

U.S. Army, Marine Corps, and Navy units will deploy JBTDS during major combat, stability, and strategic deterrence operations where an adversary's employment of BWAs could severely disrupt military operations or cause

hazardous exposure to warfighters or civilians. Service units equipped with the JBTDS will conduct biological surveillance missions to detect the presence of, collect samples, identify, and warn forces of the BWA threat. The JBTDS is intended to support commanders' force protection actions, support medical planning, and provide information to enable consequence management. The Special Operations Command will employ the JBTDS identifier to identify BWA in samples to support intelligence gathering and forensics analyses.

PROGRAM

JBTDS is a joint Acquisition Category II program which was authorized in August 2023 to enter the production and deployment phase of acquisition. DOT&E approved the MS C Test and Evaluation Master Plan (TEMP) in September 2023. As reported in the FY22 Annual Report, system performance updates will be tested and will occur post-MS C in accordance with the updated TEMP. The multi-Service operational test and evaluation is scheduled for July 2025 and the full-rate production decision is targeted for May 2026.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

DOT&E based the July 2023 JBTDS OA report on live agent testing in the laboratory, observed developmental testing, a multi-Service OA, integrated developmental and operational testing, cyber survivability testing, and modeling and simulation conducted from December 2020 to September 2022. Testing was conducted in accordance with DOT&E-approved test plans and was found adequate to support the MS C decision. DOT&E made several recommendations in the FY22 Annual Report based on the series of tests conducted prior to the MS C decision. The program office is continuing to address these recommendations. Efficacy of their corrective actions will be assessed during testing planned post MS C.

In FY23, updates were made to the built-in-test algorithm, and improvement to the JBTDS leg stand design. The internal pump design was reconfigured to address flow issues. Post-MS C testing will identify the impact of these changes. The other FY22 recommendations remain valid as the program is developing their test strategy with low-rate initial production articles. Future tests in the production and deployment phase of testing will use low-rate initial production units to verify system improvements.

PERFORMANCE

» EFFECTIVENESS

The JBTDS demonstrated satisfactory progress toward achieving operational effectiveness. The system provides actionable information needed to mitigate casualties for most required BWAs. JBTDS did not meet detection and identification performance requirements for some agents and demonstrated significant variability between prototype units. When JBTDS provides actionable information, casualties can be reduced by masking quickly after detection and administering post-exposure prophylaxis after identification.

» SUITABILITY

JBTDS operational suitability is at risk due to poor reliability and a high false alarm rate in one environment. Warfighters rated JBTDS training and usability as acceptable. Unit-to-unit variability on prototypes is a concern.

» SURVIVABILITY

Testing identified JBTDS vulnerability to threats, to include cyber, and electromagnetic effects in certain operating environments. Additionally, warfighters sometimes responded to cyber threats as they would a system malfunction because they could not distinguish between the events. Details are included in the classified annex to the July 2023 JBTDS OA.

RECOMMENDATIONS

The Joint Product Manager should:

1. Mitigate identified vulnerabilities to electromagnetic effects.
2. Add cyber-specific topics to the training curriculum to better enable operators to recognize cyber threats and to protect, mitigate, and recover from hostile cyber actions.
3. Address recommendations found in the July 2023 JBTDS OA report and classified annex.
4. Improve the identifier assays to meet performance requirements.

Joint Cyber Warfighting Architecture (JCWA)

The Joint Cyber Warfighting Architecture (JCWA) concept continues to mature, and the Services continue aggressive efforts to field critical components of the architecture without adequate OT&E. U.S. Cyber Command's (USCYBERCOM) Joint Integration Office (JIO) continues to make significant strides towards accomplishing dedicated JCWA-level OT&E; however, the JCWA OT&E program remains in the initial planning and resourcing stages.

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

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.

The FY23 National Defense Authorization Act (NDAA) Section 1509 provides for the establishment of a JCWA Program Executive Office (PEO) within USCYBERCOM, as well as the FY22 NDAA that provides the commander of USCYBERCOM enhanced budget control starting in FY24. A JCWA PEO would be responsible for the creation and maintenance of a JCWA Governance charter, requirements, and program schedules.

USCYBERCOM currently relies on the Services for acquisition of the programs that comprise JCWA. Each program has its own release, testing, and deployment schedule, and there are no validated JCWA-level requirements nor a JCWA Governance Charter.

Three out of the four current JCWA programs leverage the software acquisition pathway, which requires annual value assessments. The assessments determine if capabilities delivered have been worth the investment. The OT&E community is coordinating closely with USCYBERCOM's Value Assessment Team to share data and findings.

» 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

Service-led programs under JCWA continue to develop and execute T&E strategies independent of the JCWA construct; however, the JIO recently identified the Joint Interoperability Test Command as the program's lead Operational Test Agency and provided initial funding to begin JCWA-level OT&E planning in FY23 for the first JCWA-level OT&E event in FY24.

In FY23, the Service-led programs under JCWA continued to conduct program-level contractor, developmental, and operational testing, including cyber assessments. DOT&E has informed and monitored testing conducted to date and will use the data in operational assessments where appropriate. DOT&E will issue an early fielding report in 2QFY24. As the JCWA concept continues to mature, the scope of OT&E required to support cyber warfighting efforts will need to continuously evolve so that it addresses the entire architecture and the dynamic, operational environment within which it operates. Adequate operational test and evaluation of JCWA will require USCYBERCOM to establish a cadence of test and invest in the development of test infrastructure to successfully support JCWA integration and ensure mission effectiveness and survivability as the enterprise evolves.

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. As recommended in the FY22 Annual Report, require OT&E to inform value assessments.
2. As recommended in the FY22 Annual Report, 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.
3. As recommended in the FY22 Annual Report, establish a cadence of test for dedicated OT&E, beginning in FY24, 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. Establish a JCWA Governance Charter to identify roles and responsibilities for USCYBERCOM's enhanced budget control and new acquisition authorities over Service-led JCWA subsystems.
5. Prioritize and accelerate efforts to finalize JCWA-level requirements.

Joint Operational Medicine Information Systems (JOMIS)

In FY23, the Joint Operational Medicine Information Systems (JOMIS) Program Management Office (PMO) successfully implemented all DOT&E recommendations from the September 2022 early fielding report on the Medical Common Operating Picture (MedCOP) application, and further applied lessons learned to all other JOMIS applications. In addition to these changes, the PMO engaged with DOT&E to implement persistent cyber operations (PCO) on multiple JOMIS products; PCO will begin after the successful execution of planned cyber survivability operational test events.

SYSTEM DESCRIPTION

The JOMIS PMO provides several capabilities, referred to as managed applications, to the warfighter. The managed applications are as follows.

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

MISSION

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

PROGRAM

All of the JOMIS managed applications except MHSG-T are using the software acquisition pathway. MHSG-T is jointly

Table 1. JOMIS Managed Applications

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

developed with the Defense Healthcare Management System Modernization (DHMSM) PMO and is an Acquisition Category ID program. DOT&E approved the Overarching JOMIS Test and Evaluation Strategy in September 2022, and issued an early fielding report on MedCOP in September 2022. The other four managed applications have not yet been operationally tested or fielded.

In implementing PCO, the JOMIS PMO joins the DHMSM PMO in piloting a program level integration of PCO, successfully used at combatant commands, to help ensure the cyber survivability posture of developed capabilities are rigorously assessed throughout the life cycle of the program, rather than limited to the acquisition and development phases.

» MAJOR CONTRACTORS

- Accenture Federal Services – Arlington, Virginia (MedCOP)
- ViiMed – Washington, DC (OpMed CDP)
- T6 Health Systems – Chesnut Hill, Massachusetts (OpMed CDP)
- Air Force Research Laboratory (OpMed CDP)
- Leidos – Reston, Virginia (MHSG-T)
- Oracle Health – Austin, Texas (MHSG-T)
- Dark Wolf Solutions – Herndon, Virginia (OMDS, TBLD-M)
- Omni Federal – Gainesville, Virginia (OMDS)

TEST ADEQUACY

The Joint Interoperability Test Command (JITC) conducted an operational assessment in accordance with a DOT&E-approved test plan of MedCOP at U.S. Central Command (USCENTCOM) in January 2023, which was observed by DOT&E. However, limitations on the number of users prevented JITC from assessing progress towards effectiveness and suitability. As a result, DOT&E did not write an independent assessment report.

JITC conducted the first phase of required cyber survivability operational test events in August 2023, in order to assess survivability of MedCOP.

JITC will conduct additional operational testing events, to include cyber survivability test events, during FY24, on all JOMIS applications, after which DOT&E will submit reports.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

JITC will conduct operational testing in FY24 on all the JOMIS managed applications, from which DOT&E will determine operational effectiveness, suitability, and survivability.

RECOMMENDATIONS

The JOMIS PMO and Program Executive Office Defense Healthcare Management Systems should:

1. Continue close collaboration with JITC and DOT&E throughout the development and testing of all JOMIS capabilities to conduct operational testing that evaluates whether each managed application is operationally effective, suitable, and survivable.
2. Engage with the DHMSM PMO to explore the feasibility of using MHSG-T as a backup capability for MHS GENESIS at all MHS GENESIS facilities, to ensure continuity of care in a denied, degraded, intermittent, or limited communications environment.
3. Ensure that the upcoming operational tests have sufficient users to support assessments of effectiveness and suitability.

Joint Planning and Execution System (JPES)

The Joint Planning and Execution System (JPES) program continues agile software development to replace the legacy Joint Operation Planning and Execution System (JOPES) program in FY24. In July 2023, the Joint Interoperability Test Command (JITC) conducted an early operational assessment (EOA) of JPES which provided users an opportunity to provide feedback on the effectiveness and usability of completed portions of the software development.

SYSTEM DESCRIPTION

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

The JPES Program Management Office (PMO) is continuing sustainment of the JOPES v4.5.x until JPES can be deployed to all JOPES users. Once JPES provides current JOPES capabilities, JOPES is expected to be retired in FY24.

MISSION

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

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

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

PROGRAM

JPES is an Acquisition Category III program. The JPES PMO intends to continue development and conduct user assessments to ensure all necessary functionality meets or exceeds that of JOPES, which JPES is replacing. The JPES PMO is implementing the development, security, and operations process as part of its agile software development framework.

» MAJOR CONTRACTORS

- InterImage Inc. – Arlington, Virginia
- ERP International, LLC – Laurel, Maryland
- NextGen Federal Systems – Morgantown, West Virginia
- CompQsoft – Leesburg, Virginia

TEST ADEQUACY

In FY23, JITC conducted an EOA of JPES on the SIPRNet, in accordance with DOT&E guidance. The JPES integrated test environment on the NIPRNet does not currently capture the mission configurations associated with each combatant command and other critical sites. The JPES PMO plans quarterly operational assessments with an IOT&E in 4QFY24 but has not yet submitted a Test and Evaluation Master Plan (TEMP) for DOT&E approval.

JPES test strategies need to be developed to encompass the agile nature and varying operational site requirements and inform the TEMP and the Agile Operational Master Test Plan (AOMTP). The JPES TEMP should detail operational cyber survivability tests that include a cooperative vulnerability and penetration assessment (CVPA) followed by an adversarial assessment (AA).

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

JITC assessed the operational users' feedback from the EOA. DOT&E will consider this data in the IOT&E report, expected to be released in FY25.

» SURVIVABILITY

No operational survivability testing of JPES has yet been conducted.

RECOMMENDATIONS

DISA should:

1. Improve the operational representativeness of the JPES integrated test environment to ensure testing more closely reflects the diversity of deployment configurations.
2. Submit a JPES TEMP and an AOMTP to DOT&E for approval.
3. Conduct a CVPA and an AA prior to the operational fielding of JPES.

Key Management Infrastructure (KMI)

The Key Management Infrastructure (KMI) Capability Increment 3 (CI-3) Program Management Office (PMO) began capability development in July 2021. The National Security Agency (NSA) awarded a major contract modification in late January 2023 that increases the KMI CI-3 scope to address additional technical requirements packages in ten Agile releases. The NSA Senior Acquisition Executive re-baselined the KMI CI-3 program in late September 2023, and the KMI CI-3 PMO intends to update the KMI CI-3 acquisition strategy and the Test and Evaluation Master Plan (TEMP) in early FY24 to support a full deployment decision (FDD) in FY27. A preliminary performance assessment will be available after completion of the KMI CI-3 multi-release testing in late FY24 or early FY25.

SYSTEM DESCRIPTION

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

MISSION

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

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

PROGRAM

The NSA intended to deliver KMI CI-3 in eight planned Agile releases to enhance existing capabilities and be transition capable for the legacy Electronic Key Management System (EKMS) Tier 0 and Tier 1 cryptographic product delivery into the infrastructure. The KMI CI-3 PMO began capability development in July 2021. The KMI CI-3 PMO announced a schedule delay in April 2022, due to hardware technical refresh, supply chain delivery delays, system configuration problems, and expanded requirements. The NSA awarded a major contract modification in late January 2023 that increased the KMI CI-3 scope to address additional technical requirements packages in ten total Agile releases. The NSA Senior Acquisition Executive re-baselined the KMI CI-3 program in late September 2023, and the KMI CI-3 PMO intends to update the KMI CI-3 acquisition strategy in early FY24 to support FDD in FY27.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

DOT&E approved the initial KMI CI-3 TEMP in August 2020 that defines an adequate operational test strategy for the KMI program release testing through IOT&E. The KMI CI-3 PMO incurred a major TEMP deviation in FY23 by not adhering to the approved test strategy, and the NSA had to provide a hardware technical refresh before delivering software releases. The KMI CI-3 PMO and the Joint Interoperability Command (JITC) are updating the KMI CI-3 TEMP to address test strategy, capability scope, and integrated schedule changes with submission to DOT&E expected in FY24. The JITC KMI test team will employ a multi-release test plan that can cover up to six of the initial Agile releases in an operational test plan. JITC is developing an operational test plan to support KMI CI-3 technical refresh release testing in the production environment that will commence in FY24. The KMI CI-3 PMO and JITC intend to operationally test the initial six KMI capability releases later in FY24 or early FY25.

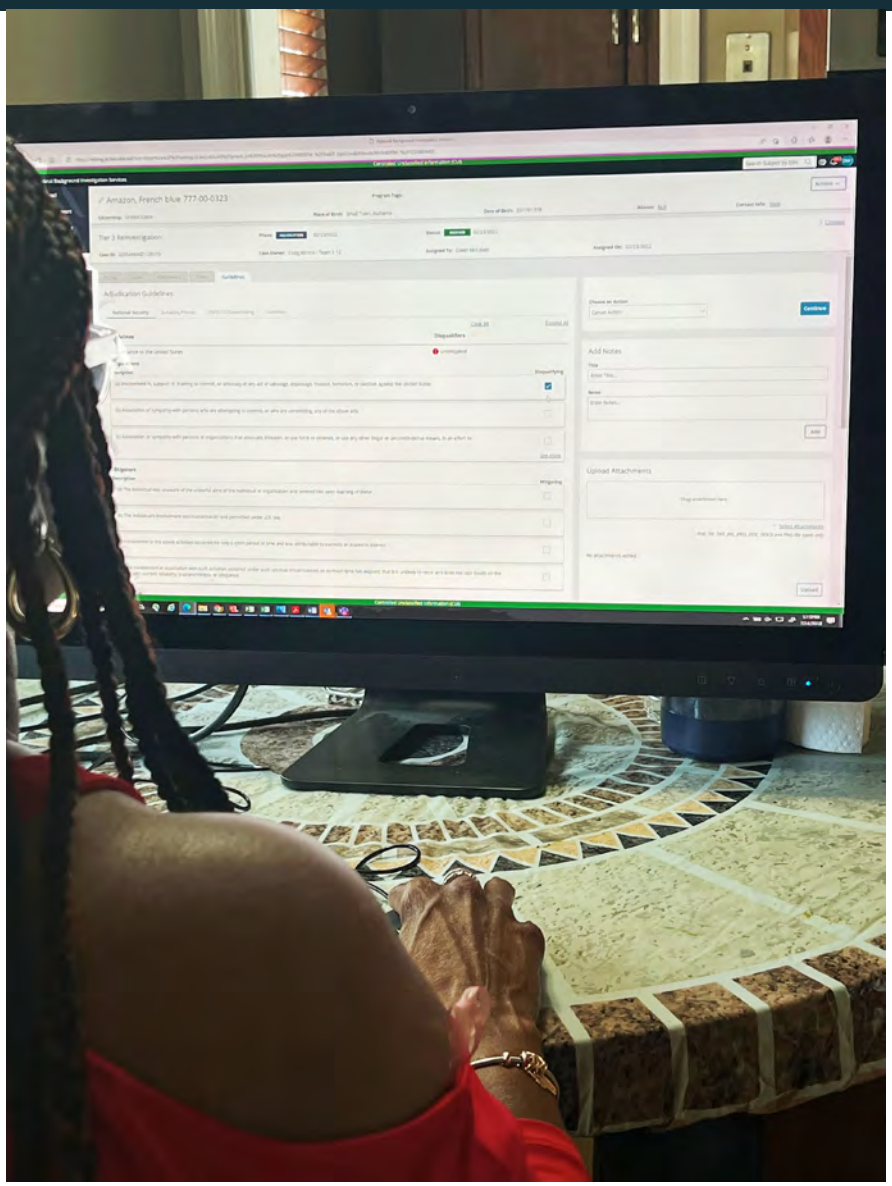
PERFORMANCE

A preliminary performance assessment will be available after completion of the KMI CI-3 multi-release testing for the initial Agile releases scheduled for late FY24 or early FY25. The current Key Management Enterprise (KME) schedule includes concurrent test planning, execution, and reporting between KMI CI-3, Symmetric Catalog Synchronization, Enterprise Service Bus, and EKMS efforts. This many parallel activities adds risk to the program. In addition, while the KMI Test Infrastructure provides a safe environment for evaluating KMI software builds, it is currently not in the same configuration as the operational KMI. This may limit the KMI Test Infrastructure users' ability to identify problems prior to deploying a new KMI release to the operational system. The KMI CI-3 PMO is in the process of a technical refresh for the KMI Test Infrastructure to mirror the production system.

RECOMMENDATIONS

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

National Background Investigation Services (NBIS)



The National Background Investigation Services (NBIS) program proficiently employs Agile software development techniques to field and build out capabilities in support of personnel security missions. Operational testing has not yet been conducted, but operational assessments are planned for FY24. Developmental testing continues.

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 several legacy systems.

MISSION

The Defense Counterintelligence and Security Agency (DCSA), other Federal agencies, and industry partners will use NBIS to authorize and support background investigations for new applicants as well as incumbent government, military, and contract personnel. NBIS has four operational mission areas: case initiation, adjudication, continuous vetting, and background investigation. It also has three cross-cutting support missions (up from one in FY22): service operations, metrics and reporting, and subject management. These missions allow agencies to initiate clearance requests, enable candidates to complete background investigation forms, gather public data concerning personnel applying, manage the findings of an investigation, adjudicating personnel clearances and provide continuous vetting of cleared personnel. The system of systems also simultaneously supports and measures system performance across these functions.

PROGRAM

NBIS transitioned to the software acquisition pathway in FY21 and is being developed using Scaled Agile Framework (SAFe) and Development Security Operations (DevSecOps) methodologies. The DCSA assumed operational control for NBIS from the Defense Information Systems Agency in October 2020, and is deploying NBIS in multiple releases of increasing capability while building upon and replacing legacy systems (such as the existing clearance application software and the visit management systems), which will be decommissioned through FY24. The program has employed SAFe methodologies to rapidly develop and field capabilities in collaboration with the testers and intended customer/user base. Early releases to a limited and restricted user base supported continuous developmental testing and a cumulative validation of system and data security. In March 2022, DOT&E placed NBIS on oversight due to program size, complexity, and importance to DoD operations. DOT&E has approved an NBIS Evaluation Strategy and an online test management process for NBIS.

» MAJOR CONTRACTORS

- Peraton, Inc. – Reston, Virginia (software development)
- Soliel, LLC – Vienna, Virginia (data migration)
- HII (formerly Huntington Ingalls Industries) – Newport News, Virginia (big data platform)
- Salient Systems – Austin, Texas (cyber support)
- Copper River Information Technology, LLC – Chantilly, Virginia (systems engineering)

TEST ADEQUACY

NBIS testing continues to focus on software validation and release, and developmental testing. Joint Interoperability Test Command has completed multiple rounds of cyber survivability tests and is planning operational assessments in FY24. DOT&E approved an NBIS Evaluation Strategy in December 2022, and approved an online test management process that makes extensive use of online planning software in lieu of written test documents for NBIS in July 2023 as a pilot effort with potential relevance to other Agile software developments. Two cybersecurity tests were conducted by the Joint Interoperability Test Command in March and June of 2023.

PERFORMANCE

» EFFECTIVENESS

The operational main mission areas of NBIS are developing at different rates: case initiation and adjudication capabilities are both relatively mature. Continuous vetting capabilities continue to mature, and background investigations capabilities are in early development. The cross-cutting mission areas are also in varying stages of maturity at this time.

» SUITABILITY

Suitability testing is ongoing, and assessments of training, helpdesk support, and issue tracking and resolution are not yet completed. DOT&E expects to complete a full assessment in FY24.

» SURVIVABILITY

Several rounds of cybersecurity testing have been conducted on NBIS and relevant connected legacy systems. One cyber test uncovered a vulnerability affecting not only NBIS but many other DoD programs which access cloud-based resources. To address this vulnerability, the Defense Information Systems Agency developed, successfully tested, and implemented a mitigation, which has been validated for NBIS. The system is currently considered survivable against a moderate threat.

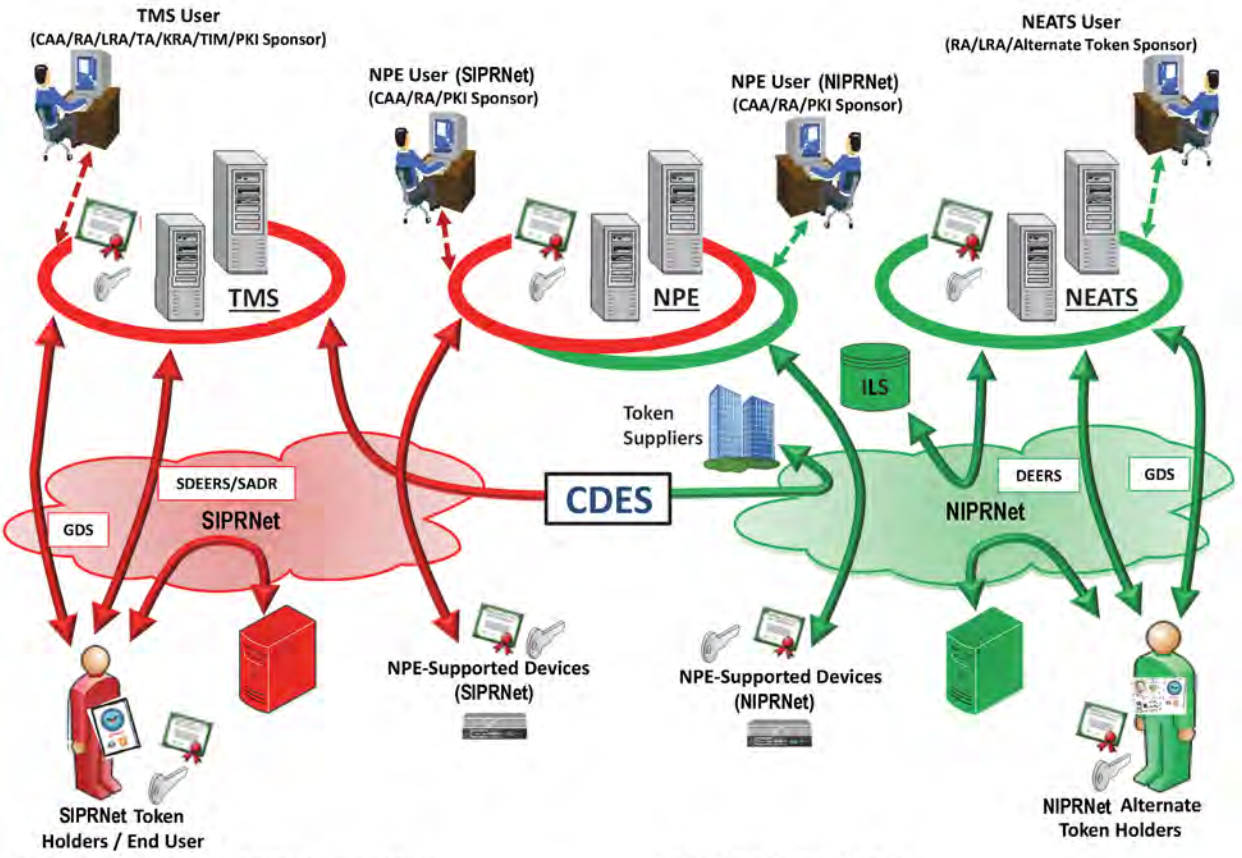
RECOMMENDATION

DCSA and the NBIS Program Office should:

1. Continue the progress demonstrated to date, including development of their online test management process.

Public Key Infrastructure (PKI) Increment 2

The DoD Public Key Infrastructure (PKI) Increment 2 (consisting of Token Management System (TMS), NIPRNet Enterprise Alternate Token System (NEATS), and the Non-Person Entity (NPE)) is operationally effective, demonstrating the capability to facilitate secure electronic information exchanges between DoD users and network devices. The PKI TMS is not operationally suitable due to problems with SIPRNet token ordering processes and accountability. The PKI Program Management Office (PMO) upgraded the TMS baseline and changed processes to enhance token order tracking for the Services and Agencies. The Joint Interoperability Test Command (JITC) reassessed TMS operational suitability and token ordering processes in FY23 and expects to complete the effort in FY24. TMS is survivable, while NEATS and NPE are not survivable against moderate cyber threats. Given the criticality of PKI to DoD's cyber posture, the National Security Agency (NSA), Defense Information Systems Agency (DISA) and Defense Manpower Data Center (DMDC) should remediate the cyber vulnerabilities to PKI as soon as possible and conduct operational testing to ensure PKI is survivable.



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

SYSTEM DESCRIPTION

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

MISSION

DoD users at all levels use DoD PKI to provide authenticated identity management via personal identification number-protected Common Access Cards, SIPRNet tokens, 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 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 DMDC, and NPE with operational support from the DISA. TMS, NPE, and NEATS use commercial and government off-the-shelf hardware and software hosted at DISA and DMDC operational sites. DOT&E 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, a classified NPE finding memo in February 2022, and a classified PKI Increment 2 Cyber Survivability Interim Annex in January 2023.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

JITC conducted the PKI Increment 2 FOT&E from late November 2020 through March 2021, in accordance with a DOT&E-approved test plan. Testing was adequate to verify system fixes and assess operational effectiveness and suitability of PKI Increment 2 capabilities for long-term sustainment and transition. JITC completed FOT&E re-testing and verifications of fixes for operational suitability issues in FY22 and FY23, which were observed by DOT&E. JITC conducted NPE and TMS cyber testing in FY21 and re-tested NPE cyber in late FY21 and FY22. The PKI PMO implemented partial NPE cyber mitigations in FY22 and intends to implement additional mitigations in FY24. JITC intends to continue cyber survivability testing and verifications of NEATS in FY24 in support of a DoD PKI Increment 2 full deployment decision in September 2024.

PERFORMANCE

» EFFECTIVENESS

NEATS, NPE, and TMS are operationally effective, with minor problems that the PKI PMO is working to remedy. JITC completed verification of fixes for some PKI capabilities in FY23. The NPE auto-rekey functionality on devices using the Enrollment over Secure Transport (EST) protocol remains not operationally effective and as a result, has not been widely adopted as an enterprise capability. The PKI PMO has no technical means to fix the EST protocol implementation for devices, and JITC has no plans to re-test the EST protocol.

» SUITABILITY

NEATS and NPE are operationally suitable. TMS is not operationally suitable because the Central Management of Tokens (CMT) system and processes resulted in a lack of token accountability. The PKI PMO updated the TMS baseline with improvements in CMT order tracking to support Service and Agency needs in FY23. JITC conducted follow-on TMS assessments in FY22 and FY23 to evaluate system changes and token ordering process improvements. JITC is reassessing TMS operational suitability and token ordering processes, with expected completion in FY24. TMS capabilities are still not ready for long-term sustainment and transition at the conclusion of FY23, a recurring issue.

» SURVIVABILITY

TMS is survivable, while NPE and NEATS are not survivable against moderate capability nearsider and advanced capability outsider threats. The PKI PMO partially mitigated the NPE problems in FY22; however, the PKI PMO has no plans to mitigate all the remaining problems in FY24 or conduct further NPE operational cyber testing and evaluation. DOT&E published a classified PKI Increment 2 Cyber Survivability Interim Annex in January 2023 that addressed NPE findings. The PKI PMO and DMDC are working to mitigate NEATS findings and other architectural problems found in previous cyber survivability testing, after which JITC will test NEATS in FY24. The PKI PMO, NSA Acquisition Security Office, and DMDC token supply chain risk management processes lack transparency and need improved monitoring of token manufacturer processes.

RECOMMENDATIONS

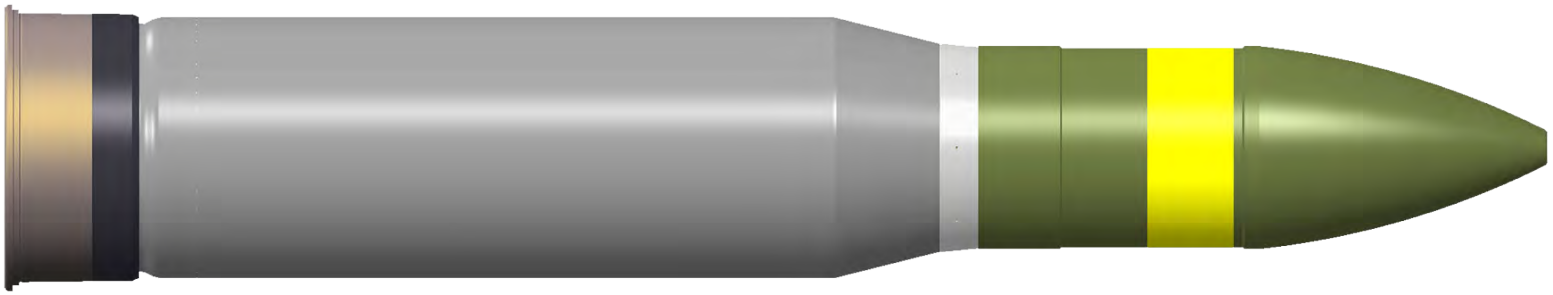
The PKI PMO and other organizations have yet to resolve the following recommendations from the FY22 Annual Report:

1. The PKI PMO and DISA should remediate the identified NPE vulnerabilities found during cyber survivability assessments and operationally test the system.
2. The PKI PMO and DMDC should remediate the identified NEATS vulnerabilities found during cyber survivability assessments to secure this system and the supporting environment, and then operationally test the system.
3. The PKI PMO and JITC should conduct operational cyber survivability assessments of NPE and NEATS prior to full deployment.
4. The PKI PMO and DMDC should establish a reproducible and accurate token ordering and accountability process for PKI tokens.
5. 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.
6. The PKI PMO, DMDC, and DISA should correct long-term sustainment problems prior to full deployment.

DEPARTMENT OF THE ARMY PROGRAMS

This page intentionally left blank.

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



In 3QFY23, the Army completed an investigation that included component-level testing that identified the root cause of failure from First Article Acceptance Testing conducted in September 2021. The Army is planning to conduct a tactical ballistic validation test in 1QFY24 to verify final design configuration changes. DOT&E published a classified M1147 120mm Advanced Multi-Purpose (AMP) combined IOT&E and LFT&E report in December 2022 assessing the cartridge's operational effectiveness, lethality, suitability, and survivability.

SYSTEM DESCRIPTION

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

MISSION

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

PROGRAM

The 120mm AMP cartridge is an Acquisition Category III program which 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. After the publication of the DOT&E combined IOT&E and LFT&E report, the full-rate production decision planned for FY23 was delayed due to an investigation to identify the root cause of failure from the First Article Acceptance Test conducted in September 2021. Army efforts are underway to re-baseline the program schedule to account for delays. Tactical ballistic validation testing is planned for 1QFY24 followed by First Article Acceptance Testing. The full-rate

production decision is planned for 4QFY24.

» MAJOR CONTRACTOR

- Northrop Grumman Defense Systems – Plymouth, Minnesota

TEST ADEQUACY

The Army completed IOT&E in September 2021, and LFT&E in April 2022. Testing was completed in accordance with DOT&E-approved test plans and DOT&E observed the IOT&E. DOT&E did not observe the lethality demonstration shots fired in April 2022, but had access to all data and video from the shots. DOT&E published a classified combined IOT&E and LFT&E report in December 2022.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

DOT&E published a classified combined IOT&E and LFT&E report in December 2022 providing assessments of M1147 120mm AMP cartridge's operational effectiveness, lethality, suitability, and survivability.

RECOMMENDATION

The Army should:

1. Continue to address recommendations found in the classified combined IOT&E and LFT&E report published in December 2022.

Abrams M1A2 System Enhancement Packages (SEPs) and Active Protection System (APS)

The Army announced in September 2023 that it will end the M1A2 SEPv4 program and instead develop the Abrams M1E3 Main Battle Tank (MBT) modernization program. The Abrams M1A2 System Enhancement Package version 4 (SEPv4) was intended to be an incremental upgrade to the Abrams M1A2 SEPv3 to improve lethality and survivability. The Army tested the TROPHY Active Protection System (APS) installed on Abrams M1A2 SEPv3 tanks in FY22 to inform an urgent materiel release (UMR) in May 2023. The TROPHY APS intercepted most of the incoming threats, and the Abrams tank base armor provided adequate force protection.

SYSTEM DESCRIPTION

The Abrams M1A2 MBT is a tracked, land combat, assault weapon system equipped with a 120-mm main gun offering shoot-on-the-move firepower and joint interoperability. When compared with SEPv3, units equipped with the Abrams SEPv4 are intended to have increased survivability, lethality, and maneuverability with the ability to respond to hostile entities on the battlefield by engaging or avoiding them before they become a threat.

The Army was continuously upgrading the Abrams M1A2 MBT through engineering change proposals, each significant upgrade is reflected in the version of the system enhancement package. SEPv2 upgrades the M1A2 by providing improved communication capabilities, target detection, recognition, and identification. SEPv3 provides increased crew survivability. SEPv4 was intended to provide improved lethality. The Abrams M1E3 MBT is intended to make the capability improvements needed to fight against future threats on the battlefield of 2040 and beyond.

TROPHY APS is an add-on kit to Abrams M1A2 SEPv2 and SEPv3 tanks, designed to detect, identify, track, and degrade enemy rocket and missile threats. The TROPHY APS adds approximately 5,000 pounds to the tank.

MISSION

Commanders employ units equipped with the Abrams M1A2 MBT to maneuver across the full range of military operations and destroy the enemy by fire. MBTs equipped with APS offer additional defense against enemy rocket and missile threats.

PROGRAM

The Abrams M1A2 is an Acquisition Category IC program. The Army was incrementally upgrading the tank design through engineering change proposals. The Army announced in September 2023 that it will end the M1A2 SEPv4 program and instead develop the Abrams M1E3 MBT modernization program.

The Army has pre-positioned TROPHY APS kits for installation on Abrams SEPv2 and SEPv3 tanks, fulfilling two directed requirements signed in October 2016 and March 2018 by the Army's Deputy Chief of Staff, G8. DOT&E published a classified early fielding report in March 2023 to inform the urgent materiel release decision in May 2023.

» MAJOR CONTRACTORS

- General Dynamics Land Systems – Sterling Heights, Michigan
- Leonardo DRS, Inc. and Rafael Advanced Defense Systems Ltd. partnership – St. Louis, Missouri

TEST ADEQUACY

DOT&E approved the Abrams SEPv4 Test and Evaluation Master Plan in March 2023. With the announcement to terminate the SEPv4 effort and proceed with the M1E3, the working level integrated product team will reconvene to update the test and evaluation strategy. The Army completed integrated testing of the 3rd generation forward looking infrared system as integrated on the tank in October 2022 to assess the system's capability to detect, recognize and identify targets. The Army initiated automotive and safety developmental testing in 3QFY23.

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 the performance envelope and capability demonstrated with Abrams SEPv3 tanks equipped with APS. Testing included live fire flight tests with inert and live threats fired against a fully functional Abrams SEPv3 tank.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

TROPHY APS effectively detects, identifies, tracks, and intercepts incoming threats with exceptions for certain range conditions and engagement profiles. The Abrams SEPv2 and SEPv3 base armor configurations provide adequate force protection against the threat and countermeasure debris generated by a successful intercept. The system, as installed on SEPv3, demonstrated similar capabilities and deficiencies as the system installed on SEPv2.

Additional details can be found in DOT&E's two classified reports on TROPHY APS. The first report, published in June 2020, assessed the performance of Abrams M1A2 SEPv2 equipped with TROPHY APS. The second report, published in March 2023, assessed the

performance of Abrams M1A2 SEPv3 equipped with TROPHY APS.

RECOMMENDATION

The Army should:

1. Address recommendations in the DOT&E classified reports for Abrams SEPv2 and SEPv3 equipped with TROPHY APS published in June 2020 and March 2023, respectively.

Abrams Live Fire Qualifications at Udairi Multi Purpose Range Complex, Kuwait, August 2023

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. DOT&E submitted a combined IOT&E and LFT&E report with a classified survivability annex to Congress in January 2023 assessing the Armored Multi-Purpose Vehicle (AMPV) Family of Vehicles (FoV) as operationally effective, suitable, and survivable against specified kinetic threats. DOT&E provided the Army with the combined IOT&E and LFT&E report and assessments to support a full-rate production decision by the Army Acquisition Executive in July 2023. The Army is considering modifying existing AMPV variants to support select modernization initiatives which include the Terrestrial Layer System, and the Modular Turreted Mortar System.

SYSTEM DESCRIPTION

The AMPV is a tracked, ground combat vehicle that supports casualty evacuation and treatment, command post operations, logistical resupply, and heavy mortar fire support to an Armored Brigade Combat Team (ABCT). There are five variants: General Purpose (GP), Mission Command (MCmd), Medical Treatment (MT), Medical Evacuation (ME), and Mortar Carrier (MC). The AMPV replaces the M113A3 Family of Vehicles (FoV), consisting of the M113A3 (GP and ME), M1064A3 (MC), M1068 (MCmd) and M577 (MT) variants, and addresses shortcomings in survivability 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 than the legacy M113A3 FoV to accomplish required operational support missions across the range of military operations. ABCT units will use AMPVs to support casualty evacuation and treatment, command post operations, logistical resupply, and heavy mortar fire support.

PROGRAM

The AMPV is an Acquisition Category IC program utilizing the major capability acquisition pathway. The Army conducted a Limited User Test in September 2018 to support a low-rate production decision in January 2019. The Army conducted the IOT&E in July 2022. FUSL testing was completed in May 2022. The full-rate production decision was made in July 2023.

» MAJOR CONTRACTOR

- BAE Systems – York, Pennsylvania

TEST ADEQUACY

The Army conducted an IOT&E in July 2022 using units from an ABCT to conduct tactical missions in a synthetic environment against a near-peer opposing force operating in an electronic warfare and cyber-contested environment. FUSL testing was conducted from May 2021 through 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 adequate, conducted in accordance with DOT&E-approved test plans, and was observed by DOT&E. DOT&E published a combined IOT&E and LFT&E report with a classified survivability annex in January 2023.

PERFORMANCE

» EFFECTIVENESS

The AMPV FoV is effective in supporting a unit to accomplish its doctrinal missions and contributed to the accomplishment of the unit's assigned task and purpose. The AMPV FoV provides increased mobility and better supports the operating tempo of an ABCT than the M113A3 FoV. Each variant maintained a tactical speed consistent with the maneuver force, and when needed, was able to accelerate to and maintain an operational speed equivalent to other vehicles in the ABCT.

Crews employed the MCmd variant to support brigade and battalion-level command post operations using digital systems. The fixed interior layout of the MCmd does not support the conduct of analog command post functions; hinders digital fire direction center operations and does not support analog fire direction center operations. Since completion of the IOT&E, the program office has made modifications to the interior of the MCmd variant in order to better support the conduct of analog operations.

Crews equipped with the MC variant provided timely fires in support of maneuvering units and conducted fire missions faster than M1064A3 MC crews. Crews reported less shock and a more stable platform while firing rounds from the MC than compared to the M1064A3 MC. Crews stated that the heavier and more stable MC platform better handled the firing impulse when firing maximum charge missions while transmitting less shock to vehicle crew. Soldiers expressed this was a significant improvement over the M1064A3.

The ME variant's litter lift system facilitates the loading, unloading and transporting of litter patients better than the M113A3 and provides increased protection of ambulatory patients. The increased mobility over the M113A3 ambulance allows medics to evacuate casualties from the battlefield faster. The ME is less likely than the M113A3 to cause additional injuries during transport because the ME's suspension provides a smoother and more stable ride than the M113A3. The ME has better storage capacity for equipment and supplies than the M113A3 and provides additional medical capability and mounting

locations for medical equipment such as suction and oxygen. Several medics commented that the placement and orientation of the medic's seat made it difficult to monitor patients when using a seatbelt during transport, and that there were no handholds to steady themselves when treating or monitoring casualties on-the-move. Since the completion of IOT&E, the program office has initiated development of a hand hold special kit which will be implemented on future medical variants.

The MT variant's treatment table enables crews to provide medical treatment under armor protection. When treating causalities, the vehicle's low interior height causes the medical staff to work hunched over or on their knees. The process of moving and adjusting the height and tilt of the table, and the time required to make these adjustments, makes it difficult to quickly configure and position the table to treat a casualty. The table blocks accessibility to the medical supplies stored on the right side of the vehicle. The table slides from the stowed position to the center of the vehicle along grooved tracks in the deck. These grooves fill with debris that makes moving the table and locking it into the stowed position difficult.

The GP variant has a larger cargo carrying capacity than the M113A3 and is equipped with litter brackets to support units conducting logistics resupply and casualty evacuation missions. The larger interior of the GP increases the quantity of supplies that can be transported during resupply operations. This increased capability aids in improving unit sustainment, while reducing the number of resupply missions.

» SUITABILITY

The AMPV FoV is operationally suitable. The AMPV FoV met its availability and mean miles between essential function failures requirements as point estimates. Although the vehicles did not meet the requirement for mean miles between system aborts during the IOT&E, the degradation to the probability of mission completion was less than 5 percent and had no operational impact to the unit's ability to conduct missions. Drivetrain and vehicle electronic failures lowered system reliability. Since completion of the IOT&E, the program office has implemented corrective actions to address the hardware and software corrective actions to address essential function failure and system abort failure modes. These fixes are planned to be verified in follow-on production testing conducted by the program office in 2024.

» SURVIVABILITY

The AMPV FoV, when equipped with reactive armor tiles, is survivable against threshold-level kinetic threats. The test team observed inadvertent discharges of the automatic fire extinguishing system (AFES) during live fire testing. The Army is examining design solutions to improve the mounting provisions of the AFES components and plans to verify the fixes through testing. AMPV FoV vulnerabilities in a cyber- and electromagnetic-contested environment are detailed in the classified survivability annex to the combined IOT&E and LFT&E report published in January 2023. The Army is implementing the survivability recommendations identified in the classified annex.

RECOMMENDATIONS

The Army should:

1. Continue initiatives to make the interior of the MCmd modular and reconfigurable to better support crews conducting analog operations.
2. Continue to develop a fire direction center-specific variant to better facilitate crews' ability to conduct fire direction center operations.
3. Continue corrective actions to address essential function failure and system abort failure modes to improve reliability.
4. Continue to address the survivability recommendations provided in the classified annex to the combined IOT&E and LFT&E report.

Army Integrated Air and Missile Defense (AIAMD)

The Army Test and Evaluation Command (ATEC) completed IOT&E of the Army Integrated Air and Missile Defense (AIAMD) program in October 2022. DOT&E published an evaluation of the system's operational effectiveness, suitability, and survivability in a classified report to inform AIAMD's full-rate production (FRP) decision in April 2023. DOT&E also approved an updated T&E strategy in February 2023 that includes FOT&E scheduled to begin in 4QFY24.

SYSTEM DESCRIPTION

The AIAMD program provides an Integrated Air and Missile Defense (IAMD) Battle Command System (IBCS) to integrate Engagement Operations Centers (EOCs), Sentinel air-surveillance radars, Patriot radars, and Patriot launchers across an Integrated Fire Control Network (IFCN). EOCs provide the operating environment for soldiers to monitor and direct sensor employment and the engagement of air threats. Hardware interface kits connect adapted Patriot and Sentinel components to the IFCN, either through an EOC or through an IFCN Relay. IFCN Relays also provide distributed operations and mobile communications nodes to extend IFCN connectivity. Future hardware and software updates will integrate additional sensors and weapons, such as the Lower-Tier Air and Missile Defense Sensor and the Indirect Fire Protection Capability, with IBCS.

MISSION

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

PROGRAM

AIAMD is an Acquisition Category ID program, developing hardware using the major capability acquisition pathway and conducting agile software development using the software acquisition pathway. In April 2023, the program received approval to enter FRP and approval for conditional materiel release for a CONUS test battalion. The Army intends to integrate new and existing sensors and weapons through a series of future increments.

DOT&E approved the program's T&E Strategy, located in the AIAMD Simplified Acquisition Management Plan, in February 2023. The T&E Strategy covers testing of future IBCS capability updates, including FOT&E scheduled to begin in 4QFY24. In addition to evaluation of capability updates, the FOT&E will evaluate the correction of deficiencies discovered before and during IOT&E. The Army plans to submit T&E annexes annually for DOT&E approval.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

ATEC conducted a multi-phased IOT&E that started in August 2021 and finished in October 2022. Testing was conducted in accordance with the DOT&E-approved Test and Evaluation Master Plan and associated test plans, and was observed by DOT&E. The IOT&E was adequate to support an evaluation of operational effectiveness, suitability, and survivability to inform the AIAMD FRP Decision.

ATEC conducted the IOT&E at White Sands Missile Range, New Mexico, which included software/hardware-in-the-loop operations with accredited modeling and simulation (M&S) tools; sustained live air operations; and three missile flight tests. ATEC also conducted a cyber adversarial assessment in both software/hardware-in-the-loop M&S and live air environments.

As additional systems are integrated with IBCS, the M&S tools for those sensors and weapons must also be integrated with the AIAMD M&S tools to support credible assessments of operational effectiveness in realistic threat environments.

PERFORMANCE

» EFFECTIVENESS

DOT&E's assessment of system operational effectiveness focused on whether the system provided the capabilities and information necessary for soldiers

to successfully conduct the air defense mission, including detection, identification, monitoring, and (if required) engagement of air threats. Details can be found in DOT&E's classified March 2023 IOT&E report.

» SUITABILITY

DOT&E's assessment of system operational suitability used hardware and software failure rate and repair time data collected during IOT&E to determine system availability and mission reliability. The assessment also covers soldiers' ability to operate the system, from both human-system interaction and training adequacy perspectives. Details can be found in DOT&E's classified IOT&E report.

» SURVIVABILITY

DOT&E's assessment of system survivability used cyber data collected during an August 2021 cooperative vulnerability and penetration assessment and an October 2021 adversarial assessment. Details can be found in DOT&E's classified IOT&E report.

RECOMMENDATIONS

The Army should:

1. Complete and demonstrate the deficiency corrections recommended in DOT&E's classified report.
2. As reported last year, continue developing an integrated suite of M&S tools to support follow-on testing of IBCS with existing and future launchers, sensors, and other systems to provide operationally representative assessments of the combat effectiveness of these increasingly complex IAMD systems.

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

In March 2023, DOT&E published a classified operational assessment (OA) report for the Dismounted Assured, Positioning, Navigation, and Timing System (DAPS) GEN II, based on a Limited User Test conducted by the Army Test and Evaluation Command (ATEC) at Fort Huachuca, Arizona in November 2022 in support of successful transition from rapid prototyping to major capability acquisition program at Milestone C (MS C). The DAPS GEN II performs better than the current Defense Advanced GPS Receiver (DAGR) in the presence of GPS interference or enemy electronic warfare (EW) attacks. The DAPS GEN II IOT&E is planned to be conducted in 1QFY24 and will support a full-rate production decision in 3QFY24.

SYSTEM DESCRIPTION

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

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

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 EW attacks.

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

DAPS GEN 1.0 and DAPS GEN 1.2 are quick reaction capabilities developed in response to an Army-directed requirement culminating in an OA in 4QFY21 and a limited equipping of four infantry brigade combat teams (IBCT) beginning in FY22. As of 4QFY23, one IBCT has been equipped with 611 DAPS GEN 1.0 units and two IBCTs have been equipped with 1,390 DAPS GEN 1.2 units. All DAPS GEN 1.0 deliveries are complete and one additional IBCT will be equipped with 629 DAPS GEN 1.2 in 1QFY24.

In early FY22, the Army selected TRX Systems Inc. as the vendor for the DAPS GEN II rapid prototyping program. In March 2023, DAPS GEN II transitioned from rapid prototyping to a major capability acquisition program at MS C with a DOT&E-approved MS C Test and Evaluation Master Plan. The Army plans to conduct the DAPS GEN II IOT&E in 1QFY24 to support a full-rate production decision in 3QFY24.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

In November 2022, ATEC conducted a LUT with a cyber survivability adversarial assessment (AA) at Ft. Huachuca, Arizona in accordance with a DOT&E-approved test plan and TEMP. The LUT and AA were observed by DOT&E. The LUT was adequate to determine that DAPS GEN II is on track to achieving operational effectiveness and suitability by IOT&E. DOT&E published a classified OA report in March 2023, supporting the Army's decision to proceed to Low-Rate Initial Production at MS C.

The Army addressed FY22 Annual Report recommendations to verify the correction of performance deficiencies prior to conducting the LUT.

PERFORMANCE

» EFFECTIVENESS

During the LUT, dismounted infantry units equipped with DAPS GEN II demonstrated the potential to be operationally effective while

conducting tactical missions. The DAPS GEN II performs better than the current DAGR in GPS contested environments and improves the Soldiers situational awareness, supports navigation, and allows the unit to maintain operational tempo while moving between objectives. During the LUT, the DAPS was not consistently accurate at notifying soldiers to the presence of GPS interference and EW attacks. Further development and testing are necessary to improve the accuracy of DAPS GEN II EW notification capability. Additional details are contained in the March 2023 classified OA report.

» SUITABILITY

The DAPS GEN II did not meet its reliability growth curve estimate during the LUT, though demonstrated the potential to be operationally suitable due to the rapid repairability of the failures and a high availability rate. The primary failure mode was a software fault which resulted in re-occurring connectivity issues. The DAPS Program Office is implementing and testing a fix for these issues. Training was sufficient for Soldiers to operate the DAPS GEN II, though they would prefer more options to train in live or simulated GPS contested environments. The Army should include the use of the existing built-in EW simulation mode during new equipment training. Additional details are contained in the March 2023 classified OA report.

» SURVIVABILITY

DAPS GEN II demonstrated the potential to be survivable with just one classified finding during the AA conducted in November 2022. A follow-on DAPS GEN II cooperative vulnerability and penetration assessment was conducted in September 2023 and results will inform an AA to be conducted during the IOT&E.

RECOMMENDATIONS

The Army should:

1. Improve DAPS consistency when notifying soldiers to the presence of GPS interference and EW attacks to improve soldier and unit situational awareness.
2. Verify through testing that the software fault has been corrected prior to IOT&E.
3. Include the use of DAPS built-in EW simulation mode during new equipment training.

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

The Army intended to operationally test Distributed Common Ground System – Army (DCGS-A) Capability Drop 2 (CD2) in October 2022, but DOT&E did not approve the operational test plan because of inadequacies in the Army's data collection, reduction, and analysis capabilities. The Army subsequently conducted the test as a customer test, which was not adequate to evaluate quantitative performance. The Army has made DCGS-A CD2 available to Army users but has not yet formally fielded it. To support evaluation of DCGS-A CD2 operational effectiveness, suitability, and survivability, the Army should improve its data collection, reduction, and analysis capabilities, and plan for operational testing of DCGS-A CD2 as soon as possible.

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. CD2 is designed to provide a cloud-based Army intelligence data architecture that will bring in intelligence data from hundreds of Services and Intelligence Community data sources. 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.

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-level 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 data.

PROGRAM

Project Manager, Intelligence Systems and Analytics (PM IS&A) is managing DCGS-A as an inactive Major Defense Acquisition Program and intends to transition capabilities currently covered by DCGS-A to other future Army programs. The Army does not plan for further capability drops for DCGS-A.

In FY19 through FY20, PM IS&A 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, PM IS&A 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) but did not complete an operational test of the CD2 on the AC2SP in FY22 or FY23.

The Army did not submit the Army-approved Test and Evaluation Master Plan (TEMP) to DOT&E for approval despite that DOT&E advised the Army that the TEMP needs to add more details about the operational test and evaluation plan.

DOT&E did not approve the DCGS-A CD2 Operational Utility Assessment Plan, because it did not describe an adequate plan for data collection, reduction, and analysis. 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 the CD2's battlefield picture because the test did not describe the process and methodology to evaluate the system's ability to import the data from each required data source accurately. The test plan also lacked methods to evaluate whether the CD2's analytical products accurately reflect the imported data.

DOT&E approved the cyber survivability cooperative vulnerability and penetration assessment (CVPA) and adversarial assessment (AA) plan for the CD2 AC2SP cloud node in August 2022.

» MAJOR CONTRACTOR

- Palantir Technologies, Inc. – Denver, Colorado

TEST ADEQUACY

The Army has not conducted an operational test of DCGS-A CD2, other than cyber survivability testing for the cloud node. U.S. Army Test and Evaluation Command conducted the CVPA and AA in September 2022. The Deployed Edge Node (DEN) was not ready for cyber testing. The CVPA and AA of the cloud node were conducted in accordance with the DOT&E-approved test plan and DOT&E observed the tests.

Army Test and Evaluation Command conducted the planned Operational Utility Assessment as a customer test in October 2022 with users at multiple sites. The DEN and cross-domain solution (CDS) were not part of this test. DOT&E observed this event. The

event revealed a lack of tools and methodologies needed to quantitatively evaluate an advanced analytic system such as CD2. The CD2 customer test did not produce data to analyze quantitative characterization, including how much of the data from each required data source was brought into CD2 accurately. Since 2014, DOT&E has recommended that the Army acquire automated data collection, reduction, and analysis capabilities for data-centric systems such as DCGS-A, but the Army still does not have such capabilities.

PERFORMANCE

» EFFECTIVENESS

The customer test conducted in October 2022 was not adequate to evaluate DCGS-A CD2 operational effectiveness quantitatively but showed indications that its advanced analytic tools may work effectively if the intelligence database is adequate. However, the customer test showed limited ability to ingest data from the required sources, and CD2 users will not be able to perform intelligence missions without an adequate ability to bring in the necessary data from those sources.

» SUITABILITY

The customer test conducted in October 2022 was not adequate to evaluate operational suitability, but the results indicated a need to improve the enterprise management to support adequate import of intelligence data from the required sources.

» SURVIVABILITY

The CVPA and AA discovered cyber vulnerabilities. The Army has stated it has implemented mitigations for those vulnerabilities but has not conducted verification of the fixes. This was previously reported in the FY22 Annual Report. Cyber survivability against attacks via CDS has not been tested.

RECOMMENDATIONS

The Army should:

1. Sustain efforts to acquire automated data collection, reduction and analysis capabilities and implement a methodology to collect and analyze quantitative performance of advanced, data-centric capabilities as soon as possible to enable adequate operational testing of these systems, including those that utilize machine learning and artificial intelligence algorithm intelligence capabilities.
2. Update and submit a TEMP for DOT&E approval.
3. When the CDS is ready, conduct cyber survivability testing to evaluate the user's ability to defend against attack vectors through the CDS.

Family of Medium Tactical Vehicles A2 (FMTV A2)

In October 2023, DOT&E issued a combined FOT&E and LFT&E report. The report states that units equipped with the Family of Medium Tactical Vehicles A2 (FMTV A2) Light Medium Tactical Vehicle (LMTV) cargo truck, the Medium Tactical Vehicle (MTV) cargo truck, the MTV Load Handling System (LHS) truck, the MTV wrecker, and the MTV dump truck are operationally effective, suitable, and survivable. The improved mobility of the FMTV A2 on secondary and unimproved roads and cross-country terrain, as well as its ability to carry heavier cargo loads, facilitates the Army's operational concept for more dispersed operations on the battlefield, which requires more frequent unit relocations and greater resupply distances.

SYSTEM DESCRIPTION

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

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

- LMTV chassis – a 3-ton cargo truck, a 2.5-ton van, and a low-velocity air drop (LVAD) cargo truck.
- MTV chassis – an 8-ton cargo truck, an 8-ton cargo truck with an extended cargo bed, a tractor, an 8-ton LVAD cargo truck, an expansible van, a 5-ton LVAD dump truck, a wrecker, an 8.8-ton load handling system (LHS) truck, and a 10-ton dump truck.

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

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

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

- Increased cargo-carrying capacity. Earlier models of the LMTV and MTV trucks carried a maximum cargo load of 2.5 and 5 tons, respectively.
- Improved mobility from increased engine horsepower, an adjustable suspension system, and higher wheel capacity.
- Upgraded vehicle data bus with a simplified electrical system that supports improved diagnostic and troubleshooting capabilities and future upgrades.
- Increased electrical power capacity to support current operations and provide growth potential for future upgrades.
- Enhanced vehicle safety with Electronic Stability Control incorporated into the anti-lock braking system.
- Augmented crew survivability with the armor protection of the FMTV A1P2 and a new underbody armor protection kit.

MISSION

The Army employs the FMTV to provide multi-purpose transportation and mobility in maneuver, maneuver support, and sustainment units. Transportation and supply units conduct line and local haul missions carrying cargo, soldiers, and equipment with the LMTV and MTV cargo trucks and their associated LMTV and MTV trailers. Medical units employ the MTV LHS and FMTV LHS trailer to transport, load, and off-load shipping containers with unit equipment. Maintenance units use the MTV wrecker to recover all immobile light- and medium-wheeled vehicles, including all FMTV variants. Engineering units employ the MTV dump truck to haul and dump construction material during quarry operations. All vehicles tested during the FOT&E and LFT&E were equipped with an armored crew cab and the underbody armor protection kit.

PROGRAM

The FMTV is an Acquisition Category IC program. DOT&E approved the Army's operational test plan for the FOT&E in March 2023 and published a combined FOT&E and LFT&E report in October 2023, assessing its operational effectiveness, suitability, and survivability. Testing was conducted to support a full-rate production decision in 1QFY25.

The Army will initially procure 1,894 FMTV A2s through FY27. Although the exact quantities of each variant are still being determined by the Army, the LMTV and MTV cargo trucks are the FMTV A2 variants expected to be procured in the greatest quantities.

» MAJOR CONTRACTOR

- Oshkosh Defense, LLC – Oshkosh, Wisconsin

TEST ADEQUACY

The U.S. Army Test and Evaluation Command conducted FOT&E from March through April 2023 at Fort Bliss, Texas and LFT&E was conducted from August 2019 through July 2022 at Aberdeen Proving Ground, Maryland in accordance with DOT&E-approved test plans. DOT&E observed these tests, which were adequate to assess the operational effectiveness, suitability, and survivability.

Five of the 17 FMTV A2 variants were included in the FOT&E: the LMTV cargo truck, the MTV cargo truck, the MTV LHS truck, the MTV wrecker, and the MTV 10-ton dump truck. These vehicles were operated by soldiers with and without their associated trailers and carried varying cargo loads from empty to the maximum allowable weight. The Army selected these vehicles, with DOT&E's concurrence, based on their planned procurement quantities, unit missions, and load carrying capabilities. During the FOT&E, the unit conducted line and local haul supply, recovery, and quarry missions using these FMTV A2 trucks with armored crew cabs and underbody armor protection kits.

PERFORMANCE

» EFFECTIVENESS

The FMTV A2 is operationally effective when executing its primary local haul missions within the Division and Brigade Area of Operations in accordance with its expected operating scenarios and profiles. The unit equipped with the FMTV A2 successfully completed 87 percent of its unit local haul resupply (cargo), recovery, and quarry missions during the FOT&E. The FMTV A2 did not contribute to any mission failures during the FOT&E. The FMTV A2 demonstrated increased mobility and speeds over secondary roads and cross-country terrain typically found in forward areas compared to earlier models of the FMTV.

The Army did not upgrade its FMTV trailers. The current FMTV trailers became mired during several off-road missions, particularly the LHS trailer. These incidents delayed the delivery of cargo to the supported units.

FMTV A2 effectiveness is reduced during highway missions because the MTV LHS truck, when carrying a full cargo load, was unable to maintain minimum highway speeds (typically 40 miles per hour) on slopes above a two percent grade. This decreased overall unit mobility while operating in a convoy on highways.

» SUITABILITY

The FMTV A2 is operationally suitable for its expected mission scenarios and profiles. The FOT&E was not scoped to determine if the FMTV A2 met its reliability requirements. The five variants tested during the FOT&E did demonstrate the required operational availability and maintainability for the unit to execute its assigned missions. Soldier maintenance times for the LMTV cargo truck and MTV LHS truck met the maintenance ratio requirement, but it was not met for the other variants.

During the FOT&E, crews of five vehicles reported seven instances when the fuel level gauge caused them to mistakenly believe they were low on fuel, thus creating uncertainty in their ability to complete their assigned mission. As a result, crews stowed additional 5-gallon fuel cans on their vehicles to refuel them during missions, which added weight

and introduced an unnecessary vulnerability and hazard. The lack in interior storage space inside the cab made it difficult for soldiers to stow their equipment and supplies needed for missions. The middle seat configuration for the gunner limited visibility and caused discomfort of the neck and back strain when the gunner's hatch was closed. Soldiers had difficulty opening and closing the cab doors, even on level terrain, due to their weight and forward-opening design.

» SURVIVABILITY

The FMTV A2 is survivable to the cyber and live fire threats encountered during operations. The armored cab protected the crew from all required threats and some objective-level threats, but there is a risk of blunt force trauma to soldiers from secondary hazards inside the crew cab. The design of the FMTV A2 provided protection against enacted cyberattacks which do not require physical access to the vehicle. A successful cyberattack requires physical access or compromise of the contractor supply chain.

RECOMMENDATIONS

The Army should:

1. Add a door assist to the crew cab doors to alleviate usability concerns observed during the FOT&E.
2. Verify the accuracy of the fuel level sender assemblies to ensure crews can determine if they need to refuel their vehicles during missions.
3. Develop operating procedures to reduce the weight of cargo loads when traveling on highways to maintain convoy speeds and decrease the likelihood of miring during operations on unimproved roads and traveling cross-country.
4. Field a more robust trailer with improved off-road mobility for the MTV LHS truck, the MTV cargo truck, and the LMTV cargo truck.
5. Eliminate secondary hazards in the cab to reduce the likelihood of crew injuries during missions.

Infantry Squad Vehicle (ISV)

Following the IOT&E conducted in August 2021, the Infantry Squad Vehicle (ISV) manufacturer implemented corrective actions to address reliability and maintainability deficiencies identified in previous testing. The Army conducted reliability compliance testing from June 2022 through January 2023 to validate these corrective actions. The ISV demonstrated a significant improvement to mean miles between system aborts (MMBSA) when compared to previous testing. A tactical airborne operation involving the ISV was conducted in August 2023 to assess soldiers' ability to rig, derig, and employ the vehicle as part of forcible entry operations.

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 can be externally and internally transportable by CH-47 helicopters, externally transportable by UH-60s, and 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 (including cyber survivability). The full-rate production decision was made in March 2023. The Army fielded the ISV to four infantry brigade combat teams in FY23 using low-rate initial production (LRIP) quantities.

» MAJOR CONTRACTOR

- GM Defense, a subsidiary of General Motors – Detroit, Michigan

TEST ADEQUACY

Following the IOT&E conducted in August 2021, the vehicle manufacturer implemented corrective actions to address reliability and maintainability deficiencies identified in previous testing. The Army conducted reliability compliance testing from June 2022 through January 2023 at Yuma Proving Ground, Arizona, to validate these corrective actions. DOT&E provided input to the test plan, but the Army was the approval authority. DOT&E observed the test.

In August 2023, the Army conducted a brigade-level mass tactical airborne operation at Fort Liberty, North Carolina, which included the aerial delivery of five ISV vehicles from U.S. Air Force aircraft. DOT&E approved the test plan and observed the tactical operation.

Consistent with DOT&E's recommendation in the FY22 Annual Report, the Army initiated a technical manual verification event in June 2023. A maintenance evaluation event is planned for 2QFY24.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

The Army reliability compliance testing completed in January 2023, consisted of a single ISV driving approximately 5,000 miles over terrain and at speeds consistent with the mission profile. The ISV demonstrated a significant improvement in MMBSA when compared to the MMBSA demonstrated during the August 2021 IOT&E, and the developmental testing completed at Yuma Proving Ground.

In August 2023, the Army conducted a brigade-level mass tactical airborne operation at Fort Liberty, North Carolina, which included the aerial delivery of five ISV vehicles from U.S. Air Force aircraft. DOT&E analysis is ongoing, precluding an evaluation of the vehicle's suitability. DOT&E 's assessment of system effectiveness and survivability were not part of the tactical airborne operation and are unchanged from the December 2021 IOT&E Report.

RECOMMENDATION

The Army should:

1. Address any DOT&E recommendations from the August 2023 aerial delivery of the ISV as part of a tactical airborne operation.

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

The Army Test and Evaluation Command (ATEC) conducted a Limited User Test (LUT) of the Integrated Personnel and Pay System – Army (IPPS-A) Increment 2 Release 3 in 2Q and 3QFY23. DOT&E is assessing the IPPS-A Release 3 LUT data and expects to issue a report in 2QFY24. IPPS-A Release 3 provides 34 business processes which were evaluated across seven capability areas. The IPPS-A Program Management Office (PMO) has started development of Release 4, which will provide full pay capability.

SYSTEM DESCRIPTION

IPPS-A is the Army's future online Human Resources (HR) and pay solution that transforms antiquated personnel and pay systems to a 21st century Talent Management System. IPPS-A 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 PMO plans to 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.

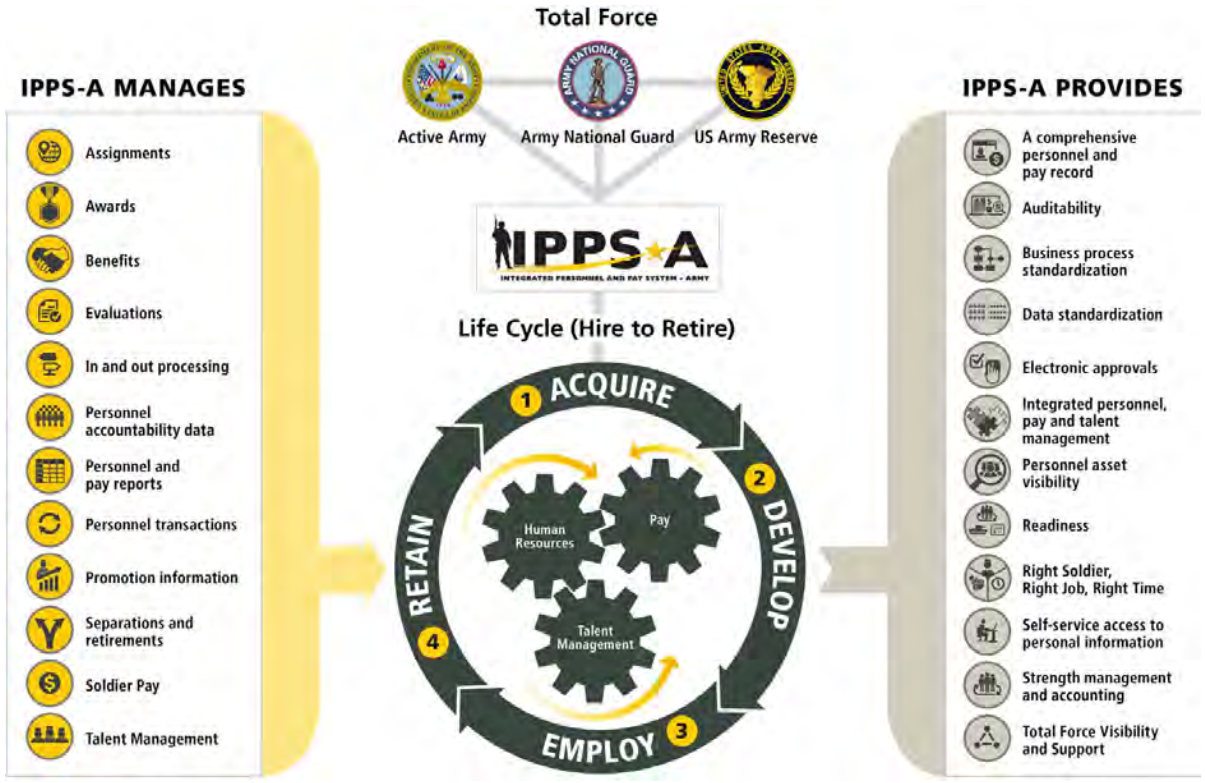
IPPS-A is intended to be a single, integrated personnel and pay system that soldiers can use to conduct self-service personnel transactions such as a change of address which is projected to reduce the need for face-to-face interaction with HR professionals.

MISSION

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

PROGRAM

IPPS-A is a Business System Category 1 program for which DOT&E approved the IPPS-A Test and Evaluation Master Plan (TEMP) in August 2018. Subsequently, DOT&E approved an update to the TEMP to address Release 3 in October 2020. DOT&E approved the operational test plan for the Release 3 LUT in September 2021. DOT&E is assessing the data and expects to issue a report in 2QFY24.



The IPPS-A Release 3 LUT informed an FY23 limited deployment authority to proceed decision to allow deployment of the Release 3 software.

IPPS-A has started development of Release 4, which will provide full pay functionality for all three components of the Army.

» MAJOR CONTRACTOR

- CACI International, Inc. – Chantilly, Virginia

TEST ADEQUACY

The Army Test and Evaluation Command conducted, and DOT&E observed, the IPPS-A Release 3 LUT in two phases in accordance with the DOT&E-approved test plan. IPPS-A Release 3 LUT Phase 2 was conducted from February through March 2023. An adversarial assessment (AA) cyber survivability test was conducted in May 2023. The four life cycle capability areas evaluated during IPPS-A Release 3 LUT were:

- Acquire: Onboard new soldiers, execute military personnel category (MPC) changes, establish benefits for new soldiers and their dependents, and modify contract information to reflect reenlistments and extensions.
- Develop: Execute records management, awards, promotions, and reductions.
- Employ: Execute assignments and account for personnel.
- Retain: Manage pay-impacting areas, such as leave and retirement points; and execute transfers, separations, and restrictions.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E is assessing the data from the IPPS-A Release 3 LUT and will report on operational effectiveness, suitability, and cyber survivability in 2QFY24.

RECOMMENDATION

The Army should:

1. Review the recommendations in the DOT&E report to be released in 2QFY24.

Integrated Tactical Network (ITN)

The Army is transitioning the Integrated Tactical Network (ITN) away from the Middle Tier of Acquisition (MTA) approach of rapidly prototyping and fielding commercial off-the-shelf (COTS) equipment and is moving towards a continuous experimentation and modernization effort. The Army has positioned the ITN to continue to experiment with the tactical network to move from brigade- to division-centric design. The Army was unable to adequately test the equipment for effectiveness, suitability, and survivability due to its inability to execute the DOT&E-approved test and evaluation strategy (TES) of Capability Set (CS) 23.

SYSTEM DESCRIPTION

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

The first CS, known as CS 21 ITN, consists of the COTS single-channel tactical radios, dual-channel headsets, variable height antennas (VHAs), high-capacity

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

MISSION

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

PROGRAM

The ITN consists of two MTA programs: one rapid prototyping and the other rapid fielding. Successful products developed during rapid prototyping have the potential to transition to the rapid fielding program. Program Executive Office Command Control Communications – Tactical is the office of primary responsibility to integrate the systems identified by the Army's Network Cross-Functional Team into the ITN.

In the FY21 Annual Report, DOT&E stated that the Army needed to submit a TES for CS 21 for approval. The Army did not submit a TES for DOT&E approval. The ITN MTA prototyping activities to date have resulted in CS 21 transitioning to rapid fielding. In response to the fielding of CS 21 equipment, DOT&E published a rapid fielding report in January 2022, which stated that the lack of an approved test plan and inadequate data prevented an assessment of operational effectiveness, suitability, and survivability. DOT&E recommended that the Army conduct a fully trained brigade-level exercise in a contested environment, equipped with the full complement of CS 21 ITN equipment, study the manpower needed to operate and maintain the ITN equipment, and continue to develop and rapidly prototype the ITN to address identified problems.

DOT&E approved the TES for CS 23 in June 2022. The Army originally intended for the ITN as an effort to rapidly prototype and field equipment to modernize Army tactical communications at battalion and brigade-level networks. The ITN is now transitioning to support division-centric networks, and the Army is working to define those specific changes. The Army intends to close out the rapid prototyping program at the Outcome Determination, and transition to the Tactical Communications Network Evaluation (TCNE) concept in October 2024. The TCNE will provide continuous test and evaluation to include user feedback, lab-based risk reduction and concept development. The Army signed a rapid fielding acquisition decision memorandum in June 2023 to continue non-recurring engineering efforts for the program until July 2024 and to return in 2QFY24 with a path forward and details of requirements trace to support MTA closeout. The Army Futures Command is in the process of updating the requirements for the future of ITN, pending Army strategic decisions.

» MAJOR CONTRACTORS

MBK

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

VHA

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

Other

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

TEST ADEQUACY

The Army began an operational demonstration of the ITN at Joint Multinational Readiness Center in Hohenfels, Germany from January to February 2023. DOT&E approved the test plan in January 2023 with noted concerns that there was not a single entity responsible for data collection, reduction, and validation and that many required elements were absent from the test plan. The test plan did not reflect the details described in the DOT&E-approved TES, nor what the Army presented to DOT&E at the test concept brief. DOT&E observed the operational demonstration, which was terminated early due to real-world deployment of the test unit.

The operational demonstration was intended to focus on CS 23 COTS equipment for the Stryker BCT with 2nd Cavalry Regiment and address the recommendations from the DOT&E rapid fielding report published in January 2022. Because of the premature termination of the operational demonstration, as well as the data shortfalls identified by DOT&E in the test plan, testing was not adequate to support an assessment.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E is unable to make an assessment of the operational effectiveness, suitability, and cyber survivability of ITN due to premature termination of the operational demonstration and inadequate data collection.

RECOMMENDATIONS

As stated in the FY21 Annual Report and repeated in the January 2022 rapid fielding report, the Army should:

1. Conduct a fully trained brigade-level exercise in a contested environment, equipped with the full complement of CS 21 ITN equipment.
2. Study the manpower needed to operate and maintain the ITN equipment.
3. Continue to develop and rapidly prototype the ITN to address identified problems.
4. Update the TES and event test plans for CS 23 ITN to enable an assessment of operational effectiveness, suitability, and survivability.
5. Identify a single entity responsible for data collection, reduction, and validation prior to conducting all future operational tests.

Integrated Visual Augmentation System (IVAS)

In FY23, Microsoft integrated software changes into the Integrated Visual Augmentation System (IVAS) 1.0 and 1.1 variants to improve reliability and hardware fixes into the IVAS 1.1 variant to improve low-light performance. The Army plans on evaluating improvements to the system and issuing IVAS 1.1 with a limited safety release to continue its campaign of learning. The Army intends to correct other system deficiencies identified in the DOT&E October 2022 IVAS 1.0 Operational Demonstration (Ops Demo) Report in the IVAS 1.2 system variant.

SYSTEM DESCRIPTION

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

MISSION

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

PROGRAM

IVAS is a Middle Tier of Acquisition program with variants in both the rapid fielding (IVAS 1.0 and 1.1) and prototyping phases (IVAS 1.2), intended to equip over 100,000 soldiers in the close combat force.

Based on the results from the IVAS 1.0 Ops Demo, which also identified cyber and electronic warfare vulnerabilities, conducted between May and June 2022, the Army adjusted the IVAS acquisition and fielding strategy to provide time for the Program Office and Microsoft to grow reliability, improve low-light performance, and develop a new form factor. The Army incorporated corrective actions to improve system reliability and performance of low-light sensors in the IVAS 1.1 variant. The Army intends to issue IVAS 1.1 systems to infantry, Stryker, and armored brigade combat team units using a limited safety release in 1QFY25 to inform the Army's campaign of learning. The Army intends to address other deficiencies identified in the 1.0 Ops Demo into the IVAS 1.2 variant and transition from MTA to the major capability acquisition pathway in FY25. The program is planning an operational test of the IVAS 1.2 variant in 2QFY25 to support a full-rate production decision in 4QFY25.

» MAJOR CONTRACTOR

- Microsoft Corporation – Redmond, Washington

TEST ADEQUACY

The vendor conducted testing in 3QFY23 of the technical changes to improve system reliability and performance of low-light sensors for the IVAS 1.1 variant. DOT&E personnel observed portions of the tests.

The Army is developing a test strategy for the IVAS 1.2 variant. Testing of IVAS 1.2 began in 4QFY23 with a User Assessment. Additional User Assessments and Soldier Touchpoints are planned through FY25. An operational test to assess operational effectiveness, suitability, and survivability of the production representative IVAS 1.2 variant is scheduled for 2QFY25 to support a full-rate production decision in 4QFY25. The Army will submit a test plan to DOT&E for approval prior to operational testing.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E published an IVAS Ops Demo report in October 2022 but could not determine the operational effectiveness, suitability, and survivability of the IVAS 1.0 system because it is not production representative.

DOT&E is awaiting the Army T&E strategy of the IVAS 1.2 variant. DOT&E will assess the operational effectiveness, suitability, and survivability (electronic warfare and cyber survivability) of IVAS 1.2 after the completion of operational testing in 2QFY25.

RECOMMENDATION

The Army should:

1. Develop and submit a T&E strategy to assess the operational effectiveness, suitability, and survivability of the IVAS 1.2 variant to DOT&E for approval.

IVAS Test at Fort Drum, New York, August 2023

Javelin Antitank Missile System – Medium

The Javelin system is undergoing two independent, but complementary upgrades, referred to as the G-model missile and Light Weight Command Launch Unit (LW CLU). The Army Test and Evaluation Command (ATEC) conducted a Limited User Test (LUT) on the LW CLU in March 2023 and an FOT&E in August 2023. While analysis is ongoing and DOT&E expects to release a report in 2QFY24, early results from the LUT and FOT&E indicate that the LW CLU achieved its performance requirements and soldiers equipped with the LW CLU performed as well as, or better than, soldiers equipped with the current Block 1 CLU when engaging targets. The LW CLU did not meet its reliability requirement during FOT&E due to a new failure that resulted in multiple system aborts. The G-model missile experienced developmental delays due to a flight test failure in FY22 and will restart government-led flight and lethality testing in FY24.

SYSTEM DESCRIPTION

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

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

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.

Results from the Javelin LW CLU FOT&E will inform the LW CLU full-rate production (FRP) decision planned in 2QFY24. The G-model missile will continue development and testing over the next four years and begin production upon the completion of a successful government-led qualification flight test series. DOT&E approved an updated Test and Evaluation Master Plan (TEMP) for the Javelin program in April 2020 and a LW CLU-specific TEMP addendum in February 2023.

» MAJOR CONTRACTORS

- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Tucson, Arizona
- Lockheed Martin Corporation – Orlando, Florida

TEST ADEQUACY

In FY23, ATEC conducted two operational tests of the Javelin system comparing the LW CLU against the Block 1 CLU, both paired with current inventory missiles. A LUT was conducted at the Cold Regions Test Center, Fort Greely, Alaska in March 2023 and an FOT&E at Yuma Proving Ground, Arizona in August 2023. Both tests were observed by DOT&E and conducted in accordance with the DOT&E-approved TEMP and respective test plans. Together, these tests were adequate to determine the operational effectiveness and suitability of the Javelin LW CLU as well as the system performance in the arctic and desert environments. Analysis of the results are ongoing. DOT&E will publish a classified FOT&E report in 2QFY24 supporting the FRP decision later that quarter.

The G-model missile was not included in the LUT or FOT&E. The Javelin TEMP is being updated to reflect the new G-model development timeline. The updated TEMP should also include a T&E concept for combined LW CLU and G-model missile testing as well as demonstrating the maximum effective range of the upgraded

Javelin as was recommended in the 2022 DOT&E Annual Report.

The LW CLU cyber survivability adversarial assessment (AA), planned for August 2023, was delayed to coincide with a logistics demonstration to better evaluate supply chain risks. An adversarial cybersecurity developmental test (ACDT) was completed in August 2023 to ensure any cyber survivability findings would be corrected in the planned LW CLU software update 4.1. Previous testing included a cooperative vulnerability and penetration assessment (CVPA) of Javelin in FY22. Future cyber survivability testing includes a Javelin AA in 3QFY24, and JOT ACDT in late FY24.

PERFORMANCE

» EFFECTIVENESS

Early results indicate soldiers equipped with the LW CLU performed as well or better than soldiers equipped with the Block 1 CLU at engaging targets day or night, and across the arctic, temperate, and hot desert climates. Infantry units equipped with the LW CLU were operationally effective at conducting their tactical missions. DOT&E will publish an FOT&E report on the system's operational effectiveness in 2QFY24.

» LETHALITY

The G-model missile experienced developmental delays due to a flight test failure in FY22. The program was re-baselined in FY23 and government-led flight and lethality testing in expected to resume in FY24.

» SUITABILITY

Early results indicate that the LW CLU met its reliability requirement at the LUT, but not during the FOT&E due to a new software fault that resulted in multiple system aborts. The program office opened a failure review board, identified a probable cause of the fault, and is planning to implement corrective actions in LW CLU software update 4.1. The corrective action for the new failure mode identified during FOT&E should be demonstrated prior to the FRP decision in 2QFY24 and the LW CLU software update 4.1 should undergo integrated testing prior to equipping the first unit. Representatives from ATEC and DOT&E should witness the demonstration and integrated testing.

Soldier feedback on the LW CLU was positive, with gunners preferring the improved camera resolution and the smaller, lighter form factor as compared to the Block 1 CLU. Soldiers expressed concerns about the LW CLU battery being too exposed to the elements. The LW CLU and Block 1 CLUs both use the same battery, though the Block 1 CLU uses a full battery enclosure and the LW CLU uses a bungee cap to hold the battery in place. Battery performance for both the LW CLU and Block 1 CLU was significantly degraded in the cold temperatures experienced during the LUT. The Army should investigate a long-term replacement strategy for the existing battery to improve cold weather performance.

Soldiers found the new BST to be intuitive, easy to use, and believed that the BST provided the training needed to prepare Javelin gunners to engage targets with the tactical system. The JOT design was not fully mature, and its reliability was poor during the LUT. The JOT performance and reliability improved during the FOT&E. Soldier feedback indicated that the JOT replicates the target engagement process and supports realistic training. Additional development and testing are required to further improve reliability and ensure the JOT can replicate the future G-model missile. DOT&E will publish an FOT&E report on its suitability findings in 2QFY24.

» SURVIVABILITY

Previous testing included a CVPA of Javelin between August and September 2021, and four cyber survivability findings were identified. An ACDT was conducted in August 2023 and the findings will be corrected in LW CLU software update 4.1. Fixes will be verified prior to the AA planned for 3QFY24. A JOT Cyber Vulnerability Identification and ACDT are planned for late FY24. DOT&E will include an update on the system's cyber survivability in 4QFY24 as an addendum to the FOT&E report.

RECOMMENDATIONS

The Army should:

1. Demonstrate the effectiveness of corrective actions for the

new failure mode identified during FOT&E prior to the FRP decision and conduct integrated testing of LW CLU software update 4.1 prior to equipping the first unit. Representatives from ATEC and DOT&E should witness the demonstration and integrated testing.

2. Continue development and testing of the JOT to improve reliability and accurately replicate the G-Model missile.
3. Address the ACDT findings through LW CLU software update 4.1 and conduct fix verification testing prior to conducting the AA in 3QFY24.
4. Update the Javelin TEMP to reflect delays in the G-model missile development and plan for combined G-model missile and LW CLU testing, as well as demonstrating the maximum effective range of the upgraded Javelin system.
5. Investigate a long-term replacement strategy for the existing LW CLU battery to improve cold weather performance.

Joint Air-to-Ground Missile (JAGM)

In accordance with DOT&E's FY22 recommendation to perform arctic testing on the Joint Air-to-Ground Missile (JAGM) to assess the effect of sustained exposure to extreme cold, the Army conducted arctic developmental testing at the U.S. Army Cold Regions Test Center in February 2023. Analysis of the findings is ongoing.

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 in August 2022. The Army completed the first phase of IOT&E in 3QFY20 and the Navy completed the second phase in 2QFY22. DOT&E published a combined IOT&E and LFT&E report in July 2022. The Army approved the JAGM to enter full-rate production in 4QFY22.

» MAJOR CONTRACTOR

- Lockheed Martin Corporation – Orlando, Florida

TEST ADEQUACY

The Army completed arctic environment developmental testing in January and February 2023, at the U.S. Army Cold Regions Test Center, Fort Greely, Alaska. This arctic testing fulfills a recommendation from the DOT&E Combined IOT&E and LFT&E Report published in July 2022. The recommendation was for the Army to conduct missile flight testing in the arctic environment to assess the effect of sustained extreme cold temperatures. This developmental testing was conducted in accordance with the DOT&E-approved Test and Evaluation Master Plan and was observed by DOT&E evaluators.

PERFORMANCE

» EFFECTIVENESS

As previously reported, the JAGM is operationally effective when employed from the AH-64E and AH-1Z, exceeding key performance parameter hit requirements.

Analysis from the developmental testing of the JAGM in the arctic environment is ongoing. Initial findings indicate that winter conditions present some unique challenges for aircrews to effectively employ the JAGM.

The Army and Marine Corps are continuing to develop and field a JAGM Captive Aircrew Training Missile (CATM) for the AH-64E and the AH-1Z. The CATM is a training device allowing aircrews to train and develop JAGM system unique tactics, techniques, and procedures (TTP) without carrying live ordinance. The Marine Corps completed testing during IOT&E in 2QFY22 and is in the process of fielding initial production CATMs for the AH-1Z. The Army is scheduled to receive their initial production CATM for the AH-64E in 3QFY24.

Effectiveness is reduced under high pilot workloads or in time-constrained conditions when the JAGM is employed from the AH-1Z, primarily due to interoperability deficiencies and a cumbersome pilot-vehicle interface (PVI). The Navy continues to conduct root cause analysis to determine the necessary corrections needed to improve AH-1Z interoperability.

» LETHALITY

As previously reported, the JAGM is lethal when employed from the AH-64E and AH-1Z and is more lethal than the HELLFIRE Romeo missile against tanks and light armored vehicles.

The Army is continuing to develop software enhancements to improve height-of-burst lethality. These enhancements may prove effective against vehicle active protection systems. The Army plans to perform verification testing to assess revised software performance.

» SUITABILITY

As previously reported, 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.

The arctic conditions found at the U.S. Army Cold Regions Test Center had no impact on JAGM reliability. The test center stored missiles in an exposed munitions

storage area for 6 months prior to testing, in temperatures as cold as -43 degrees Fahrenheit.

» SURVIVABILITY

As previously reported, the JAGM is survivable against a nascent or limited cyber attacker. JAGM is not survivable against a moderate-to-advanced capability threat.

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. Continue to 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 TTP to ensure aircrew effectiveness.
4. Develop TTP for JAGM employment in winter conditions to optimize effectiveness.
5. Continue to conduct additional tests to refine height-of-burst lethality.
6. Assess the performance of JAGM against vehicles equipped with active protection systems.

Long Range Hypersonic Weapon (LRHW) – Dark Eagle

In August 2023, the Army transitioned to Middle Tier of Acquisition (MTA) rapid fielding authorities to deliver a ground-launched Long Range Hypersonic Weapon (LRHW) (Dark Eagle). The Army program consists of the LRHW transporter-erector-launcher (TEL) and battery operations center (BOC). The Navy is developing the prototype All-Up Round (AUR) under the Conventional Prompt Strike (CPS) program, which is being reported on in a separate article, and supplying them to the Army.

Flight testing of the AUR continued with an attempted launch from the Army's LRHW (Dark Eagle) prototype TEL in March 2023. This test, Joint Flight Campaign-2 (JFC-2), did not occur due to challenges in pre-flight checks. The JFC-2 Retest (JFC-2R) was attempted in September 2023 but did not occur as a result of pre-flight checks. The JFC-3 test is planned for FY24, also planned to be launched from the Army LRHW TEL. JFC testing continues through FY29 using both Navy and Army launchers.

SYSTEM DESCRIPTION

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

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

MISSION

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

PROGRAM

The Army Rapid Capabilities and Critical Technologies Office was responsible for developing and fielding prototype LRHW equipment to the first unit equipped. In August 2023, the Army designated the LRHW as an MTA rapid fielding program and transferred the LRHW (Dark Eagle) program, consisting of the BOC and TEL, to Program Executive Office, Missiles and Space. The Army intends to field two additional batteries of LRHW to complete the MTA rapid fielding phase by FY27.

The Navy's CPS program designed the AUR+C and elements of the weapons control system for the Army's LRHW (Dark Eagle) program in FY23. The Army will integrate the AUR+C with its weapon control system to field a BOC and four TELs to the LRHW unit in FY24.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

As recommended in the FY21 Annual Report, the Army developed a plan for transitioning prototypes for production, fielding, operations, and sustainment to the MTA rapid fielding pathway and completed the transition in FY23.

As recommended in the FY21 Annual Report, the Army is developing the LRHW Master Test Strategy to be submitted for DOT&E approval by 2QFY24. The test strategy should include the following considerations: a concept of employment consistent with the expected operational and threat environment; an operational demonstration which includes strategic-level mission planning; testing and evaluation in the full-spectrum contested environment, including representative targets; and validated modeling and simulation (M&S), combined with ground and subscale test data to support evaluation of mission effectiveness, suitability, survivability, and lethality.

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

The CPS program has performed arena testing on an operationally representative warhead, which is fundamental to the development of the lethality model. Navy CPS sled and flight tests have not included operationally representative targets and do not allow for a direct assessment of the weapon's lethal effects. The Navy intends to rely on a combination of M&S, component testing, and hardware-in-the-loop evaluations to incorporate the contested environment and is investigating methods to obtain lethality and effectiveness data

by incorporating representative targets into flight and ground tests.

The Army has not evaluated the effects of a full-spectrum threat (kinetic, non-kinetic, electromagnetic, cyber) contested environment on the performance of the AUR, the TEL, or the BOC. The Army is relying on the Navy's use of a combination of M&S, component testing, and hardware-in-the-loop evaluations to evaluate full-spectrum survivability of the AUR in the representative threat environment. The LFT&E strategy, written by the Navy and incorporating Army-specific targets and environments, is expected to be submitted for DOT&E approval in 2QFY24.

The Army and Navy conducted one JFC test shot of the prototype AUR in FY22, during which a test anomaly prevented acquisition of data over a portion of the planned flight profile. Flight testing of the CPS prototype AUR continued with an attempted launch from the Army's LRHW prototype TEL in March 2023. This test, JFC-2, did not occur due to a system anomaly which prevented ignition of the AUR. The Navy has identified the cause of the anomaly and implemented corrective actions. The retest (JFC-2R), planned to be launched from the LRHW TEL, was intended to be conducted in September 2023. As a result of pre-flight checks, the test did not occur. The test was not planned to be conducted in an operationally realistic environment (cyber and electromagnetic) and did not use representative threat targets. JFC-3 is planned for FY24, also to be launched from the LRHW TEL. JFC testing is scheduled to continue through JFC-10 in FY29.

DOT&E will provide an early fielding report of the demonstrated operational effectiveness, lethality, suitability, and survivability of the LRHW and CPS AUR+C system with associated flight tests conducted through FY26.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

Not enough data are yet available to evaluate the operational effectiveness, lethality, suitability, and survivability of the LRHW system.

RECOMMENDATIONS

The Army should:

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

Mounted Mission Command – Software (MMC-S)

The Army Test and Evaluation Command (ATEC) conducted the Mounted Mission Command – Software (MMC-S) Version 3.1 IOT&E in April 2023, at Fort Liberty, North Carolina in support of a full deployment decision in October 2023. In September 2023, DOT&E published the MMC-S IOT&E report that assessed the software as operationally effective, suitable, and survivable.

SYSTEM DESCRIPTION

MMC-S is the main software piece of the Mounted Computer Environment (MCE) which makes up part of the Army's Common Operating Environment (COE). MMC will leverage the existing Joint Battle Command – Platform (JBC-P) program of record and evolve utilizing a phased modernization approach with four lines of effort under the MMC Family of Systems:

- Software
- Network
- Transport Hardware
- Compute and Store

MMC-S is based on open standards that promote competition and enable the ability to incorporate new technology. As part of the MCE, MMC-S provides all the movement and maneuver apps but also supports the needs of the wider community and warfighting functions.

MMC-S will be deployed as a software-only upgrade to replace JBC-P software. MMC-S will evolve over time using existing MMC transport and hardware capability-maturation. MMC-S is intended to provide a common user experience that enables leaders to lead their formations from anywhere on the battlefield.

MISSION

MMC-S is part of the Army's concept to facilitate the seamless transfer of information across numerous platforms and provide critical situational awareness to commanders at all echelons. MMC-S contributes to the Army's doctrinal Operations Process by enhancing the commander's ability to coordinate the warfighting functions (Fires, Maneuver, etc.) through the Plan, Prepare, Execute, and Assess components of the Operations Process. MMC-S contributes to mission success through a variety of capabilities to include the Common Operating Picture, Mobile Command on the Move, collaboration tools, and a common look and feel and interoperability with legacy systems.

PROGRAM

The program conducted a materiel development decision in May 2020 entering MMC-S into the acquisition system as an ACAT II program at the limited deployment decision. However, the program adjusted in June 2022 to cancel the limited deployment decision and continue with developmental testing along with a planned IOT&E to support a full deployment decision in September 2023 on the 3.1 version of the software. DOT&E approved the Test and Evaluation Master Plan (TEMP) in January 2023.

DOT&E published the IOT&E report in September 2023, assessing the system as operationally effective, suitable, and survivable. The Army conducted a full deployment decision in October 2023. The program will pivot to an Agile approach for quarterly software releases. The program intends to incorporate this Agile approach in an updated TEMP.

» MAJOR CONTRACTORS

- Government Lead System Integrator – Aberdeen Proving Ground, Maryland
- Combat Capabilities Development Command, System Simulation, Software and Integration – Huntsville, Alabama

TEST ADEQUACY

The Army conducted an IOT&E of MMC-S in April 2023 with a complete cavalry squadron from the 2nd Brigade 82nd Airborne Division. DOT&E approved the test plan in March 2023 and observed the IOT&E. MMC-S IOT&E was adequate to assess operational effectiveness, suitability, and survivability. Operational testing was conducted in accordance with the DOT&E-approved test plan. MMC-S and JBC-P were the primary means of communication for the test unit during the test. The test unit provided a fully manned headquarters command post that included representation from all staff elements. In addition, the squadron was comprised of two complete reconnaissance troops equipped with vehicles integrated

with either MMC-S or JBC-P systems. The squadron also had a combat support troop present that contained a mix of MMC-S and JBC-P equipped vehicles as well as dismounted soldiers using the Nett Warrior system. This third troop provided combat support and service support such as refueling, medical evacuation, etc. to the squadron headquarters and two reconnaissance troops.

The Army conducted an adversarial assessment (AA) of MMC-S at Fort Liberty during the record test window in accordance with the DOT&E-approved test plan. U.S. Army Combat Capabilities Development Command Analysis Center provided data collectors and analyzed the prevent, mitigate, and recover data from the test site and the Network Operations Center. The U.S. Army Threat Systems Management Office supported the AA as the cyber threat stimulus. The purpose of the AA was to characterize how a cyber compromise might degrade the mission capability of MMC-S in the presence of representative defensive tools, personnel, training, and procedures.

The IOT&E uncovered shortcomings in the quality and quantity of delivered instrumented data, and a significant set of technical questions could not be assessed. Data reduction proved to be insufficient due to complexities in the reduction of the data. DOT&E leveraged Mission Event Logs produced by MMC-S to supplement its effectiveness evaluation to overcome instrumentation shortcomings.

PERFORMANCE

» EFFECTIVENESS

MMC-S is operationally effective. MMC-S was useful for all phases of the Operations Process and across all operational factors: time of day, set of cavalry missions, weather, and electronic warfare conditions. Unit leaders stated that MMC-S provided utility and flexibility. The messaging system, particularly chat and free messaging, allowed for quick, long-range communications. Overall, unit soldiers preferred MMC-S over the legacy JBC-P system and provided recommendations for improvement to better support their mission as MMC-S does not yet offer the complete set of messages that JBC-P supports, nor does it integrate with onboard sensor systems such as mounted vehicle optics.

The MMC-S common operational picture allowed operators to develop and maintain situational awareness of the battlespace and the messaging system, particularly chat and free text messaging, allowed for quick, long-range communications, to include disseminating orders, across all tactical echelons. The data DOT&E was able to use showed that messages arrived in a timely and accurate manner. Several anomalies were noted during the test; however, the lack of sufficient instrumentation data prevented any further analysis.

» SUITABILITY

MMC-S is operationally suitable. The system is rapidly recoverable by operators when problems occur, the user interface is intuitive and easy to use, and the provided training prepared soldiers to operate and maintain the system without field service representatives. Operators were able to resolve most failures without external support.

The system does need to improve in order to meet its reliability requirements. The MMC-S training was sufficient for the IOT&E, but did not emphasize troubleshooting, and the quick reference guides and training manuals were not easily available on the MMC-S interface. Unit leaders acknowledged the lack of collective training that teaches units how to use MMC-S to support the Operations Process.

» SURVIVABILITY

DOT&E found that the MMC-S, as configured, is cyber survivable to nascent actors from outsider threat postures. Details can be found in the classified annex of the IOT&E report.

RECOMMENDATIONS

The Army should:

1. Create collective training requirements and program for operating and managing the MMC-S.
2. Integrate vehicle systems and sensors to MMC-S (such as mounted vehicle optics).

3. Incorporate soldier feedback into technical manuals and quick reference guides that are easily accessible within MMC-S.
4. Continue refining the test activities required to support the Agile development and release of software and submit an updated TEMP to DOTE for approval.
5. Address the cyber recommendations in the classified annex of the IOT&E report.

Next Generation Squad Weapons (NGSW) Weapons and Ammunition (W&A)

Next Generation Squad Weapon Rifle XM7 (NGSW-R) (top) and Automatic Rifle XM250 (NGSW-AR) (bottom)

In FY23, the Army conducted developmental and Live Fire Limited Lethality Assessment (LLA) on Next Generation Squad Weapons (NGSW). The Army plans to conduct a Limited User Test (LUT) at Fort Campbell, Kentucky in 1QFY24. DOT&E intends to write a report after completion of the LLA and LUT.

SYSTEM DESCRIPTION

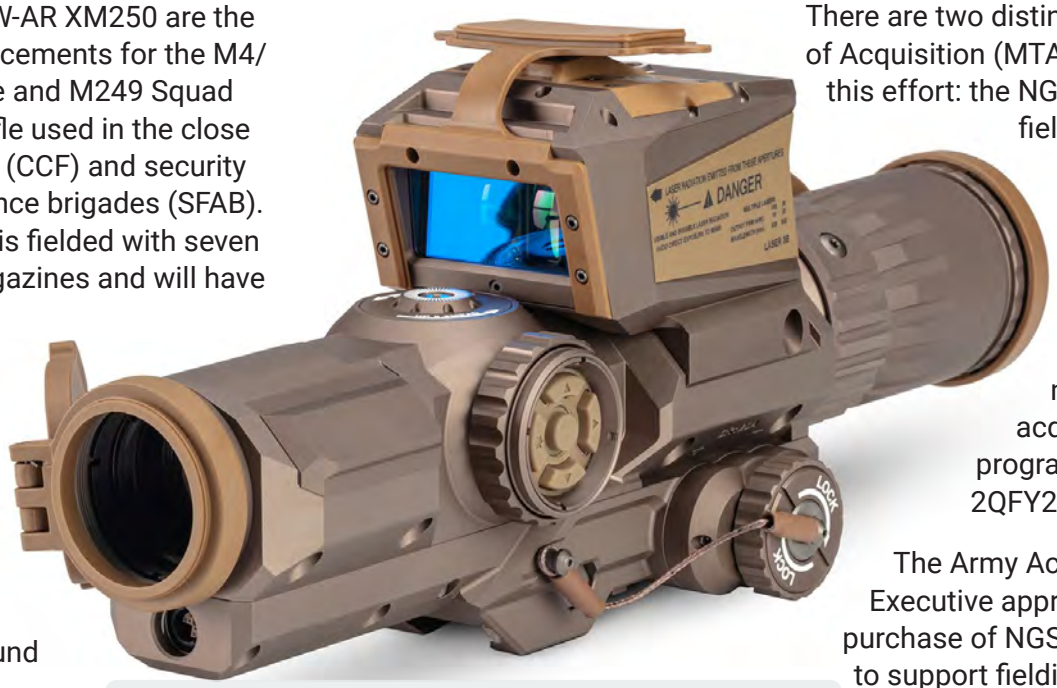
The NGSW system includes the Rifle (NGSW-R) XM7, Automatic Rifle (NGSW-AR) XM250, 6.8mm ammunition common to both weapons, and Fire Control (NGSW-FC) XM157 to be mounted on each weapon. The NGSW-R XM7 and the NGSW-AR XM250 are the planned replacements for the M4/M4A1 carbine and M249 Squad Automatic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

The 6.8mm ammunition includes General Purpose (GP), Special Purpose (SP), Blank, Reduced Range, Tracers, marking, and Drill Dummy Inert ammunition.

MISSION

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

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



Next Generation Squad Weapon Fire Control (NGSW-FC)

PROGRAM

There are two distinct Middle Tier of Acquisition (MTA) programs in this effort: the NGSW W&A rapid fielding and the NGSW-FC rapid fielding. The programs may transition to multiple major capability acquisition programs (MCAs) by 2QFY27.

The Army Acquisition Executive approved the purchase of NGSW systems to support fielding to the CCF starting in 2QFY24. DOT&E plans to write a report following the LUT and LLA in support of this fielding. The NGSW-R and -AR will initially be fielded and tested with GP and Blank ammunition. Testing of the SP ammunition is scheduled to begin in FY24.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

DOT&E approved the TEMP for the MTA phase in August 2023, with caveats to include testing the capability to stow the weapons, and the effect on crew members' ability for ingress/egress on major weapons platforms. In support of the continued campaign of learning, DOT&E expects testing not currently covered during the MTA phase to be addressed by the Army in the next TEMP update.

During the MTA phase, the Army is planning to conduct a LUT in 1QFY24, which is equivalent to an operational demonstration per DoD Instruction 5000.89, followed by an operational assessment in 1Q – 2QFY25. If the program transitions to MCAs, a DOT&E-approved TEMP will outline the additional testing requirements.

DOT&E plans to write a report after completion of the LLA and LUT to support the Army's fielding decision. The LUT is not intended for DOT&E to make a complete assessment of operational effectiveness, lethality, suitability, and cyber survivability. The data and testing obtained during the MTA phase will enable an expedited operational assessment (OA). A report will follow the OA currently planned for 1QFY25, assessing the operational effectiveness, lethality, suitability, and survivability.

In FY23, the Army conducted developmental and live fire lethality testing on NGSW components. The testing included:

- A Soldier Touchpoint in 1QFY23 to confirm technical test results, assess the maturity of NGSW, and obtain soldier feedback.
- A First Article Test completed in 3QFY23 to verify that the NGSW-FC XM157 conformed to all contract requirements.
- An LLA in 4QFY23 to assess the lethality of the GP 6.8mm round against a subset of operationally relevant targets. The full range of operationally relevant targets will be assessed for the 6.8mm GP and SP rounds in the LFT&E scheduled for 3QFY24 –1QFY25.
- A Production Qualification Test from 3Q – 4QFY23 to measure the current design compliance to system performance requirements.

The GP 6.8mm munition exceeds current training range capacities for the use of NGSW for urban and close quarters combat testing. The Army's real-time casualty assessment system is being upgraded to support force-on-force testing. The Army intends to address both limitations to enable an adequate OA in FY25.

A cooperative vulnerability and penetration assessment (CVPA) is planned in 4QFY23 to characterize the cyberattack surface and cyber resiliency of the NGSW. This CVPA will enable the adversarial assessment planned to be conducted during the OA in FY25.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

Sufficient data do not exist yet to assess NGSW operational effectiveness, lethality, suitability, and cyber survivability. DOT&E will write a report after completion of LUT and LLA to support the fielding of the CCF in 2QFY24 but will not make a full assessment of operational effectiveness, lethality, suitability, and cyber survivability at that time. A report that will assess the operational effectiveness, lethality, suitability, and survivability will be published following completion of the OA in FY25.

RECOMMENDATIONS

The Army should:

1. Submit an operational test plan for DOT&E approval for the FY25 OA to assess operational effectiveness, lethality, suitability, and cyber survivability of the system.
2. Provide for DOT&E's approval a test strategy to evaluate the capability to stow the weapons, and the effect on crew members ability for ingress/egress on major weapons platforms.

Sentinel A4 Radar

The U.S. Army Test and Evaluation Command (ATEC) conducted a Limited User Test (LUT) in March and April 2023 to support the Sentinel A4 Radar Milestone C (MS C) decision in July 2023. The Army used results and lessons learned from the LUT and other events to scope its planned engineering and developmental testing after MS C in preparation for IOT&E beginning in 1QFY25.

SYSTEM DESCRIPTION

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

MISSION

The Sentinel Radar is a major component of the Army Integrated Air and Missile Defense system of systems architecture. It provides a 360-degree surveillance and fire control capability against low to mid-altitude threats, to include CM, UAS, FW and RW aircraft, and RAM threats. In order to continue to meet its mission requirements and to address counter-RAM requirements, the Army plans to replace its legacy Sentinel A3 radars with the Sentinel A4 radar, which use advanced Active Electronically Scanned Array sensor technologies to improve performance. The Sentinel A4 is a Multi-Mission Radar which simultaneously provides search and track against FW and RW aircraft, UAS, CM, and RAM threats.

PROGRAM

Sentinel A4 Radar is an Acquisition Category II program that DOT&E placed on oversight in February 2023. The Milestone Decision Authority approved the program's MS C decision in July 2023.

The program office submitted a Test and Evaluation Master Plan (TEMP) in September 2023 for DOT&E's approval. It was returned and requested to be resubmitted in 90 days.

The total acquisition objective is 240 Sentinel A4 Radars.

The Army plans to conduct IOT&E beginning in 2QFY25. DOT&E will publish a classified report following the conclusion of the IOT&E in support of a full-rate production decision in 4QFY25.

» MAJOR CONTRACTOR

- Lockheed Martin Corporation – Syracuse, New York

TEST ADEQUACY

ATEC conducted a LUT from March 6 to April 14, 2023, in accordance with the Army-approved test plan to inform the MS C decision. The planning and approval of this test was conducted prior to the program being placed on DOT&E oversight. DOT&E did not approve the operational test plan but observed the testing. Two Sentinel A4 Radars performed multiple 72-hour missions under day and night conditions against a variety of air targets. ATEC published a classified Operational Test Agency Milestone Assessment Report (OMAR) following the LUT. The Army is applying lessons learned from the deficiencies identified during the LUT and other testing to scope its planned engineering and developmental testing after MS C, to ensure the program is ready to begin IOT&E in 2QFY25. DOT&E will consider the Army's OMAR and the data from the LUT when assessing the IOT&E plan and developing the IOT&E report.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

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

RECOMMENDATIONS

The Army should:

1. Address the deficiencies identified in the ATEC's OMAR.
2. Develop an IOT&E plan in accordance with an approved MS C TEMP.

Soldier Protection System (SPS)

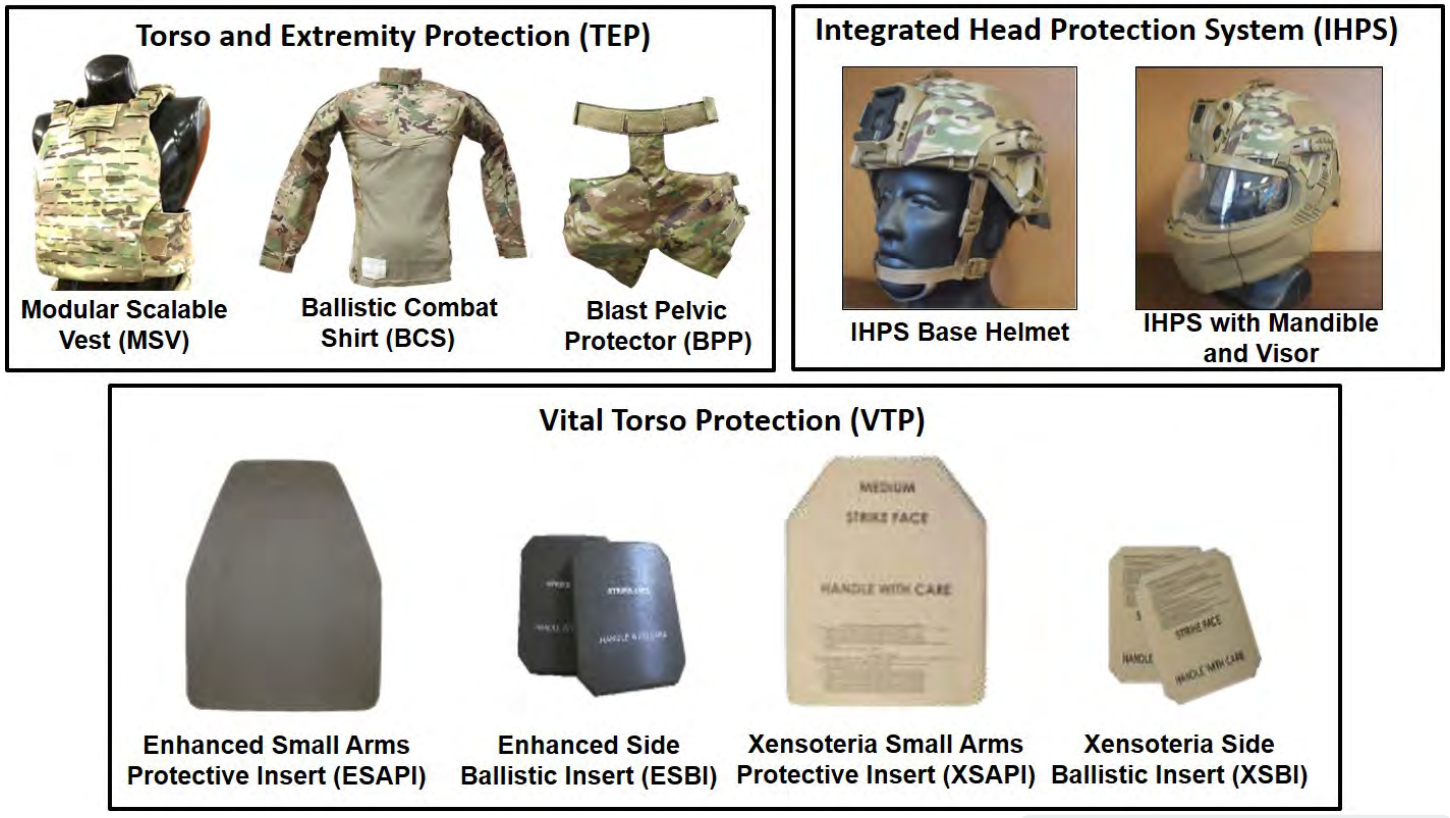
The Army continues to field the Second Generation Modular Scalable Vest (MSV Gen II) and Third Generation Vital Torso Protection (VTP Gen III) hard armor plates, with fielding expected to complete in 4QFY28. Since last year's Annual Report, the Army completed First Article Testing (FAT) for multiple vendors and over 150 Lot Acceptance Tests (LAT) for all SPS systems with zero LAT failures. The Army should plan testing beyond FAT and LAT for the Next Generation Integrated Head Protection System (NG-IHPS) to be able to assess soldier survivability.

SYSTEM DESCRIPTION

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

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

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

The Army started early fielding of MSV Gen II and VTP Gen III plates in 4QFY21 and plans to field through 4QFY28. The target acquisition quantity is approximately 150,000 sets of each of the SPS torso subsystems. The Army plans to begin fielding of the NG-IHPS in 1QFY24.

DOT&E, in coordination with the Program Executive Officer Soldier, and the Commander of Marine Corps Systems Command will provide a briefing to the House Committee on Armed Services not later than December 23, 2023, on female soldier and marine equipment evaluation and what, if any, processes are in place to ensure future body-worn systems are evaluated for fit and appropriate wear through the 98th percentile of all possible sizes.

» MAJOR CONTRACTORS

TEP Vendors:

- Armor Express – Eden, North Carolina (MSV, BPP)
- Bethel Industries, Inc. – Jersey City, New Jersey (MSV, BPP)
- Slate Solutions – Sunrise, Florida (MSV)
- Point Blank Enterprises, Inc. (Protective Apparel & Uniform) – Pompano Beach, Florida (MSV, BCS)
- Carter Enterprises, LLC – Brooklyn, New York (BCS)

VTP Vendors:

- Engense, Inc. – Camarillo, California (ESBI)
- Florida Armor, LCC – Miami Lakes, Florida (ESBI)
- Leading Technology Composites, Inc. – Wichita, Kansas (ESAPI, ESBI)
- TenCate Advanced Armor USA, Inc. – Hebron, Ohio (ESAPI, XSBI)
- Avon Protection– Irvine, California (XSAPI, ESAPI, XSBI)

NG IHPS Vendors:

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

TEST ADEQUACY

The Army conducts multiple FATs and LATs every year to qualify new vendors and designs. In FY23, the Army completed FAT for multiple vendors to include: TEP's MSV, VTP's Enhanced Small Arms Protective Insert (ESAPI) and Enhanced Side Ballistic Insert (ESBI) designs, and NG-IHPS. The designs that passed FAT proceeded to LAT. The Army completed all test series at Aberdeen Test Center, Maryland in accordance with DOT&E-approved test plans. DOT&E observed most of the FAT testing. As recommended in the FY22 Annual Report, the Army has begun an expanded developmental test series, which is scheduled to be completed in 1QFY24, to compare legacy VTP and SPS VTP Gen III plates against nonstandard fragmenting threats.

The Army is investigating the options to test beyond FAT and LAT to be able to assess potential injuries to soldiers from threats that penetrate the NG-IHPS, and to compare the results with IHPS protection.

Current PPE test methods are limited in the ability to accurately assess soldier injuries. Test mannequins for soft armor vests and hard armor plates do not sufficiently mimic the wearer. The Army developed the Hybrid Foam Mannequin to address these limitations in FY16, but still has not finished the accreditation process. As DOT&E recommended in the FY22 Annual Report, the Army should complete accreditation of the Hybrid Foam Mannequin and adopt test methods used by lethality programs (e.g., use of gel blocks, and instrumentation to characterize the in-flight projectile characteristics) to be able to assess potential injuries to soldiers from penetrating threats. Test data are needed to enable modeling of the relevant hard plates and helmets as penetrable materials, limiting the ability to use modeling and simulation to assess conditions without LFT&E.

PERFORMANCE

» SURVIVABILITY

Two MSV Gen II designs tested in FY23 met the ballistic FAT requirements. Four VTP designs (a combination of ESAPI and ESBI plates) were submitted for FAT since last year's Annual Report; 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. Since the last Annual Report, over 150 LATs (for all SPS systems) have been conducted with zero LAT failures.

As reported in the FY22 Annual Report, one vendor failed to meet the NG-IHPS FAT ballistic test requirements. The vendor submitted a redesigned helmet for re-FAT in FY23 and the redesigned helmet passed FAT. Additional testing is required to assess NG-IHPS protection compared to legacy helmets and to assess the degree of potential injuries to warfighters from penetrating threats to the NG-IHPS.

RECOMMENDATIONS

The Army should:

1. Plan and conduct testing on the NG-IHPS to enable a comparison to the protection provided by the legacy IHPS and the assessment of warfighter injuries against penetrating threats.
2. Start the accreditation process of the Hybrid Foam Mannequin or develop another accredited soldier surrogate for assessing injuries from penetrating threats to hard and soft body armor.
3. Collect the necessary data to improve modeling and simulation capabilities to be able to assess potential warfighter injuries for a range of conditions not tested.

UH-60V Black Hawk Digital Cockpit

The Army completed IOT&E II on the UH-60V in August 2022. DOT&E published the report in December 2022, finding the UH-60V operationally effective, suitable, and survivable. The Army's production decision is pending.

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 medical evacuation (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 one to 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 was approved in 2014 and with a revision in December 2020. DOT&E approved the updated Test and

Evaluation Master Plan in October 2021. The Army completed IOT&E II in August 2022. The Army planned to make a full-rate production decision in 2QFY23 but is continuing to conduct acquisition strategy analysis. The Army now anticipates a full-rate production decision 2QFY24. Planning is ongoing for the UH-60V MEDEVAC variant FOT&E, scheduled to occur 4QFY24.

» MAJOR CONTRACTORS

- Redstone Defense Systems – Huntsville, Alabama (development and engineering)
- Northrop Grumman Corporation – Woodland Hills, California (avionics enhancements)

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 a cyber adversarial assessment on the UH-60V in March 2022, at Redstone Arsenal, Huntsville, Alabama, and IOT&E II in July and August 2022, at Fort McCoy, Wisconsin. The adversarial assessment and IOT&E II were conducted in accordance with DOT&E-approved test plans and was adequate to assess system performance. DOT&E published the IOT&E II report with a classified annex in December 2022. The Army plans to make a full-rate production decision on the UH-60V in 2QFY24.

PERFORMANCE

» EFFECTIVENESS

The UH-60V is operationally effective. The UH-60V digital cockpit provides pilots with improved situational awareness, enhanced mission planning capability, an expanded communication suite, and improved instrument flight capabilities when compared to the UH-60L. The UH-60V meets external lift and troop movement requirements with approximately the same performance margin as the UH-60L. IOT&E II data indicate that key performance shortfalls observed during IOT&E I, including map display latency, missing map data, and uncommanded range scale changes, have been resolved.

The Aviation Mission Planning System needs improvements to enhance the effectiveness of aircrew mission planning. Currently, the system does not transfer planned airspeeds to the UH-60V mission computers, resulting in aircrews having to manually input airspeeds.

» SUITABILITY

The UH-60V is operationally suitable. The UH-60V met its reliability, availability, and maintainability requirements, demonstrating improvements during IOT&E II compared to IOT&E I.

There are areas that require improvement, and these will be reassessed during the planned FOT&E of the UH-60V MEDEVAC variant. The interactive electronic technical manuals and operator manual should be updated to correct missing information and inaccuracies. Maintenance personnel did not believe that the hands-on portion of new equipment training was sufficient due to the degree of changes and pilots stated that additional training on the Blue Force Tracker system is needed. Additionally, pilots have reported issues with the Heads-Up Display's power cord snagging during certain body movements and that applying the parking brake is ergonomically uncomfortable. Crew chiefs expressed concerns regarding their seats and the possible cumulative effects on fatigue.

» SURVIVABILITY

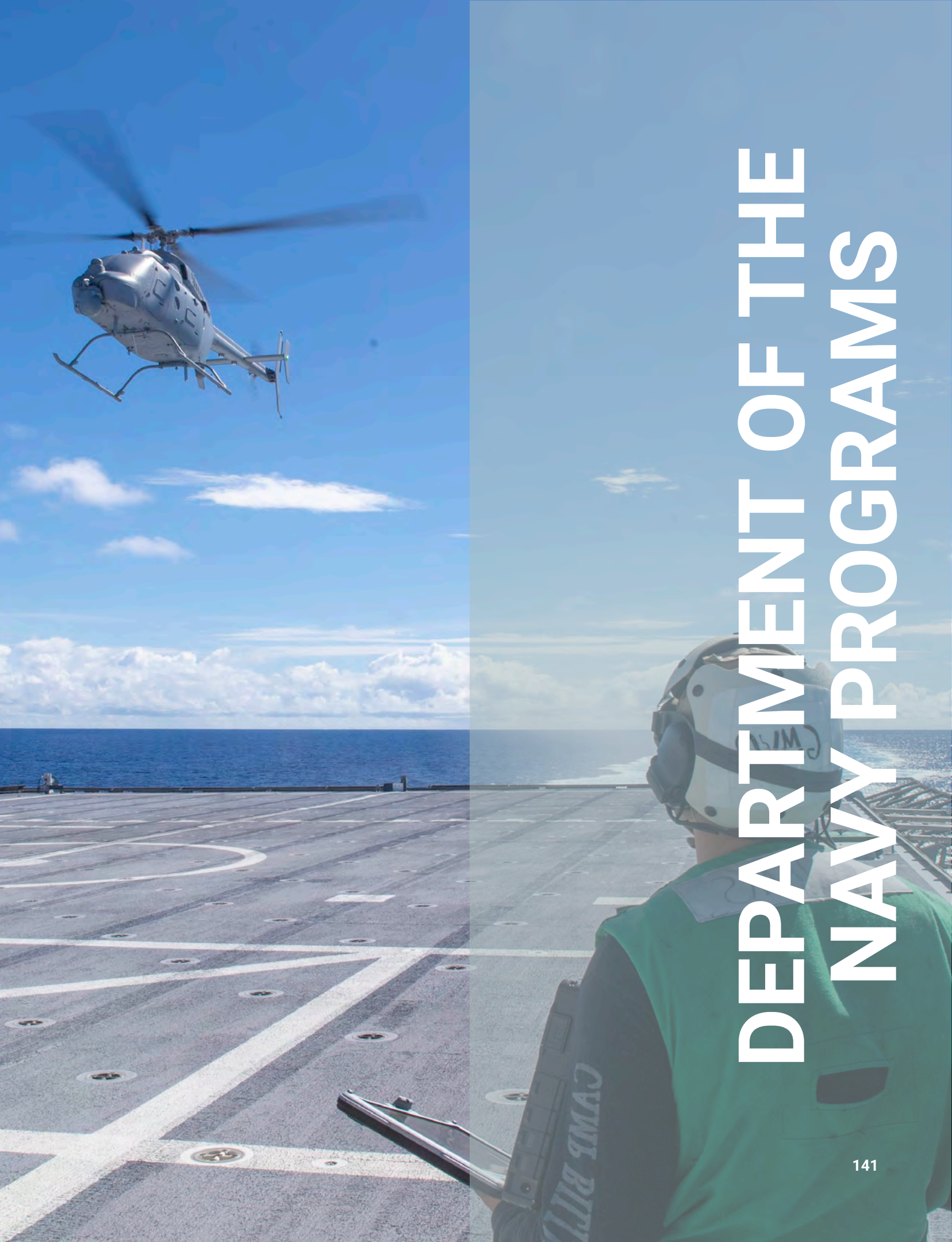
The UH-60V's survivability against ballistic, infrared, radar, and laser threats is equivalent to the UH-60L fleet. It is survivable against moderate cyber threats with nearsider or insider access.

RECOMMENDATIONS

The Army should:

1. Update UH-60V interactive electronic technical manuals and operators manuals to ensure they are complete and accurate for changes to UH-60V subsystems.
2. Improve maintenance personnel training by incorporating more hands-on UH-60V troubleshooting into the UH-60V training program.

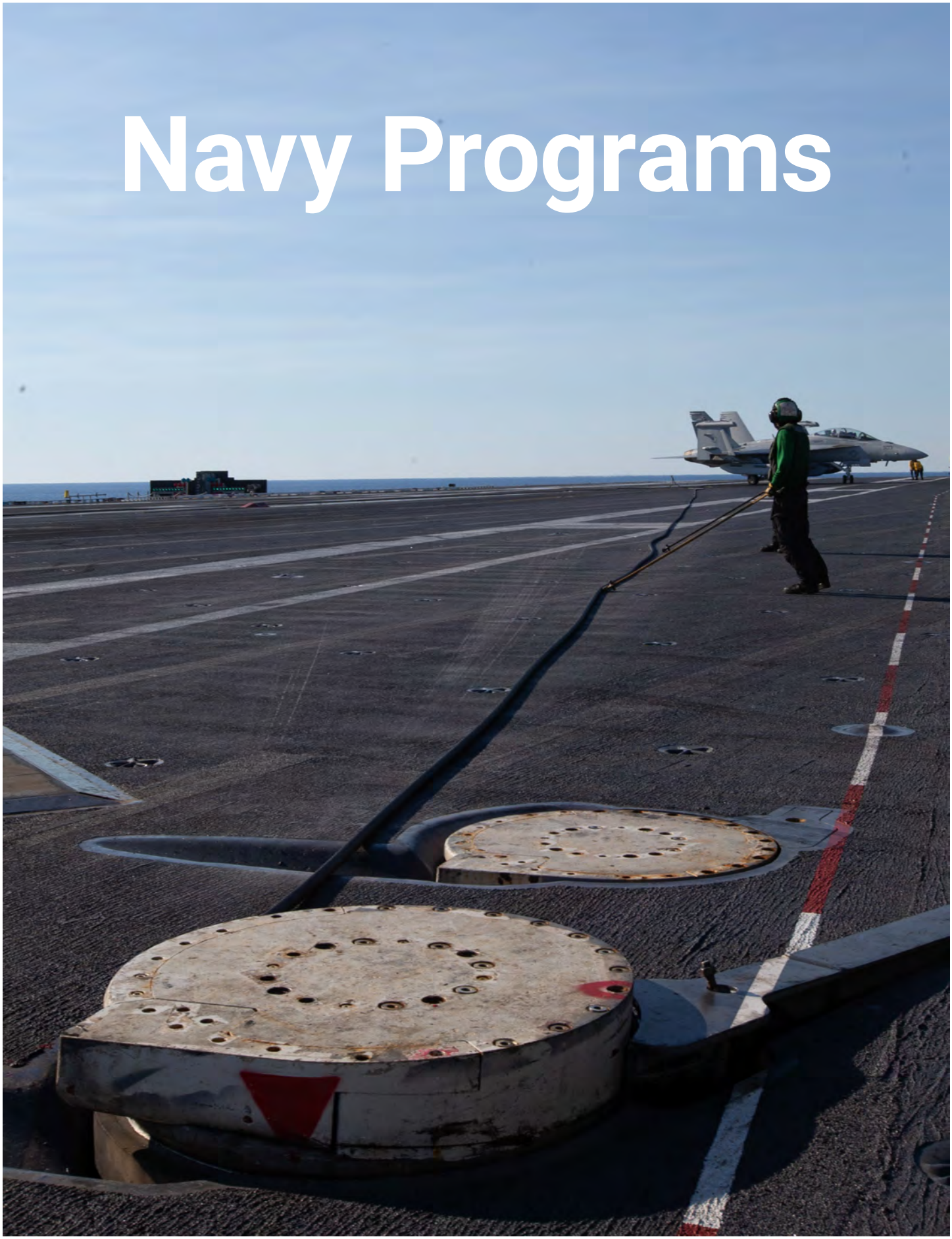
3. Modify the Head's-Up Display to reduce the likelihood that the cord will snag.
4. Modify the UH-60V software to import airspeeds planned with the Aviation Mission Planning System.
5. Refine pilot training to cover Blue Force Tracker usage in more depth and increase the focus on procedures unique to UH-60V.
6. Modify the UH-60V parking brake to make it easier to set.
7. Conduct an ergonomic study to investigate the usability and fatigue contribution factors of the UH-60V crew seats.



DEPARTMENT OF THE NAVY PROGRAMS

This page intentionally left blank.

Navy Programs



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

The Navy has completed six developmental test (DT) shots (DT1-DT6) since FY21 for the AGM-88G Advanced Anti-Radiation Guided Missile – Extended Range (AARGM-ER), to identify and fix problems before beginning integrated operational testing. The Navy executed three developmental free-flight tests in FY23 from F/A-18Fs in November 2022 (DT4), April 2023 (DT5), and July 2023 (DT6). AARGM-ER IOT&E free-flight tests are scheduled to begin in 1QFY24.

SYSTEM DESCRIPTION

The AARGM-ER, is an air-to-ground missile designed to passively detect and guide on radio frequency emissions from a threat radar site and then transition to an active millimeter wave (MMW) terminal radar seeker to detect, track, and suppress or destroy radio frequency-enabled, surface-to-air missile systems. AARGM-ER reuses the same MMW radar as AARGM (non-extended range) and introduces a new warhead and a larger diameter, but shorter, rocket motor for increased lethality at relevant ranges against modern surface-to-air threats. The F/A-18E/F and EA-18G are threshold employment platforms for AARGM-ER, while the F/A-18C/D

and F-35A/B/C (internal carriage for the F-35 A and C variants) are designated objective employment platforms with associated key schedule parameters.

MISSION

Operational commanders will employ AARGM-ER to suppress or destroy enemy air defenses. The AARGM-ER missile targets relocatable, integrated air-defense radars and other targets that can employ shutdown tactics. The multi-mode seeker of AARGM-ER counters those enemy shutdown tactics.

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 and an updated cyber survivability test strategy in August 2022. The production and deployment phase, with the low-rate initial production contract award, came after the Navy's Knowledge Point-4 program review in July 2021. AARGM-ER operational testing began with the first phase of cyber survivability testing, a cooperative vulnerability and penetration assessment (CVPA), in 4QFY23. IOT&E free flights will begin in 1QFY24. The Navy is planning for initial operational capability in 3QFY24.

» MAJOR CONTRACTOR

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

TEST ADEQUACY

The program completed six DT shot events (DT1-DT6) since FY21 to identify and fix problems before beginning integrated operational testing, along with a CVPA, per the DOT&E-approved Test and Evaluation Master Plan and associated test plans. DOT&E observed the testing. The F/A-18F has conducted all the DT free flight events to date; EA-18G Growler has not yet executed a free flight test event as the other designated threshold platform. Free flight events occurred at Point Mugu Sea Range, California, and the China Lake Ranges, California, through coordination and integration with the Nevada Test and Training Range, Nevada.

The missiles fired prior to DT5 incrementally incorporated new AARGM-ER hardware components. DT5 incorporated the complete low-rate initial production AARGM-ER hardware, but not the fielding-representative software. DT6 included the low-rate initial production AARGM-ER hardware and the most current version of AARGM-ER software at the time of the test. DT4 took place in November 2022 and engaged a moving maritime target, whereas DT5 conducted in April 2023, and DT6 conducted in July 2023, engaged threat-representative, land-based, integrated air defense targets. These test events provided opportunities to identify discrepancies and implement fixes; however, the discrepancies required software updates that proved more complex than anticipated, requiring additional time to correct and implement. The time necessary to analyze data, develop, and incorporate fixes resulted in delays to Flight Test Vehicle delivery, revisions to the test schedule, and delays in the final software delivery, all of which delayed Integrated Test One (IT1) from 4QFY23 to 1QFY24.

AARGM-ER has yet to execute a successful end-to-end test that achieves threshold range employment, anti-radiation homing guidance with a transition to MMW seeker target discrimination, and engagement of the designated threat with the newly designed anti-radiation homing subsystem. FY24 will contain IT events to test the end-to-end system processes at threshold range, and operational test (OT) events to test the end-to-end processes with the newly designed warhead, under governing range safety restrictions. IT will occur after the final software is delivered from Northrop Grumman in 1QFY24, which will require a series of regression tests of the new software, including multiple captive carry missile events in a compressed time period. After the first IT event, there is a scheduled IOT&E free-flight event approximately every two weeks, beginning in October 2023 through 2QFY24. The

compressed schedule will likely challenge the program's ability to continue to identify anticipated discrepancies and implement fixes rapidly. The schedule will also stress the program's ability to analyze data and inform models and simulations for follow-on flight events.

The extended range and advanced capabilities of AARGM-ER exceed the capabilities of most test range infrastructures, as does the requirement to test against advanced target sets in threat-representative and contested, electromagnetic operational environments. As a result, range availability and suitability have been challenges for the program, resulting in test plan adjustments and scheduling delays. DT6 demonstrated some progress as cooperation between the Air Force's Nevada Test and Training Range and the Navy's China Lake Range enabled a cross-range-complex employment of AARGM-ER, shot from one range at a target set in the other range, through coordination with the Federal Aviation Administration, in the pursuit of threshold-distance shot employments to test the weapon.

The operational test program uses DT and IT events to collect data to verify and validate modeling and simulation. The data collection plan assumes that the current model will successfully predict performance in future test events. If this assumption proves incorrect, additional test events, including captive-carry events, may be required to complete verification, validation, and accreditation.

The Navy conducted its fifth and final AARGM-ER warhead arena ground test event in 4QFY23. DOT&E plans to observe select future test events and will report on the adequacy of warhead lethality, cyber survivability, and free flight testing once all event data has been received.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

The current data available are inadequate to provide a preliminary assessment of AARGM-ER operational effectiveness, lethality, suitability, or survivability. Additional testing and flight data are required from both F/A-18E/F and the EA-18G threshold platforms. Successful end-to-end functionality of all AARGM-ER-designed missile components, employed from the threshold range, has not yet been demonstrated.

RECOMMENDATIONS

The Navy should:

1. Demonstrate a successful end-to-end operational test of AAARGM-ER, by employing at or beyond the threshold range out to the objective range, demonstrate anti-radiation homing guidance, transition to MMW seeker target discrimination, and engage the designated threat with the newly designed warhead, in a threat representative environment.
2. Increase the completeness and adequacy of data availability for modeling and simulation by incorporating the EA-18G threshold platform for flight events, with an overall increase of captive carriage events, to better anticipate discrepancies before initial operational capability and assist during a compressed FY24 testing period.

Aegis Modernization Program

In FY23, the Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted operational testing on ships with the Capability Package (CP) 22-1 and Baseline 9.2.1 variants of the Aegis Weapon System (AWS) Advanced Capability Build 16 (ACB 16). Due to scheduling delays and correctable performance issues, the Navy now expects ACB 16 testing to continue until 1QFY25. DOT&E plans to deliver an early fielding report on ACB 16 CP 22-1 operational performance in 2QFY24 and a final ACB 16 OT&E report in FY25 after completion of operational testing. Operational testing continues to demonstrate hardware reliability and software stability concerns with the Aegis Display System and the AN/SPY-1 radar. As stated in the FY22 Annual Report, 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 airborne, surface, and subsurface threats. The Aegis Combat System's key components include: 1) an AWS that comprises the hardware and software modifications to integrate combat systems capabilities, as well as the AN/SPY-1 or AN/SPY-6(V)1 three-dimensional multi-function radar on Flight III *Arleigh Burke*-class (DDG 51) Aegis guided missile destroyers; 2) a Phalanx Close-In Weapon System; 3) a 5-inch diameter multipurpose gun system; 4) the Vertical Launch System that can launch Tomahawk missiles, SM-2, SM-3, and SM-6 Standard Missiles, Evolved Sea Sparrow Missiles (ESSM), and Vertical Launch Anti-Submarine Rockets; 5) AN/SPQ-9B Horizon Search Radar; 6) Surface Electronic Warfare Improvement Program (AN/SLQ-32(V)6); 6) Cooperative Engagement Capability; and 7) an AN/SQQ-89 undersea warfare suite, which also incorporates

integration with the MH-60R helicopter. The Navy's Aegis Modernization Program updates the AWS to improve Aegis Combat System integration and capabilities on *Ticonderoga*-class (CG 47) Aegis guided missile cruisers and *Arleigh Burke*-class (DDG 51) Aegis guided missile destroyers.

MISSION

The Joint Force Commander/ Strike Group Commander employs CG 47 ships and DDG 51 ships equipped with Aegis to conduct:

- Area and self-defense anti-air warfare in defense of the strike group;
- Anti-surface warfare;
- Anti-submarine warfare;
- Strike warfare, when armed with Tomahawk missiles;
- Integrated air and missile defense (IAMD); 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 a non-acquisition category program of record. The Navy updates the AWS through quadrennial ACBs that comprise hardware and software modifications to improve capability. The latest upgrade is ACB 16. The Navy intends four incremental deliveries within ACB 16: Baseline 9.2.0, Baseline 9.2.1, Baseline 9.2.2, and CP 22-1 (also referred to as Baseline 9.2.3). Each baseline update is intended to build on the previous baseline and improve capabilities through a combination of hardware and software upgrades. The Navy made the decision in FY23 that DDG 51 ships with Technology Insertion (TI16) hardware upgrades, that received, or were scheduled to receive, ACB 16 Baseline 9.2.2, will be upgraded to ACB 16 CP 22-1 to more efficiently resolve technical issues; however, some ships that are intended to be backfit with TI-12H may still receive Baseline 9.2.2 in the future. The evaluation of ACB 16 will be accomplished as a cumulative collection of operational test data from all baseline variants and is expected to complete by 1QFY25. ACB 16 evaluation informs deployment decisions and determines delivered capability for ACB 16 and its variants.

In coordination with DOT&E in FY19, the Navy developed an Aegis ACB 16 TEMP draft, which included the test strategy for the first three ACB 16 baselines, but the Navy did not provide it for DOT&E approval. The Navy subsequently updated the draft TEMP, in coordination with DOT&E, to incorporate CP 22-1. The TEMP is currently in Navy signature routing, but DOT&E has not yet received the TEMP for approval.

In 2QFY24, the Navy intends to begin initial operational testing of the next Aegis ACB, ACB 20, Baseline 10.0 variant in conjunction 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 IAMD. The Navy, in coordination with DOT&E, developed a single TEMP describing the testing strategy for ACB 20 (Baseline 10.0), and DDG 51 Flight III with the AN/ SPY-6(V)1. DOT&E approved the combined TEMP in September 2022. The Navy took delivery of the first DDG 51 Flight III guided missile destroyer with ACB 20 Baseline 10.0, USS *Jack H. Lucas* (DDG 125), in June 2023. The Navy should begin developing a follow-on TEMP update to address the next iteration of ACB 20 (Baseline 10.1 variant) capabilities that are not covered in the combined TEMP.

» MAJOR CONTRACTORS

- Lockheed Martin Rotary and Mission Systems – Moorestown, New Jersey
- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Tucson, Arizona
- Bath Iron Works, a subsidiary of General Dynamics Corporation – Bath, Maine
- HII (formerly Huntington Ingalls Industries) – Pascagoula, Mississippi

TEST ADEQUACY

No testing of AWS ACB 16 Baseline 9.2.0 occurred in FY23. OPTEVFOR conducted operational testing of AWS ACB 16 Baseline 9.2.1 on USS *Gettysburg* (CG 64) from August to September 2023 in

accordance with a DOT&E-approve test plan and with observation by DOT&E. Tests consisted of tracking exercises with simulated engagements against manned aircraft, and live fire and tracking exercises against fast inshore attack craft surrogates.

OPTEVFOR conducted additional operational testing of ACB 16 CP 22-1 on USS *McCampbell* (DDG 85) in November 2022, on USS *Lena Sutcliffe Higbee* (DDG 123) in July 2023, and on USS *Preble* (DDG 88) in August 2023. Tests included live missile firings and tracking exercises against anti-ship cruise missile surrogates, tracking exercises with simulated engagements against manned aircraft, live fire against an unmanned aerial vehicle, and live fire and tracking exercises against fast inshore attack craft surrogates. Live missile firings included SM-2 Block IIIA, SM-2 Block IIIB, and ESSM firings. Due to a hardware failure on DDG 88, only suitability data were collected during that operational test period. OPTEVFOR conducted all tests in accordance with DOT&E-approved test plans and with observation by DOT&E.

The Navy is developing the Combat System Test Bed (CSTB) modeling and simulation suite to support the test strategy in the combined TEMP for ACB 20 (Baseline 10.0), DDG 51 Flight III, and the AMDR IOT&Es. The Navy intends to trial the use of the CSTB within the evaluation of Aegis ACB 16 to supplement live testing of the air warfare mission. CSTB is likely to inform attributes of the air warfare mission but limitations of the CSTB in the ACB 16 configuration preclude an end-to-end assessment of self-defense capability as defined by the ACB 16 Probability of Raid Annihilation requirements. To support this, OPTEVFOR developed a CSTB accreditation plan in FY23 for the assessment of ACB 20 (Baseline 10.0). The Navy is developing the CSTB in incremental stages that align with planned operational testing. However, the Navy does not expect to accredit the CSTB for evaluation of all mission areas until FY27. The Navy should continue development of the CSTB to support current and future AWS baseline testing.

OPTEVFOR plans to continue ACB 16 testing on Baselines 9.2.0, 9.2.1, and CP 22-1 in FY24, and plans cyber survivability testing of ACB 16 CP 22-1 on a DDG 51 ship in April and May 2024. All ACB 16 testing is expected to be completed by 1QFY25. The Navy should ensure that all remaining test assets are scheduled to support completion of ACB 16 testing.

OPTEVFOR is developing a test plan for operational testing of DDG 51 Flight III, Aegis ACB 20 (Baseline 10.0), and AN/SPY-6(V)1 on USS *Jack H. Lucas* (DDG 125) that is planned for 2QFY24.

PERFORMANCE

» EFFECTIVENESS

Not enough data are yet available to determine Aegis ACB 16 operational effectiveness as operational test remains in progress. DOT&E did not submit an early fielding report for ACB 16 Baseline 9.2.2 and ACB 16 CP 22-1 as intended in the FY22 Annual Report. This reporting is delayed until completion of operational testing of CP 22-1 due to delayed fielding caused by the program's intended correction of deficiencies identified in CP 22-1 testing, and the transition of ships from Baseline 9.2.2 to CP 22-1. DOT&E now intends to submit an early fielding report for Aegis ACB 16 in 2QFY24. DOT&E expects to submit a final Aegis ACB 16 OT&E report in 2QFY25 after completion of remaining operational tests.

The AWS integration with active missiles including ESSM Block 2, SM-2 Block IIIC, and SM-6, which are intended for close-in air warfare self-defense and area-air defense, have the potential to improve overall performance of the weapon system. Details are available in the classified early fielding report for ESSM Block 2 utilizing AWS ACB 16 Baseline 9.2.2 of September 2022. DOT&E additionally expects to release a Standard Missile 2 Block IIIC early fielding report, for testing conducted on an ACB 16 CP 22-1 platform, in 2QFY24.

» SUITABILITY

Not enough data are yet available to determine Aegis ACB 16 operational suitability as operational test remains in progress. However, testing continues to demonstrate hardware reliability and software

stability concerns with the Aegis Display System and the AN/SPY-1 radar. Problems with the AN/SPY-1 radar prevented the Navy from completing an operational test event planned for USS *Preble* in August 2023.

» SURVIVABILITY

Not enough data are available to assess the cyber survivability of ACB 16. The Navy plans to complete cyber survivability assessment of CP 22-1 in 3QFY24.

RECOMMENDATIONS

The Navy should:

1. As recommended in the FY22 Annual Report, submit the ACB 16 TEMP for DOT&E approval as soon as feasible to support allocation of necessary test resources.
2. Determine and correct the cause of hardware reliability and software stability problems with the Aegis Display System and AN/SPY-1 radar, as recommended in the FY22 Annual Report.
3. Continue to determine and correct causes of performance deficiencies identified during CP 22-1 testing that have prevented the ability to conduct some operational test events and may have also impacted test results.
4. Continue development, verification, and validation of the CSTB to support its intended use in each AWS baseline's test program.
5. Schedule remaining test assets to support completion of the ACB 16 test program, including the cyber survivability assessment of CP 22-1.
6. Develop the TEMP update for evaluation of ACB 20 (Baseline 10.1) capabilities not in the combined ACB 20 (Baseline 10.0), DDG 51 Flight III, and AN/SPY-6(V)1 TEMP.

AIM-9X Block II Sidewinder

The AIM-9X Block II is in the process of several hardware (HW) and software (SW) changes. Planning for operational testing is underway for an updated Operational Flight Software (OFS) that includes performance improvements and addresses a previous deficiency. Test planning for a new AIM-9X Block II HW configuration is in process as well. The new HW will be tested with a re-host of the current, fleet-released OFS 9.411 for quick fielding. Future OFS improvements are planned to capitalize on these HW performance upgrades.

SYSTEM DESCRIPTION

AIM-9X Block II is the latest-generation, infrared, short-range, air-intercept missile designed to detect, acquire, intercept, and destroy a wide range of airborne threats. It is day and night capable, uses a passive infrared seeker, and is capable of large attack angles against a wide variety of enemy aircraft. The designated threshold platforms are the F-18C/D/E/F and the F-15C/D. Current and future integration efforts also include the F/A-18A/B, E/A-18G, F-15E/EX, F-16C/D, F-22, F-35A/B/C, MQ-9, AV-8B, and AH-1Z.

MISSION

AIM-9X Block II is utilized by the U.S. Navy, Marine Corps, and Air Force, as well as several foreign military forces, to execute short-range offensive and defensive air-to-air combat missions. AIM-9X Block II is also a primary element of the Integrated Air and Missile Defense and Theater Air and Missile Defense Family of Systems.

PROGRAM

AIM-9X Block II is an Acquisition Category IC program. It is a joint program led by the Navy's Air-to-Air Missiles Program Office (PMA-259). The Services are in the process of operational test planning for AIM-9X Block II SW updates and HW obsolescence updates. Operational testing on these upgrades is planned to begin in 2QFY24.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Tucson, Arizona

TEST ADEQUACY

The Navy completed FOT&E of the AIM-9X Block II OFS 9.410 in January 2021. OFS 9.411 is the current fielded version, but OFS 9.410 is functionally the same software with the same missile capabilities. Testing was accomplished in accordance with the DOT&E-approved test plan and DOT&E personnel observed the testing. Testing was adequate to demonstrate the operational effectiveness and suitability of the missile. DOT&E published an AIM-9X Block II OFS 9.410 FOT&E report in September 2021 with the intention of releasing a combined lethality and survivability annex in 2022. The annex was delayed so that the Navy could accredit the cyber test asset. The accreditation letter and report annex are expected to be complete in 2QFY24. Test planning documents, including the Test and Evaluation Master Plan and test plans, for upcoming operational tests still need to be submitted to DOT&E for review and approval.

PERFORMANCE

» EFFECTIVENESS

DOT&E assessed the AIM-9X Block II as operationally effective in an FOT&E report completed in September 2021. AIM-9X remains on oversight and DOT&E will continue to evaluate operational effectiveness in upcoming operational testing beginning in 2QFY24.

» SUITABILITY

DOT&E assessed AIM-9X Block II as suitable in an FOT&E completed in January 2021. AIM-9X remains on oversight and DOT&E will continue to evaluate its operational suitability in an upcoming operational testing beginning in 2QFY24.

» LETHALITY AND SURVIVABILITY

AIM-9X Block II's lethality and cyber survivability evaluation is pending cyber test asset accreditation by the Navy. Details will be available in a published DOT&E classified annex to the September 2021 FOT&E report, expected in 2QFY24.

RECOMMENDATIONS

The Navy should:

1. Submit a Test and Evaluation Master Plan and test plans for upcoming operational testing to DOT&E in accordance with DoD Instruction 5000.89 timelines.
2. Submit an accreditation letter for the cyber survivability test asset to DOT&E.

Air and Missile Defense Radar (AMDR) / AN/SPY-6

In FY23, the Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted an operational assessment (OA) of the Air and Missile Defense Radar (AMDR), designated AN/SPY-6(V)1, to provide early evaluation of the radar's performance and enable modifications that can optimize performance at IOT&E. DOT&E expects to deliver a classified AMDR OA report in 2QFY24 upon completion of data analysis. OPTEVFOR plans IOT&E of AMDR, designated AN/SPY-6(V)1, between FY24 and FY27.

SYSTEM DESCRIPTION

AN/SPY-6 is the Navy's next-generation, AMDR S-Band, family of radars. AN/SPY-6 uses a radar modular assembly (RMA) as a building block for the radar's antenna. Each individual RMA is a self-contained radar antenna built from a set of active transmit/receive (T/R) digital modules that are electronically scanned. Each RMA block can integrate with other RMA blocks to create antenna assemblies of various size and capability. The large

number of T/R modules provides a high degree of fault tolerance through antenna redundancy and graceful degradation.

AMDR fielded on DDG 51 Flight III *Arleigh Burke*-class guided missile destroyers is designated AN/SPY-6(V)1. AN/SPY-6(V)1 uses four, fixed-antenna assemblies (faces) with each antenna having 37 RMAs. This provides a 360-degree field-of-view about the ship. AN/SPY-6(V)1 integrates with Aegis Weapon System (AWS) to provide DDG 51 Flight III ships with enhanced surveillance, tracking, and ballistic missile defense (BMD) discrimination. AN/SPY-6(V)1 is designed to operate in high clutter, littoral regions near land, and electromagnetic congested, contested, and complex environments.

AN/SPY-6 family of radars has other variants such as:

- AN/SPY-6(V)2 is comprised of nine RMAs for the single-face rotating antenna intended for the next flights of the *San Antonio*- and *America*-class amphibious ships and as a back-fit to the *Nimitz*-class aircraft carriers.
- AN/SPY-6(V)3 is comprised of three fixed-antenna faces with nine RMAs on each antenna face, intended for the *Gerald R. Ford*-class aircraft carrier and a modified version intended for the *Constellation*-class frigates.
- AN/SPY-6(V)4 is a planned back-fit modernization to the DDG 51 Flight IIA ships that will use 4 fixed-antenna faces, with each antenna face having 24 RMAs.

MISSION

Navy commanders will use AMDR to detect, track, and support engagements against cruise and ballistic missiles, aircraft, and unmanned aerial vehicles in support of air warfare (AW) missions, BMD, or concurrent AW and BMD known as integrated air and missile defense (IAMD). Commanders additionally use AMDR for contact localization and situational awareness in surface warfare missions. AN/SPY-6(V)4 is expected to support similar missions as AN/SPY-6(V)1. AN/SPY-6(V)2 and AN/SPY-6(V)3 will also support similar missions, except for BMD and IAMD.

PROGRAM

AN/SPY-6 is an Acquisition Category IC program. DOT&E approved a combined Test and Evaluation Master Plan (TEMP) describing the testing strategy for AN/SPY-6(V)1, DDG 51 Flight III, and AWS Baseline 10 in September 2022. OPTEVFOR plans to conduct AN/SPY-6(V)1 IOT&E in FY24 with completion in FY27 in conjunction with the OT&E of DDG 51 Flight III with AWS Baseline 10. In June 2022, the Navy accepted delivery of the lead ship USS *Jack H. Lucas* (DDG 125) and has conducted various sea trials with AMDR as part of developmental testing.

The Navy expects to deliver a combined TEMP in FY24 that supports test and evaluation of AN/SPY-6(V)2, AN/SPY-6(V)3, and the Ship Self-Defense System Baseline 12 Combat System. The Navy intends to conduct IOT&E of AN/SPY-6(V)2 and AN/SPY-6(V)3 radars between FY25 and FY28.

The AMDR program intends to cover AN/SPY-6(V)4 testing in a future Aegis Modernization TEMP.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Marlborough, Massachusetts

TEST ADEQUACY

In December 2022, OPTEVFOR conducted an OA of AN/SPY-6(V)1 at the Advanced Radar Detection Laboratory (ARDEL) on Pacific Missile Range Facility, in Kauai, Hawaii. The OA evaluated capability of AN/SPY-6(V1) to detect and track fighter aircraft, anti-ship cruise missile surrogates, unmanned aerial vehicles, helicopters, airborne early warning and control aircraft, and small-boat targets. Test events were executed in both clear and electromagnetic-contested environments and included projection from tower-based simulators. OPTEVFOR conducted the OA in accordance with a DOT&E-approved test plan with observation by DOT&E.

The OA provides early evaluation of the AN/SPY-6(V)1 radar performance and identifies modifications that can optimize performance at system employment. The OA additionally

informs planning of IOT&E campaign test events. The OA was not intended to determine operational effectiveness and suitability of the delivered AMDR due to the AN/SPY-6(V)1 at ARDEL being an engineering development model (EDM) that uses obsolete T/R Integrated Microwave Modules from that of the delivered system and not enough test data are available on the delivered AMDR. The AMDR program did not evaluate cyber survivability due to differences that the delivered AMDR will have from the AMDR EDM version at ARDEL. DOT&E expects to deliver a classified AN/SPY-6(V)1 OA report in 2QFY24 upon completion of data analysis.

Assessment of the resident AN/SPY-6(V)1 at ARDEL is limited by the following:

- The AN/SPY-6(V)1 is an EDM version that is in a degraded state and requires upgrade to provide representative performance. The AN/SPY-6(V)1 was adequate to support OA objectives but will not be adequate for IOT&E. The AMDR program plans to address within POM 25 adjustments to their program budget.
- The current aerial anti-ship cruise missile targets do not emulate more stressing threats, including advanced electronic attack capabilities. Aerial targets are needed to demonstrate performance and validate the modeling and simulation for IOT&E.
- The operational test strategy within the AN/SPY-6(V)1, DDG 51 Flight III, and AWS Baseline 10 TEMP that supports IOT&E for all three programs depends upon using the AN/SPY-6(V)1 at ARDEL to evaluate some specific capabilities which cannot be tested in an at-sea environment. However, the OA did not fully demonstrate the intended method of test, for this specific test objective, due to the system setup and software configuration issues.

PERFORMANCE

» EFFECTIVENESS

The AMDR OA demonstrated radar performance in a limited set of scenarios. DOT&E expects to provide performance results and risks to IOT&E in a classified AMDR OA report in 2QFY24. DOT&E expects to report operational effectiveness of AMDR in a classified IOT&E report in FY28 after IOT&E.

» SUITABILITY AND SURVIVABILITY

Suitability and survivability were not assessed as part of the AMDR OA due to the expected differences between the AMDR EDM and the delivered AMDR. DOT&E expects to report operational suitability and survivability of AMDR in a classified IOT&E report in FY28 after IOT&E.

RECOMMENDATIONS

The Navy should:

1. Replace the AN/SPY-6(V)1 EDM version at ARDEL with a production representative system to support AMDR IOT&E.
2. Update aerial anti-ship cruise missile targets to better emulate more stressing threats, including advanced electronic attack, and support AMDR IOT&E.
3. Validate the method of test used during the AMDR OA at ARDEL for assessing specific AN/SPY-6(V)1 capabilities which cannot be tested in an at-sea environment during IOT&E.
4. Continue to develop and submit the combined AN/SPY-6(V)2, AN/SPY-6(V)3, and the Ship Self-Defense System Baseline 12 Combat System TEMP for DOT&E approval in FY24.

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

In May 2023, the Navy declared initial operational capability of the AN/AQS-20C, referred to as "Minehunt," as deployed from the Mine Countermeasures (MCM) Unmanned Surface Vehicle (USV). The Navy intends to complete IOT&E of MCM USV and Minehunt in FY24 upon completion of its cyber survivability evaluation. DOT&E will report operational effectiveness, suitability, and cyber survivability after completion of IOT&E.

SYSTEM DESCRIPTION

AN/AQS-20C projects acoustic energy (i.e., active sonar) and records returning acoustic energy from its surrounding environment. The AN/AQS-20C is powered by and towed from the MCM USV. This combination, or MCM USV and Minehunt, deploys from the littoral combat ship (LCS) as a component of the MCM Mission Package (MP) or can deploy independently from ashore.

A remote USV operator uses MCM USV and Minehunt to search along pre-planned tracks using a radar and camera surveillance suite to redirect the MCM USV and Minehunt if needed to avoid obstacles and other watercraft. The system also provides sensor status and sonar information to a remote payload operator. Operators can analyze recorded data from the MCM USV and Minehunt after its return to the LCS, or shore, to identify and localize potential mines. Sailors can also configure the MCM USV to tow a mine sweep payload, and in that configuration the system is called the Unmanned Influence Sweep System.

MISSION

Commanders will deploy MCM USV and Minehunt from the LCS, or ashore, to identify and localize moored and bottom mines in sea lanes, straits, choke points, fleet operating areas, and amphibious objective areas. Other systems are then used to neutralize existing mines. The Navy intends for the LCS MCM MP with the MCM USV and Minehunt to replace the functionality provided by the *Avenger*-class MCM ships and MH-53E Sea Dragon MCM helicopters.

PROGRAM

MCM USV and Minehunt is an Acquisition Category II program. The Navy declared initial operational capability of MCM USV in April 2022 and Minehunt in March 2023. DOT&E approved an update to the MCM USV and Minehunt Test and Evaluation Master Plan (TEMP) in January 2023. The cyber survivability test of MCM USV and Minehunt will be conducted in conjunction with the LCS MCM MP testing and will be resourced in the LCS TEMP.

» MAJOR CONTRACTORS

- Textron Systems – Hunt Valley, Maryland
- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Arlington, Virginia
- Bollinger Shipyards – Lockport, Louisiana

TEST ADEQUACY

The Navy conducted several IOT&E events in August and September 2022 which included LCS-based and shore-based functionality testing. The LCS-based testing was conducted in conjunction with the LCS MCM MP IOT&E and observed by DOT&E. Some test events were inconsistent with the DOT&E-approved test plan and required added test. The remaining IOT&E event, the cyber survivability evaluation of the MCM USV and Minehunt, is scheduled to be conducted in 3QFY24 to complete IOT&E.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

DOT&E will provide a classified IOT&E report that details operational effectiveness and suitability in FY24 after completion of IOT&E.

» SURVIVABILITY

Insufficient data are available to determine cyber survivability of MCM USV and Minehunt. DOT&E will provide a classified IOT&E report that details cyber survivability after completion of the required cyber survivability test of MCM USV and Minehunt in FY24.

RECOMMENDATIONS

The Navy should:

1. Identify and correct all observed AN/AQS-20C software failures from operational test and then conduct FOT&E of MCM USV and Minehunt under operationally representative conditions.
2. Complete IOT&E in accordance with the DOT&E-approved test plan.

CH-53K® King Stallion®

The Navy approved the CH-53K for full-rate production (FRP) in December 2022. Earlier that month, DOT&E published a combined IOT&E and LFT&E report of CH-53K's operational effectiveness, suitability, and survivability to inform the FRP decision. The CH-53K is operationally effective when transporting external cargo, troops, and lightweight pallets. There are several deficiencies with heavy payload delivery and crew-vehicle interface that should be corrected. The CH-53K is not operationally suitable because of low aircraft availability. Phase II LFT&E has yet to be resourced, planned, and scheduled. The Navy is updating the Test and Evaluation Master Plan (TEMP) and developing test plans in order to conduct FOT&E in FY24. CH-53K® and King Stallion® are registered trademarks of the Department of the Navy.

SYSTEM DESCRIPTION

The CH-53K is a three-engine, dual-piloted, heavy lift helicopter intended to replace the aging CH-53E helicopter. The CH-53K mission payload external load transport is more than twice the CH-53E capability. The triple hook system is designed to transport independent external loads, which allows for three different location drops per sortie. Another major improvement is the replacement of mechanically actuated flight controls with a fly-by-wire system.

CH-53K is equipped with aircraft survivability equipment designed to provide self-defense capability against ground-to-air and air-to-air missile threats. This suite consists of the Department of Navy Large Aircraft Infrared Countermeasures system with advanced threat warning sensors, radar warning receiver, and countermeasure dispensing system.

The Marine Corps will support CH-53K Organizational-Level (O-level), Intermediate-Level (I-level), and Depot-Level (D-level) maintenance concepts. The number of personnel per squadron required to maintain the CH-53K is expected to remain the same as for the CH-53E.

MISSION

Units equipped with the CH-53K aircraft provide the Marine Air-Ground Task Force with assault support to include maritime special operations, by transporting heavy equipment, armored vehicles, combat troops, and supplies from ships to inland locations under all weather conditions. Secondary CH-53K missions include tactical recovery of aircraft and personnel, helicopter air-to-air refueling, air evacuation, aerial delivered ground refueling, forward arming and refueling point operations, air delivery, and rapid insertion and extraction operations.

PROGRAM

The CH-53K is an Acquisition Category IC program. The program of record stipulates the procurement of 200 aircraft. The program completed IOT&E in April 2022 in accordance with a DOT&E-approved test plan. DOT&E provided a combined IOT&E and LFT&E report in December 2022, in support of the FRP decision, which the Navy approved later that month.

The CH-53K Program Office (PMA-261) is updating the TEMP in support of two phases of FOT&E. The first FOT&E phase consists of two integrated test (IT) periods and an operational test period. The two IT periods were conducted in FY23 to collect data for secondary missions and updated aircraft survivability equipment. The operational test period, which will complete the first FOT&E phase, is scheduled for FY24 and will assess the operational effectiveness, suitability, and cyber survivability of the aircraft's survivability equipment and the Digital Interoperability system, and verify the correction of deficiencies observed during IOT&E. The Navy will submit an operational test plan for DOT&E's approval, and DOT&E will publish an FOT&E report after testing is complete. Initial planning has started for the second phase of FOT&E but is yet to be scheduled.

Phase II LFT&E has yet to be resourced, planned, and scheduled. DOT&E has been reporting since FY20 that the Navy has yet to fund the Phase II LFT&E in accordance with the DOT&E-approved TEMP.

» MAJOR CONTRACTOR

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

TEST ADEQUACY

As reported in last year's Annual Report, IOT&E was adequate to support the evaluation of operational effectiveness, operational suitability, and cyber survivability. IOT&E was not adequate to characterize aircraft survivability equipment performance. In last year's report, DOT&E recommended a retest of aircraft survivability equipment. The Navy intends to conduct this test in FY24 with a DOT&E-approved test design. The results will be included in a DOT&E FOT&E report in FY24.

The Marine Operational Test and Evaluation Squadron (VMX-1), under the auspices of the Navy Operational Test and Evaluation Force, conducted two FY23 IT events, both in accordance with DOT&E-approved test plans and observed by DOT&E. The first event was conducted from October 2022

through July 2023, collecting IT data on low-rate initial production Lot 2 aircraft to evaluate CH-53K's ability to conduct its secondary missions. VMX-1 conducted the second IT event from May through August 2023, collecting data on a new version of aircraft survivability equipment installed in an engineering development model aircraft.

PERFORMANCE

» EFFECTIVENESS

In the December 2022 IOT&E report, DOT&E determined that the CH-53K is operationally effective when transporting external cargo, troops, and lightweight pallets. The aircraft demonstrated it exceeds the external load and range performance requirement. The CH-53K is not effective for internal heavy payload delivery or the transport of standard Air Mobility Command 463L pallets because the cargo rollers and portable electric winch deficiencies increase the time required to load heavier pallets into the cabin. Interface deficiencies prevented effective data transfer between the Joint Mission Planning System and the aircraft's mission computer, which increased pilot workload and could hamper mission execution.

» SUITABILITY

In the December 2022 IOT&E report, DOT&E determined that the CH-53K is not operationally suitable. The aircraft demonstrated acceptable results for all reliability and maintainability metrics. However, the demonstrated low aircraft availability does not support sustained operations. Additionally, the low probability of success of the automatic blade fold system will result in mission aborts and extended deck cycles that could hamper amphibious operations. The aircraft demonstrated its sortie generation rate requirement. Unexpected main and tail rotor blade erosion damage was observed on aircraft operating in the desert environment during IOT&E. Extended time was needed to repair blade erosion damage because of the lack of a structural repair manual. Battle damage assessment and repair also requires a structural repair manual that has yet to be delivered.

» SURVIVABILITY

The lack of a structural repair manual for battle damage assessment and repair negatively impacts survivability. The classified annex to the DOT&E combined IOT&E and LFT&E report contains a detailed cyber survivability assessment.

RECOMMENDATIONS

The Navy should:

1. Fund and complete the planned Phase II LFT&E program in accordance with the DOT&E-approved TEMP.
2. Improve internal cargo and 463L pallet loading capability.
3. Improve automatic blade fold system reliability to make CH-53K suitable for amphibious operations.
4. Improve the design of the leading edge and tip caps of the main and tail rotor blades to increase component life when operating in all desert environments.
5. Continue to develop the structural repair manual to facilitate organizational-level repairs.
6. As recommended in the FY22 Annual Report, conduct aircraft survivability equipment operational testing prior to fielding to characterize aircraft susceptibility to threat weapon systems.
7. Conduct additional cyber survivability testing to fully characterize cyber threats.
8. Investigate and correct the integration deficiencies between the Joint Mission Planning System and the aircraft's mission computer that could prevent successful mission execution.
9. Continue to address recommendations found in DOT&E's combined IOT&E and LFT&E report, to include the survivability recommendations from the classified annex.

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

The CMV-22B achieved initial operational capability (IOC) in December 2021. In FY22, DOT&E reported that full operational capability was expected in FY23, but now the Navy is expecting it in FY24. The Navy started a second period of FOT&E in December 2022 to evaluate the operational effectiveness, suitability, and cyber survivability of the CMV-22B aircraft equipped with the Communications Upgrade suite. Testing is scheduled to complete in 1QFY24. FOT&E data analyses are ongoing, precluding an assessment in this article. DOT&E will publish a combined FOT&E and LFT&E report in 2QFY24.

SYSTEM DESCRIPTION

The CMV-22B Osprey is a tiltrotor vertical/short takeoff and landing aircraft that can take off and land as a helicopter, and transit as a turboprop aircraft. The Navy intends the CMV-22B to replace the in-service C-2A Greyhound carrier onboard delivery (COD) aircraft. The CMV-22B is based on the MV-22B design with several changes to support the COD mission: increased fuel capacity to extend the range, fuel jettison system, integrated public address system for making announcements in the cabin area, high-frequency radio for over-the-horizon communications, and cabin and cargo lighting to assist with cargo loading.

The Communications Upgrade suite includes a Link-16 tactical datalink and an Iridium satellite phone to enhance capabilities when conducting logistics, search and rescue, and mobility missions as part of a Carrier Strike Group. Link-16 provides secure communications and a common operational picture for the network's participants by exchanging their location information. The Iridium Sat phone enables over-the-horizon communications and acts as a backup for the high-frequency radio.

MISSION

The Navy will employ units equipped with CMV-22Bs to perform the COD mission of transport of personnel, mail, and cargo from forward logistics sites to aircraft carriers at sea. A detachment of three aircraft will support a Carrier Strike Group. The CMV-22B also has a mobility mission by which the aircraft can self-deploy into theater, whereas the COD mission and other missions can be conducted in support of the Carrier Strike Group. The CMV-22B must be capable of conducting operations in a permissive threat environment, day/night, and in all weather conditions. Secondary missions include vertical onboard delivery, vertical replenishment, medical evacuation, Naval Special Warfare support, missions of state, and search and rescue support.

PROGRAM

The CMV-22B, as part of the overall V-22 program of record, is an Acquisition Category IC program. The Navy procured a total of 48 CMV-22B variants. 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 plans to declare full operational capability in FY24 rather than FY23 as DOT&E reported last year. DOT&E approved the CMV-22B Test and Evaluation Master Plan and the Alternative LFT&E plan in March 2020. DOT&E published a combined FOT&E and LFT&E report in June 2022, and approved an FOT&E OT-D2 test plan in November 2022. DOT&E also approved a cyber survivability test plan in March 2023.

» MAJOR CONTRACTOR

- Bell-Boeing Joint Project Office – Amarillo, Texas

TEST ADEQUACY

Air Test and Evaluation Squadron 1 (VX-1), under the auspices of the Navy's Operational Test and Evaluation Force (OPTEVFOR), is conducting a second period of FOT&E, called OT-D2, that started in December 2022. This FOT&E is designed to assess the operational effectiveness, suitability, and cyber survivability of the Communications Upgrade suite, assess training, and verify the corrections of deficiencies discovered during the first period of FOT&E in 2021. DOT&E will report the results in the combined FOT&E and LFT&E report in FY24.

OPTEVFOR conducted a cyber cooperative vulnerability and penetration assessment and an adversarial assessment of the Communications Upgrade suite installed on a production-representative engineering development model CMV-22B aircraft at Naval Air Station Patuxent River, Maryland in March 2023. DOT&E approved the cyber survivability test plan in March 2023. OPTEVFOR executed the objectives outlined in that plan but discovered an unplanned test limitation. DOT&E observed those events and determined it was executed in accordance with the test plan. DOT&E will report the results of this test in the combined FOT&E and LFT&E report in FY24.

NAVAIR provided the final fuel system aircraft survivability test data and analysis in August 2023; DOT&E will report the adequacy and results of CMV-22B survivability in the combined FOT&E and LFT&E report in FY24.

PERFORMANCE

» EFFECTIVENESS

Assessment of the CMV-22B Communications Upgrade is pending the completion of data analysis from FOT&E tests and will be included in the 2QFY24 DOT&E combined FOT&E and LFT&E report.

» SUITABILITY

As reported in the combined FOT&E and LFT&E report of June 2022, DOT&E found that CMV-22B was not operationally suitable due to failures of many subsystems, with the ice protection system accounting for 44 percent of the total operational mission failures. Additionally, the maintenance hours per flight hour (MH/FH) did not meet the requirement, with 45 percent of the total MH/FH attributed to special inspections and scheduled maintenance requirements. Analysis is ongoing on the data collected in the second FOT&E for reassessing these metrics. An assessment of operational suitability, to include suitability of the Communications Upgrade suite and training using the Containerized Flight Training Device and the Virtual Maintenance Trainer, will be included in the 2QFY24 DOT&E combined FOT&E and LFT&E report.

» SURVIVABILITY

Data analysis is ongoing to evaluate the CMV-22B survivability in a cyber-contested environment. LFT&E and the cyber survivability assessment will be included in the 2QFY24 DOT&E combined FOT&E and LFT&E report.

RECOMMENDATION

The Navy should:

1. Continue to implement the recommendations in DOT&E's June 2022 combined FOT&E and LFT&E report.

Consolidated Afloat Networks and Enterprise Services (CANES)

Previous testing ending in 2017 demonstrated the Consolidated Afloat Networks and Enterprise Services (CANES) to be operationally effective and suitable for surface ships, and survivable for smaller ships such as cruisers and destroyers, but not for larger ships such as aircraft carriers and large-deck amphibious ships. The Navy Operational Test and Evaluation Force (OPTEVFOR) and the program office worked with the fleet to find a test submarine for the CANES submarine variant. Their combined effort resulted in conducting a useful cyber survivability test. The Navy is continuing to look for a submarine to finish the FOT&E of the CANES submarine variant.

SYSTEM DESCRIPTION

CANES is an enterprise information system consisting of computing hardware, software, and network services (i.e., phone, email, chat, video teleconferencing, web hosting, file transfer, computational resources, storage, and network configuration and monitoring).

The CANES network provides a single, consolidated physical network with logical sub-networks for Unclassified, Secret, Secret Releasable, and Top Secret security domains. It includes a cross-domain solution for information transfers across these security boundaries. This consolidation reduces the network infrastructure footprint on naval platforms and the associated logistics, sustainment, and training costs.

CANES has three variants tailored to the employing platform: unit-level for smaller ships such as destroyers and cruisers, force-level for large deck ships such as aircraft carriers and large deck amphibious ships, and a submarine variant.

MISSION

Navy shipboard users use CANES to:

- Host their applications on computing resources and network services in support of naval and joint operations.
- Support weapon systems, command and control, intelligence, and business information applications.
- Communicate via chat, email, voice, and video.

PROGRAM

In a July 2015 IOT&E report, DOT&E evaluated CANES for unit-level ships to be operationally effective, suitable, and survivable. The USD(AT&L) (restructured in 2018 into USD(A&S) and USD(R&E)) approved full deployment of CANES in October 2015. The full deployment acquisition decision memorandum delegated milestone decision authority to the Secretary of Navy, and designated CANES an Acquisition Category IAC program. The Navy tested unit-level and force-level ships in accordance with DOT&E-approved test plans, both in 2015. The Navy initially expected an FOT&E of the submarine variant during 2019, but the test was cancelled and rescheduled multiple times because the submarines designated for testing had to be deployed to support operational requirements.

» MAJOR CONTRACTORS

- BAE Systems, Inc. – Rockville, Maryland
- DRS Laurel Technologies – Johnstown, Pennsylvania
- Global Technical Systems – Virginia Beach, Virginia
- L3Harris Technologies, Inc. – Camden, New Jersey
- Leidos – Reston, Virginia
- Peraton, Inc. – Herndon, Virginia
- Serco – Herndon, Virginia
- Milcom – Virginia Beach, Virginia

TEST ADEQUACY

In early 2QFY23, a *Los Angeles*-class submarine became available when an unscheduled 10-day availability window occurred. Because of the small availability window, OPTEVFOR recommended focusing on cyber survivability testing rather than a full operational test, since the submarine variant of CANES had performed well in prior developmental tests and CANES has been used effectively on surface ships and submarines for many years. DOT&E approved the cyber survivability test plan in January 2023.

OPTEVFOR conducted and DOT&E observed the CANES cooperative vulnerability and penetration assessment (CVPA) and adversarial assessment (AA) in January and February 2023. Given the shortened test window, the cyber test team and DOT&E agreed that the Top Secret/Sensitive Compartmented Information (TS/SCI) enclave should take priority, because the TS/SCI enclave had not been tested in prior CANES cyber survivability tests.

However, while preparing for the cyber test, the test team learned that submariners do not use CANES for TS/SCI traffic. Instead, crews use carry-on temporary equipment (Lime Rock) to access

SCI traffic. When OPTEVFOR found out, they recommended still continuing with the test as planned, because the TS/SCI enclave was not tested in previous CANES testing of any variant and the force-level ships do use the CANES TS/SCI enclave. DOT&E agreed with the recommendation.

In preparation for when a submarine will become available, the Navy prepared an FOT&E test plan, which DOT&E approved in May 2023.

PERFORMANCE

» EFFECTIVENESS

The CANES submarine variant was not tested for operational effectiveness, but CANES for both the unit-level and force-level versions were previously found to be operationally effective. Additionally, Application Integration System Integration Test events for systems hosted on CANES have consistently showed that CANES provides effective network services.

» SUITABILITY

The CANES submarine variant was not tested for operational suitability, but CANES for both the unit-level and the force-level versions were previously found to be operationally suitable.

» SURVIVABILITY

While the execution of the CVPA and AA events were not sufficient for a comprehensive evaluation due to limited platform availability, the tests identified several vulnerabilities that need to be mitigated. When the Navy identifies a test submarine for FOT&E, OPTEVFOR should conduct an FOT&E that includes an adequate CVPA and AA.

RECOMMENDATIONS

The Navy should:

1. Fix the vulnerabilities discovered during the CVPA and AA as reported by the OPTEVFOR in March 2023.
2. Identify a test submarine to complete the FOT&E.

Conventional Prompt Strike (CPS)

Flight testing by the Navy and Army of the Conventional Prompt Strike (CPS) prototype All-Up Round (AUR) continued in March 2023. This test, Joint Flight Campaign-2 (JFC-2), was an intended launch from the Army's Long Range Hypersonic Weapon (LRHW) prototype transporter-erector-launcher (TEL). The test did not occur because failed pre-flight checks prevented the launch. The Navy and Army reattempted JFC-2 in September 2023 but again could not launch the AUR due to failed pre-flight checks. The Navy and Army intend to reattempt JFC-2 and conduct JFC-3 in FY24, with both being LRHW TEL launches.

SYSTEM DESCRIPTION

CPS is a conventional, boost-glide hypersonic weapon system. The CPS AUR missile includes a two-stage solid rocket motor booster and a Common Hypersonic Glide Body containing a kinetic energy projectile warhead. The Navy will integrate CPS into both *Zumwalt*-class destroyers and *Virginia*-class submarines. The Navy will utilize cold-gas ejection ("cold launch") to launch the AUR from both platforms. The Army LRHW system, which is being reported on in a separate article, will fire a common AUR from their TEL, igniting it in the launch canister ("hot launch").

MISSION

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

PROGRAM

The Navy is employing a three-phase acquisition strategy to deliver CPS. Phase 1 is a Middle Tier of Acquisition (MTA) rapid prototyping effort to develop and demonstrate a prototype hypersonic missile system capability through a five-flight test campaign ending with JFC-5 in FY24. Phase 2 is an MTA rapid fielding effort. The Navy intends to begin the rapid fielding phase after conducting a successful flight test. The Navy intends to field CPS aboard the first *Zumwalt*-class destroyer in FY25. The Navy intends to continue fielding CPS aboard the remaining two *Zumwalt*-class destroyers and commence fielding CPS aboard *Virginia*-class submarines as Phase 3. The program intends to complete an initial Life Cycle Support Plan by FY24 to address product support and fielding aboard both the *Zumwalt*-class destroyer and the *Virginia*-class submarine.

The CPS program continued development of the CPS AUR missile and elements of the weapons control system for the Army's LRHW (Dark Eagle) program in FY23. The Army integrated the CPS AUR missiles and weapon control system into a prototype LRHW Battery Operations Center and TEL system.

DOT&E placed CPS under oversight in June 2021. The Navy updated their Master Test Strategy (MTS) to address programmatic changes and additional performance metrics in January 2023. DOT&E conditionally approved the updated MTS in March 2023, provided that the CPS Program Office submit the Phase 2 and Phase 3 test strategies, the cyber survivability test and evaluation strategy, and the LFT&E strategy to DOT&E for approval prior to the end of 2023. The Navy has committed to providing a Test and Evaluation Master Plan to address these strategies.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

In March 2023, the Navy and the Army attempted the JFC-2 test flight. This was to be a hot launch from the Army's prototype TEL into a Broad Ocean Area in the Atlantic Ocean. The test did not occur due to failed pre-flight checks that prevented the launch. The Navy and the Army reattempted the JFC-2 flight test (JFC-2R) in September 2023. The AUR did not launch due to failed pre-flight checks. The Navy and the Army intend to reattempt JFC-2 and conduct the third test, JFC-3, in FY24. Both events use Army equipment and demonstrate hot-launch capability for the Dark Eagle program. JFC-4 and -5, to occur in FY24, are expected to demonstrate the cold-gas launch capability necessary for launch from *Zumwalt*-class destroyers and *Virginia*-class submarines. DOT&E will submit an early fielding report in FY25 in support of Navy fielding of CPS on the *Zumwalt*-class.

The Navy has not evaluated the effect of a contested environment (e.g., GPS denial, threat electromagnetic spectrum operations, threat kinetic and non-kinetic defensive capabilities) on CPS AUR missile performance. The

Navy plans to use a combination of modeling and simulation (M&S), component testing, and hardware-in-the-loop evaluations to assess CPS performance in the contested environment but has yet to detail this test strategy. DOT&E will report on the operational effectiveness in an IOT&E report upon completion of Phase 3 in FY29, but adequate testing in the contested environment is required to determine CPS effectiveness under combat conditions.

The Navy completed nine cyber survivability tabletop events in FY23 to identify the attack surface and potential vulnerabilities of the CPS AUR missile and its supporting combat system. These events will support cyber survivability evaluations in Phase 2 and Phase 3. The Navy has not yet submitted a cyber survivability test strategy for DOT&E approval. Cyber survivability testing of CPS in Phase 2 and Phase 3 must be adequate to support determination of its installation on the *Zumwalt*-class destroyer and the *Virginia*-class submarine.

As noted in the FY22 Annual Report, insufficient data are available to determine the survivability of CPS to kinetic or non-kinetic attack because the Navy has not yet completed the LFT&E strategy nor evaluated CPS against operationally representative threats. DOT&E will evaluate the validity of the Navy's proposed approach, including the use of M&S to bridge testing gaps, when the LFT&E strategy is submitted for approval in 1QFY24.

PERFORMANCE

» EFFECTIVENESS

The CPS Program has not demonstrated a prototype operational capability. JFC-1 experienced an in-flight anomaly that prevented collection of data over portions of the intended flight profile. The Navy has implemented corrective measures that have not yet been demonstrated. Further, no data are available to assess the effectiveness of CPS in the full-spectrum operational threat environment because the Navy has yet to evaluate these effects on CPS.

DOT&E will provide an assessment of the demonstrated capability of the CPS prototype system at the completion of the Phase 1 CPS prototype flight tests and Phase 2 CPS rapid fielding tests. DOT&E will assess CPS operational effectiveness within an IOT&E report upon the completion of Phase 3 testing that is planned for FY29.

» LETHALITY

As noted in the FY22 Annual Report, CPS sled and flight tests have not included operationally representative targets and consequently do not provide direct evidence of the weapon's lethal effects. The Navy is investigating methods to obtain lethality and effectiveness data by incorporating representative targets into the JFC tests and/or ground tests. The LFT&E strategy, which would allow DOT&E to evaluate the validity of the proposed approach, including the use of M&S tools to bridge testing gaps, is expected to be submitted for DOT&E approval in 1QFY24. A failure to demonstrate end-to-end effectiveness using representative targets could also limit the Navy's ability to create validated weaponeering tools, limiting operational utility.

» SUITABILITY

The CPS is not sufficiently mature to assess suitability. DOT&E will provide an assessment of the suitability metrics at the completion of Phase 1 CPS prototype flight tests and Phase 2 CPS rapid fielding tests. DOT&E will assess CPS operational suitability within an IOT&E report upon the completion of Phase 3 testing that is planned for FY29.

The program intends to complete an initial Life Cycle Support Plan in FY24 to address product support and fielding aboard both the *Zumwalt*-class destroyer and the *Virginia*-class submarine.

» SURVIVABILITY

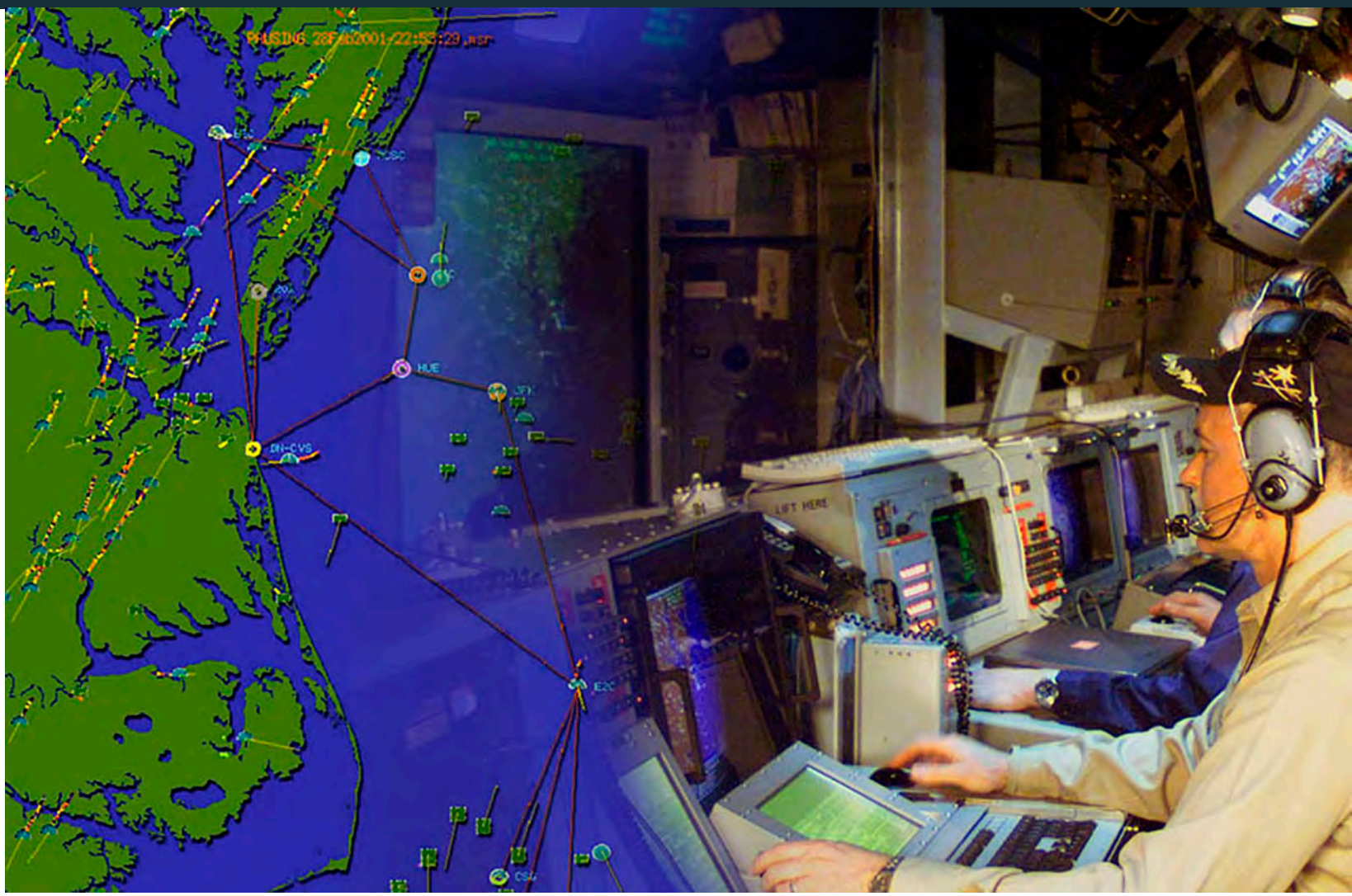
Insufficient data are available to determine the survivability of CPS to operationally relevant threats. DOT&E will report CPS survivability at the completion of Phase 2 CPS rapid fielding tests and within an IOT&E report upon completion of Phase 3 testing that is planned for FY29.

RECOMMENDATIONS

The Navy should:

1. Develop and submit for DOT&E approval in FY24, a test strategy for all phases of CPS development and delivery and that will sufficiently determine CPS AUR missile effectiveness, suitability, and survivability in the full spectrum contested environment.
2. Develop, and submit for DOT&E approval in FY24, a cyber survivability test strategy that supports assessment of CPS on the *Zumwalt*-class destroyer in Phase 2 and the *Virginia*-class submarine in Phase 3.
3. Develop and submit for DOT&E approval in FY24, the LFT&E strategy to evaluate the survivability and lethality of the CPS AUR missile in the operationally representative environment against threat representative targets. Coordinate this effort with the Joint Technical Coordinating Group for Munitions Effectiveness to include data required to validate the CPS weaponeering tools for operational use.

Cooperative Engagement Capability (CEC)



In FY23, the Navy commenced cyber survivability evaluation of the Cooperative Engagement Capability (CEC) variant used by the CVN 78 *Gerald R. Ford*-class nuclear aircraft carrier and commenced OT&E of CEC as integrated on Aegis Advanced Capability Build (ACB) 16 guided missile cruisers and destroyers. The Navy is developing CEC Increment II variants and creating the Test and Evaluation Master Plan (TEMP) for the associated test strategy.

SYSTEM DESCRIPTION

CEC is a real-time sensor fusion and netting system intended to enhance the situational awareness of equipped units and provide integrated fire control capability. CEC is comprised of a Cooperative Engagement Processor (CEP) and Data Distribution System (DDS). The CEP fuses data from the organic sensors of the employing platform/unit with data from remote sensors of other platforms/units within the net to construct target tracks. The CEP integrates with the employing platform/unit combat systems to display these tracks. DDS exchanges sensor data (e.g., radar and identification, friend or foe (IFF) measurements) between CEC-equipped platforms/units within line-of-sight.

CEC uniquely integrates the sensors and combat system of the host platform/unit. U.S. variants of CEC have three numeric designators. The "B" designator represents a capability upgrade that occurred within the legacy CEC program.

- AN/USG-2/2B for Navy surface ships
- AN/USG-3/3B for Navy E-2C Hawkeye 2000 and E-2D Advanced Hawkeye
- AN/USG-4B for U.S. Marine Corps Composite Tracking Network units

CEC Increment II will provide updates to both hardware and software from the legacy CEC and is intended to provide advanced capabilities and address more stressing threats. The Navy intends a phased delivery of CEC Increment II with the first phase designated as CEC Block 2.

MISSION

Navy commanders use units equipped with CEC to improve battle force air and missile defense capability by combining participating units' sensor data into a single, real-time, composite track picture. Combined data increases units' situational awareness, improves air picture quality, expands the battlespace, increases depth-of-fire, and enables integrated fire control. On aircraft carriers and select amphibious ships, CEC provides accurate air and surface tracking data for the Ship Self Defense System combat system.

CEC Increment II is intended to expand the use of CEC to support surface warfare and electronic warfare.

PROGRAM

CEC is an Acquisition Category IC program that achieved full operational capability in 2005. The draft CEC TEMP 1415 Revision 6 Change 1, dated April 2022, provides the test strategy for CVN 78, E-2D, DDG 1000, and Aegis ACB 16.

CEC Increment II is a separate Acquisition Category II program. The Navy intends to deliver CEC Increment II in a series of phases with the first phase designated as CEC Block 2. The Navy started development of an Increment II TEMP that will document the CEC Block 2 test strategy.

» MAJOR CONTRACTOR

- Collins Aerospace, a subsidiary of RTX (formerly Raytheon Technologies) – St. Petersburg, Florida

TEST ADEQUACY

From November 2022 to February 2023, the Navy conducted a cyber survivability evaluation of the DDG 1000 *Zumwalt*-class destroyer as part of the DDG 1000 IOT&E. Testing was conducted in accordance with a DOT&E-approved test plan and observed by DOT&E. The Navy intended for this test to simultaneously support a cyber survivability evaluation of the DDG 1000 variant of AN/USG-2B CEC. However, the DDG 1000 cyber survivability evaluation did not sufficiently investigate the AN/USG-2B CEC during the platform test. The Navy can still take advantage of platform-level testing to assess specific variants of CEC but must fully account for CEC test objectives and identify system expertise to support these objectives in associated test plans.

In July 2023, the Navy commenced the cyber survivability evaluation of the CVN 78 variant of AN/USG-2B CEC in conjunction with the CVN 78 IOT&E. The Navy conducted a cooperative vulnerability and penetration assessment (CVPA) and an adversarial assessment

(AA) at the land-based test facility at the Surface Combat System Center (SCSC), Wallops Island, Virginia. The Navy conducted testing in accordance with a DOT&E-approved test plan and with observation by DOT&E. Data collected are not yet adequate to assess cyber survivability of the CVN 78 variant of AN/USG-2B CEC because final assessment depends on remaining shipboard evaluation that the Navy plans to conduct in 2QFY24.

In July 2023, the Navy began FOT&E of the AN/USG-2B CEC as integrated with the ACB 16 of the Aegis Combat System used by guided missile cruisers and destroyers. This FOT&E is being conducted in conjunction with the Aegis ACB 16 FOT&E. The Navy conducted the test in accordance with the DOT&E-approved test plan and with observation by DOT&E. However, the test was not adequate to assess operational effectiveness and suitability of this version of CEC due to issues with SM-6 availability and E-2D reliability that prevented several planned test events from being conducted. The Navy conducted a subset of aircraft tracking, missile tracking, and missile firing events. The Navy expects to complete remaining test events in FY24. Further, the Navy plans to conduct cyber survivability evaluation of this variant of AN/USG-2B CEC during Aegis ACB 16 cyber survivability evaluation in FY24.

The Navy intends to conduct testing to support evaluation of operational effectiveness and suitability of the DDG 1000 and CVN 78 variants of AN/USG-2B CEC during platform IOT&Es in 1QFY24.

The Navy has taken no action on DOT&E's recommendations provided in the FY20 Annual Report that pertain to the AN/USG-3B variant of CEC on E-2D.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Insufficient data are available to determine operational effectiveness and suitability of the DDG 1000 or CVN 78 variants of AN/USG-2B CEC, or integration of AN/USG-2B CEC with Aegis ACB 16, due to tests remaining in progress.

» SURVIVABILITY

Insufficient data are available to determine the cyber survivability of the DDG 1000 variant of the AN/USG-2B due to failure to attain sufficient data related to CEC during the DDG 1000 cyber survivability evaluation.

Insufficient data are available to determine the cyber survivability of the CVN 78 variant of AN/USG-2B CEC, or integration of AN/USG-2B CEC with Aegis ACB 16, due to tests not completing in FY23.

RECOMMENDATIONS

The Navy should:

1. Complete FOT&E on the DDG 1000 and CVN 78 variants of AN/USG-2B CEC, and integration of AN/USG-2B CEC with Aegis ACB 16.
2. Provide a CEC Increment II TEMP for DOT&E approval.
3. Address the DOT&E recommendations provided in the FY20 Annual Report that pertain to the AN/USG-3B variant of CEC on E2D.
4. Define a cyber survivability evaluation strategy to efficiently evaluate CEC across its supported platforms and comprehensively include CEC test requirements within any test plan that is intended to attain evaluation of a CEC variant.

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

In May 2023, USS *Gerald R. Ford* (CVN 78) deployed to meet operational needs, prior to completing IOT&E. In April 2023, DOT&E issued a classified early fielding report (EFR), based on limited data collected from IOT&E events. In FY23, prior to the ship's deployment, the Navy continued IOT&E on CVN 78, completing two significant at-sea periods as part of the carrier strike group (CSG), with an operationally representative crew executing operationally representative flight operations, and continuing land-based cyber survivability testing. In FY23, CVN 78 conducted almost as many flight operations as it had in the previous five years combined since commissioning. Reliability and maintainability challenges with systems critical to consistent and on-demand flight operations continue to pose the most risk to CVN 78 demonstrating operational effectiveness and suitability in IOT&E, which is now expected to extend through FY27. Executing planned sortie generation and self-defense tests will be critical to evaluating the ship's effectiveness and survivability, along with accrediting high-fidelity flight operations and Probability of Raid Annihilation (P_{RA}) models, which are essential for evaluating key performance parameters (KPPs).

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 Aircraft Launch System (EMALS) catapults and electromechanical Advanced Arresting Gear (AAG). The originally planned AAG engine and wire positioning (consisting of four engines and three wires) was similar to the USS *Ronald Reagan* (CVN 76) and USS *George H. W. Bush* (CVN 77) flight decks. However, the fourth AAG engine has not been installed on *Ford*-class to date as a cost savings measure. 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 compared to *Nimitz*-class (CVN 68) aircraft carriers. The CVN 78 class combat system incorporates the following systems:

- Dual Band Radar (DBR) that combines the phased-array SPY-4 Volume Search Radar and the SPY-3 Multi-Function Radar. CVN 78 is the only ship with DBR; it will eventually be replaced with the SPY-6(V)3 Enterprise Air Surveillance Radar (EASR) fixed variant, the SPQ-9B horizon search radar, and Mk 9 Tracker Illuminator System as will be installed on *John F. Kennedy* (CVN 79) and follow-on carriers.
- Ship Self-Defense System (SSDS) Mk 2 Mod 6 with Baseline 10 combat management system, which will be upgraded to the new capability build, Baseline 12, on CVN 79.
- AN/USG-2B Cooperative Engagement Capability (CEC) tracking, data fusion, and distribution system, which will be upgraded to CEC Block II starting on CVN 79.
- SLQ-32B(V)6 electronic warfare system equipped with the Surface Electronic Warfare Improvement Program (SEWIP) Block 2.
- Rolling Airframe Missile (RAM) Block 2 and Evolved Sea Sparrow Missile (ESSM) Block 1. CVN 79 and beyond will be upgraded to a mix of new RAM variants Block 2A and 2B, plus a mix of ESSM Block 1 and Block 2.
- Close-In Weapon System, which operates in stand-alone mode on CVN 78, but will be integrated with AN/USG-2B CEC and SSDS on CVN 79.

Ford-class ships also have enhanced survivability features, including improved protection for magazines and other vital spaces; shock-hardened mission systems and components; and installed and portable damage control, firefighting, and dewatering systems intended to expedite response to and recovery from fire, flooding, and battle damage.

MISSION

CSG commanders will use *Ford*-class ships to:

- Provide credible, sustainable, independent forward presence during peacetime without access to land bases;
- Operate in a supported or supporting role with a joint and/or allied maritime expeditionary force in response to crises; and
- Carry the war to the enemy, independent of forward-based land facilities, through joint multi-mission offensive operations by:
  - Operating and supporting aircraft to attack enemy forces ashore, afloat, or submerged;
  - Protecting friendly forces from enemy attack through the establishment and maintenance of battlespace control; and
  - Engaging in sustained operations in support of the United States and its allies.

PROGRAM

The CVN 78 *Gerald R. Ford*-class is an Acquisition Category IC program. DOT&E approved Revision E of the Test and

Evaluation Master Plan (TEMP) in September 2022 and Revision B of the LFT&E Management Plan in September 2023. The first ship in the *Ford*-class, CVN 78, was delivered to the Navy in 2017. It completed Post Delivery Test and Trials in April 2021 to demonstrate the basic functionality of the carrier, certify the flight deck, and embark an air wing. CVN 78 also completed Full Ship Shock Trials (FSST) in August 2021 and a Planned Incremental Availability in February 2022. DOT&E approved the first of two planned phases of the IOT&E test plan, and IOT&E began in September 2022. IOT&E is now expected to complete in FY27. This timeline is three years longer than that reported in the FY22 Annual Report for two reasons: The first is a change in the ship's schedule, which has delayed key test events, including sortie generation rate (SGR) and self-defense tests, and the second is the time required for the Navy to incorporate data from the SGR and self-defense tests into the respective models, run the models, and analyze the model outputs.

The Navy deployed CVN 78 in May 2023, which was earlier than the scheduled timeline for first deployment in TEMP Revision E. In preparation for the first deployment, CVN 78 completed its first Composite Training Unit Exercise (COMPTUEX) in April 2023. DOT&E approved Revision 1 to the IOT&E test plan in March 2023 to include IOT&E data collection opportunities during the COMPTUEX. Due to this schedule change, the original two-phase structure of the IOT&E test plan will be replaced with a more incremental test plan approach. The Navy should submit a test plan revision to DOT&E to reflect this new approach.

CVN 79 delivery is now scheduled for late FY25, a year later than reported in the FY22 Annual Report. The delay is due to the Navy moving some work from CVN 79's post-delivery Post Shakedown Availability to before delivery, in order to mitigate schedule risk to its first deployment. CVN 79 will be capable of supporting F-35 operations. *Enterprise* (CVN 80) construction began in August 2017 and is expected to be delivered to the Navy in FY28. *Doris Miller* (CVN 81) construction began in August 2021 and is expected to be delivered to the Navy in FY32. The most significant upgrades with CVN 79 and beyond are related to the combat system. The TEMP is being updated to include operational testing of F-35 on *Ford*-class and CVN 79's self-defense capabilities. The Navy expects to update the TEMP in 1QFY25 before CVN 79 is delivered. This timeline is later than that reported in FY22 to facilitate synchronizing the test strategy with the ship's updated delivery schedule.

» MAJOR CONTRACTOR

- Newport News Shipbuilding, a division of HII (formerly Huntington Ingalls Industries) – Newport News, Virginia

TEST ADEQUACY

The Navy began CVN 78 IOT&E in September 2022 and is conducting it in accordance with TEMP Revision E and the DOT&E-approved portions of the IOT&E test plan. However, analysis of the data provided to DOT&E to date revealed gaps in data collection, which, if not rectified, could result in insufficient data to inform conclusive assessments of reliability, maintainability, logistics and/or availability (RMLA) for some key subsystems. In addition to affecting suitability assessments, these data gaps could also affect effectiveness assessments due to the on-demand nature of many key subsystems and the reliance upon accurate RMLA data in both the self-defense and SGR models. The Navy has acknowledged these shortcomings, committed to improve data collection, and will update the IOT&E test plan for the major remaining tests such as SGR, self-defense, and cyber survivability tests. In April 2023, DOT&E submitted a classified CVN 78 *Ford*-class Aircraft Carrier EFR to Congress, detailing operational and live fire test results to date.

Prior to deployment, CVN 78 conducted two significant underway periods during IOT&E that included fixed-wing flight operations, both of which were in accordance with the DOT&E-approved test plan and observed by DOT&E. A brief summary is below, and detailed results of the underway periods can be found in DOT&E's classified EFR.

In the first significant underway period of IOT&E, CVN 78 executed a service-retained early employment from October 4 to November 26, 2022, as part of CSG 12 that included Tailored Ship's Training Availability (first deployment work-up integrated with CSG); port calls in Halifax, Canada and Portsmouth, England; and multiple operations with allies and partners. The early employment was the first time the air wing, destroyer squadron staff, and CSG staff embarked on the ship together, and the first period of consistent cyclic flight operations for the *Ford*-class, which resulted in 896 arrested landings (not including carrier qualifications). During the early employment, the maximum air wing compliment was approximately 75 percent of the full air wing.

In the second significant underway period of IOT&E, CVN 78 completed its first COMPTUEX (final pre-deployment workup) from March 2 to April 2, 2023, off the U.S. east coast. Administered by CSG 4, COMPTUEX was the first time CVN 78 operated with an operationally representative air wing embarked, conducting consistent, combat-representative scenarios. During COMPTUEX, CVN 78 executed 1,600 total arrested landings, including 1,185 arrested landings during cyclic and alert flight operations. At the end of COMPTUEX, CVN 78 had conducted a total of 14,177 catapult launches and arrested landings since its commissioning.

In July 2023, the second of three planned CVN 78 land-based cyber survivability operational tests was completed on SSDS, CEC, and SEWIP. The test was conducted in accordance with the DOT&E-approved test plan and observed by DOT&E. These land-based tests are intended both to inform planning for shipboard testing and to perform testing deemed too risky to conduct during shipboard cyber survivability tests prescribed by TEMP Revision E.

Many systems specific to CVN 78 have yet to undergo any operational cyber survivability assessments. In June 2023, the Navy updated its cyber survivability testing strategy by replacing the third land-based cyber survivability test with additional testing during shipboard cyber assessments after deployment. The third land-based test was scheduled for late FY23, and its focus was on hull, mechanical, and electrical systems. This change in strategy was primarily due to a lack of existing, robust cyber survivability testing facilities for shipboard industrial control systems. The Navy needs to conduct the shipboard tests to assess CVN 78's overall cyber survivability and enable post hoc accreditation of the test facilities used in completed land-based cyber survivability tests. The Navy is still developing these shipboard cyber survivability test plans.

The CVN 78 Total Ship Survivability Trial (TSST) has been delayed by approximately one year, until 4QFY24, due to the ship's deployment being earlier than planned. The TSST is an onboard, extensive damage-control test to demonstrate how the ship design enables the crew to perform its recoverability-related procedures. For the CVN 78 TSST to be adequate, the testing will require at-sea execution with participation of an embarked air wing. Planning is ongoing to ensure that this adequacy requirement is met.

In 1QFY24, the Navy intends to publish two vulnerability assessment reports (VARs) examining the class's survivability against above-water and underwater kinetic threats. These reports will include findings from survivability testing and modeling of the ship conducted since 2007. However, these reports as drafted do not accurately model the ship as built and do not include findings from more recent testing. Without updating the models, the analysis in the VARs will not support conclusions on the survivability of the CVN 78 class against threat weapons. The Navy intends to issue a final survivability assessment report that will include the findings from recent testing and update model-based survivability analysis by 4QFY25. If the survivability modeling and simulation (M&S) is updated to accurately model the ship as built, this assessment will support DOT&E's report on the survivability of the class against threat weapons.

Together the CVN 78 TEMP Revision E and the Capstone Enterprise Air Warfare Ship Self-Defense (AW SSD) TEMP 1714 of March 2008 provide for a series of

live missile fire events aboard CVN 78 against specific types of ASCM threat surrogates to assess the ship's anti-air warfare capabilities. The Navy intends to execute these tests in FY25. These live tests are necessary to assess ship self-defense capability of the as-built, deployed combat system, and to provide validation data for the M&S suite of the CVN 78 combat system. While these live fire tests, as planned, are adequate, DOT&E has concerns with the Navy's ability to adequately resource them. The M&S is intended to assess the Navy's P_{RA} KPP. These tests, combined with those conducted on the self-defense test ship, and the P_{RA} model runs are required to determine CVN 78's operational effectiveness against specific types of ASCM threats. In FY23, the Navy continued to develop a draft new Enterprise TEMP in support of SSDS Mk 2 Baseline 12 and SPY-6 V(2) and V(3) platforms (TEMP 1910) that includes FOT&E on CVN 79. While CVN 79 self-defense test design will mature during the TEMP 1910 development, any delay in the current timeline for testing the CVN 79 combat systems will be challenged by the planned deactivation timeline for the self-defense test ship, the ex-USS *Paul F. Foster*. The Navy should maintain the capability of the self-defense test ship, currently provided by the ex-USS *Paul F. Foster*.

The CVN 78 SGR evaluation comprises M&S (for both *Ford* and *Nimitz* class), a four-day sustained test on CVN 78, a one-day surge test on CVN 78, and flight operations observations on a *Nimitz*-class carrier. Development of the M&S suite intended to evaluate the SGR, the Sea Strike/Sea Basing Aviation Model (SSAM), is ongoing. The CVN 78 SGR tests are incomplete. The CVN 78 sustained SGR test was originally scheduled for the first COMPTUEX; however, due to COMPTUEX syllabus changes, ship and air wing schedule changes, and resourcing, it was deferred to the second COMPTUEX, now expected to occur in FY25. The Navy plans to apply lessons from the CVN 78 sustained SGR test to the surge SGR test which is currently unscheduled. A *Nimitz*-class COMPTUEX to collect flight operations data to support a *Nimitz*-class SGR M&S suite (part of SSAM) for comparative analysis is planned for FY24. DOT&E approved these deferments in Revision 1 to the IOT&E test plan. The Navy needs to provide an updated test plan prior to conducting these events.

PERFORMANCE

» EFFECTIVENESS

Insufficient data are available to determine CVN 78's operational effectiveness due to IOT&E being incomplete. Observations based on testing to date are below.

Combat System

Self-defense testing against unmanned aerial vehicles (UAVs) and high-speed maneuvering surface targets (small boats) was conducted in July 2022. Details can be found in DOT&E's classified EFR. The Navy is developing fixes to combat system deficiencies identified in DOT&E's classified USS *Gerald R. Ford* (CVN 78) Self-Defense Interim Assessment report dated April 2022. However, to date the fixes remain largely unfunded.

Sortie Generation

In FY23, CVN 78 conducted almost as many flight operations (as measured by the number of aircraft launch and recoveries) as it had in the previous five years combined since commissioning. From the first arrested landing on CVN 78 in July 2017 until the end of FY22, CVN 78 had conducted 10,826 arrested landings. In FY23 alone, CVN 78 conducted 9,266 arrested landings. The reliability and maintainability of CVN 78's EMALS and AAG continue to adversely affect sortie generation and flight operations, which remains the greatest risk to demonstrating operational effectiveness and suitability in IOT&E. Despite these continuing reliability challenges, DOT&E observed general increases in crew proficiency and decreases in some repair times. While this has improved sortie generation compared to previous years, SGR tests have not been completed yet nor have training sortie rates flown to date approached that of the KPP requirement. CVN 78 earned the flight operations efficiency portion of its Blue Water Certification as part of the Navy's deployment certification process. Observations during COMPTUEX suggests that the *Ford*-class flight deck design improves the efficiency of aircraft turnarounds compared

to that of a *Nimitz*-class flight deck. Additional details on sortie generation effectiveness can be found in DOT&E's classified EFR. Executing the planned SGR testing, as outlined in TEMP Revision E, will be crucial to evaluating the ship's combat effectiveness and accrediting the high-fidelity SSAM which is an essential tool for evaluating the SGR KPP and supporting life-of-class upgrades.

Electromagnetic Spectrum Compatibility

Developmental testing identified significant electromagnetic radiation hazard and interference problems. The Navy implemented some mitigation measures and conducted follow-on characterization testing during independent steaming events in developmental test, but some operational limitations and restrictions are expected to persist into IOT&E and deployment. The Navy should verify developmental test electromagnetic spectrum compatibility during operational test, particularly when integrated with CSG operations in an advanced electronic attack environment. This will enable capability assessments at differing levels of system use to inform decisions on system employment.

» SUITABILITY

Insufficient data are available to determine CVN 78's operational suitability. However, the following four new CVN 78 systems have shown low or unproven reliability and are highlighted as the most significant challenge to flight operations.

AAG

During FY23, DOT&E observed AAG reliability similar to recent developmental testing (115 mean cycles between operational mission failures [MCBOMF] in FY21 and 460 MCBOMF in FY22). Despite some software and hardware improvements in AAG, reliability has not appreciably changed because the FY23 data reflects many short-duration failures that were unreported in developmental test, as well as system-of-systems degradations, all of which would have prevented landing. Naval Air Systems Command (NAVAIR) delivered hardware updates after early employment and before COMPTUEX, along with a software update before deployment. NAVAIR continues to work on short- and long-term improvements to address AAG reliability degraders.

However, difficulties such as obtaining replacement parts and the reliance on off-ship technical support remain a challenge. The Navy is also using IOT&E to inform the decision of whether to retrofit the fourth AAG engine on *Ford*-class aircraft carriers (as designed, which would make it similar to the arresting gear engine/wire configuration on CVN 76 and CVN 77). The fourth AAG engine was not installed as a cost savings measure. In a 2016 requirements review board, the Navy committed to informing a potential retrofit decision with the results of IOT&E. The criteria on which to base a potential retrofit decision were not specified, and with changes to the IOT&E schedule, more data will be available before the end of IOT&E. The fourth engine would improve the reliability and availability of AAG, improve pilot boarding rate, and restore barricade redundancy. Additional details on AAG suitability can be found in DOT&E's classified EFR.

EMALS

During FY23, DOT&E observed EMALS reliability remained consistent with recent developmental test (460 MCBOMF in FY21 and 614 MCBOMF in FY22). Despite engineering upgrades to hardware and software, reliability has not appreciably changed from prior years and reliance on off-ship technical support remains a challenge. As part of an effort to provide short- and long-term improvements to address EMALS reliability degraders, NAVAIR delivered a software update and upgraded all catapult position sensor blocks prior to CVN 78's deployment and is continuing development on further improvements. Furthermore, a situational awareness display was added in the EMALS Maintenance Workstation that facilitates troubleshooting during operations. Additional details can be found in DOT&E's classified EFR.

Advanced Weapons Elevators (AWEs)

The early employment and COMPTUEX provided CVN 78's first operationally representative opportunities to demonstrate ordnance movement during cyclic flight operations. The AWEs met operational mission needs during these underway periods, but preliminary data suggest AWE is unlikely to meet its operational availability requirement of 99.7 percent. Of note, the crew is reliant on off-ship technical support for correction of hardware and software failures. As of the end of COMPTUEX, the ship had conducted 23,042 total AWE cycles. The Navy has yet to build and transfer ordnance to the flight deck at combat-representative rates. DOT&E expects the SGR tests to be the first operationally representative demonstration of high ordnance throughput. Additional details can be found in DOT&E's classified EFR.

DBR

During COMPTUEX, DBR availability was observed to be lower than that during developmental testing. This is in part due to the operational expectation of continuous radar coverage. Reliability concerns are amplified due to the one-of-a-kind nature of the DBR. The radar relies on embarked contractor support and there is uncertainty on sourcing replacement parts as the system ages. The Navy should ensure replacement parts are manufactured and available for the life of the system or develop a timeline and strategy for replacing DBR with EASR on CVN 78 to bring it in line with CVN 79's radar configuration. Additional details on DBR suitability can be found in DOT&E's classified EFR.

Manning and Berthing

Per the Navy's Shipboard Habitability Program, all new ships are required to have a growth allowance of 10 percent of ship's company when the ship delivers. This Service Life Allowance provides both empty bunks to allow for changes in the crew composition over the ship's life and berthing to support crew turnover, visitors, and personnel temporarily assigned to the ship for repairs, inspections, test, and training. However, sufficient berthing is not installed for CVN 78 to conduct combat operations with all hands assigned a bed. While the ship's company manning is reduced from *Nimitz*-class carriers by approximately 500 personnel, the lack of berthing capacity is driven by embarked units. Based on the composition of the ship and embarked units during COMPTUEX and their respective manning documents, if each was at 100 percent manning, the ship would have a shortfall of 159 beds. These berthing shortfalls will affect quality of life onboard and could reduce the Navy's operational flexibility in employing the ship across its full spectrum of missions and logistical support roles for the CSG. Furthermore, there is potential that the berthing shortfalls could increase as the air wing diversifies to include CMV-22, F-35, and MQ-25, none of which are on CVN 78 today. Additional details on manning and berthing can be found in DOT&E's classified EFR.

» SURVIVABILITY

An adequate survivability assessment of the CVN 78 class depends upon a combination of FSST, TSST, and related modeling of the class supported by component and surrogate testing. To date, the Navy has completed all planned LFT&E, with the exception of TSST, the VARs, and the final survivability assessment.

From June to August 2021, the Navy conducted FSST on CVN 78,

including three shock events of increasing severity. In December 2022, DOT&E published a classified FSST report that details findings from the trial, and in July 2023, the Navy published its own FSST report. Both reports identify deficiencies that, if addressed, will improve the class's survivability against weapon events.

The survivability of CVN 78 in a cyber-contested environment has not yet been fully evaluated. Results from the land-based cyber survivability tests will inform the shipboard cyber survivability tests. Some systems specific to CVN 78 have yet to undergo any operational cyber survivability assessments.

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

RECOMMENDATIONS

The Navy should:

1. Improve the suitability of AAG, EMALS, AWE, and DBR while minimizing the requirement for off-ship and/or contractor technical support.
2. Reevaluate the timeline and better define the criteria for a decision to retrofit the fourth AAG engine.
3. Collect data in accordance with the test plan for the remainder of IOT&E.
4. Resource and execute the testing per Enterprise AW SSD TEMP 1714 and CVN 78 TEMP, including the planned SGR testing, along with completing, verifying, and validating the SGR M&S suite; shipboard cyber survivability testing; and self-defense tests and P_{RA} modeling.
5. Address the recommendations in DOT&E's classified self-defense interim assessment report from April 2022, and the additional recommendations in DOT&E's classified EFR from April 2023.
6. Develop a plan to sustain DBR on CVN 78 or replace it as soon as possible with the EASR configuration on CVN 79 and subsequent *Ford*-class carriers.
7. Re-examine manning and berthing for future ships of the class to ensure sufficient berthing is available and that 10 percent Service Life Allowance is allocated to allow future growth.
8. Submit for DOT&E approval a test plan revision to update the test plan schedule.
9. Continue to develop more robust capabilities to test the cyber survivability of shipboard industrial control systems.
10. Execute the TSST with an embarked air wing in FY24.
11. Prioritize and correct deficiencies identified in DOT&E's classified FSST report of December 2022.
12. Produce a project schedule to complete required updates to the vulnerability modeling and simulation by 4QFY24 to support accurate vulnerability reporting in the CVN 78 final survivability assessment report in 4QFY25.
13. Submit for DOT&E approval in 1QFY25 an update of the CVN 78 TEMP, aligned with the new Enterprise TEMP 1910, that provides the test strategy and test resources to determine operational effectiveness of new and/or upgraded capabilities on CVN 79.
14. Ensure the availability of the capability provided by ex-USS *Paul F. Foster*, the Navy's self-defense test ship, to support combat system testing.
15. To better inform effectiveness and survivability, verify developmental test electromagnetic spectrum compatibility during operational test, particularly when integrated with CSG operations in an advanced electronic attack environment.

DDG 1000 *Zumwalt*-Class Destroyer

As part of the ongoing IOT&E that commenced in FY22, the Navy commenced modeling and simulation (M&S) testbed runs in FY23 that will inform DDG 1000 *Zumwalt*-class anti-air warfare capability against threat anti-ship cruise missiles (ASCMs). Insufficient data are available to change the assessment provided in DOT&E's classified early fielding report of November 2022. The Navy also completed evaluation of *Zumwalt*-class survivability to cyberattack which will be included in a classified report upon completion of IOT&E, currently expected in FY24.

SYSTEM DESCRIPTION

Zumwalt-class ships are long range, low observable, destroyers. They are equipped with: 1) a modified AN/SPY-3 Multi-Function (X-band) radar that adds a volume search capability; 2) 80 vertical launch cells to employ Tomahawk Land Attack Missiles, Standard Missiles (SM-2/SM-6), 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 missions, with a secondary mission of surface warfare dominance. As

designed, the *Zumwalt* class included undersea warfare capabilities, but the Navy now does not intend to use the ship in this role. The *Zumwalt* class is designed for independent operations but can be integrated into Carrier or Expeditionary Strike Group operations.

Between 1QFY24 and 2QFY28, the Navy will install Conventional Prompt Strike (CPS) modules on each ship of the class. These modules will provide the *Zumwalt* class additional strike warfare capability.

PROGRAM

The *Zumwalt* class is an Acquisition Category IC program. The President's Budget in 2011 truncated the class to three ships. The Navy commissioned USS *Zumwalt* (DDG 1000) in 2016 and USS *Michael Monsoor* (DDG 1001) in 2019 and expects the delivery of *Lyndon B. Johnson* (DDG 1002) in FY27 after CPS install.

The Navy continues to update 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 surface strike, removed all requirements related to mine avoidance capability, and codified additional changes in a June 2021 revision to the Operational Requirements Document, to include the addition of CPS. The Navy also intends to remove requirements to test undersea warfare capabilities of the ship in the next revision of the TEMP based on revised employment of the class. The *Zumwalt*-class IOT&E started in October 2021 and will continue into FY24. DOT&E will require testing not completed during IOT&E to be addressed in FOT&E as part of the TEMP revision.

» MAJOR CONTRACTORS

- Bath Iron Works, a subsidiary of General Dynamics Corporation – Bath, Maine
- HII (formerly Huntington Ingalls Industries) – Pascagoula, Mississippi
- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Arlington, Virginia

TEST ADEQUACY

Zumwalt-class testing to date was conducted in accordance with the DOT&E-approved test plans and observed by DOT&E. The Navy began modeling and simulation (M&S) Probability of Raid Annihilation testbed runs in July FY23 and expects to complete in FY24. These runs will evaluate the *Zumwalt* class's probability of defeating inbound anti-ship cruise missiles (ASCMs) as part of *Zumwalt* class's anti-air warfare mission. Additional live fire testing against ASCM surrogates is scheduled aboard DDG 1001 in December 2023, however there is currently no plan to rerun M&S with updated data from the live fire testing.

The Navy completed a cyber cooperative vulnerability and penetration assessment and an adversarial assessment between November 2022 and March 2023. Testing encompassed Internet Protocol (IP) networks aboard the ship along with industrial control systems associated with its hull, mechanical, and electrical systems. These tests were adequate to assess cyber survivability of the class, in accordance with the DOT&E-approved test plan, and observed by DOT&E.

As noted in the FY22 Annual Report, the Navy has not yet 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. The Navy is currently evaluating options for completion of the equipment shock qualification program and conduct of an alternative to shock trial that would sufficiently assess the risk to the warfighter from associated weapon events.

The Navy has not yet updated vulnerability and recoverability M&S meant to support the LFT&E survivability assessment of the *Zumwalt* class to reflect the ship as built. In the FY22 Annual Report, DOT&E recommended that the Navy work to develop an updated M&S strategy that would include survivability model updates, but currently the Navy does not intend

to update, validate, or accredit LFT&E survivability assessments prior to completing their LFT&E program in FY24, previously expected to be completed 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.

PERFORMANCE

» EFFECTIVENESS

Not enough data are yet available to determine *Zumwalt*-class operational effectiveness. Simulation runs for AAW remain in progress and no update in the determination of AAW performance can be made from the preliminary assessment provided in DOT&E's classified early fielding report of November 2022. Similarly, torpedo defense testing conducted with DDG 1000 in October 2021 provided data on the class's ability to evade torpedoes, but the postponement and proposed cancellation of other undersea warfare test events prevents further assessment of the class's effectiveness against undersea threats. 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.

» SUITABILITY

Not enough data are yet available to provide an assessment of *Zumwalt*-class operational suitability. DOT&E will report operational suitability after changes to hardware and software baselines associated with the install of CPS and the technological refresh of the class's Command, Control, Communication, Computer, Cyber and Intelligence (C5I) systems.

» 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. DOT&E will require that the survivability M&S be updated and validated as part of the upcoming TEMP revision.

Failure and recoverability mode testing aboard DDG 1001 conducted in 2022 provided insight into the recoverability of the class after damage. However, testing was not sufficient to resolve associated LFT&E critical issues due to limitations on the systems under test. DOT&E will address the strategy for completing the LFT&E assessment of the *Zumwalt* class's mission system recoverability as part of the upcoming TEMP revision.

Results from cyber survivability testing aboard DDG 1000 conducted between November 2022 and March 2023 will be included in a classified report upon completion of IOT&E, currently expected in FY24.

RECOMMENDATIONS

The Navy should:

1. Complete remaining IOT&E events in accordance with the DOT&E-approved test plans.
2. Complete revision of the TEMP that includes completion of existing IOT&E requirements and an adequate test strategy for the as-delivered mission capabilities after installation of CPS.
3. Complete development and validation of the combat system M&S testbed, to include debris, missile, radar, and electronic warfare models.
4. As noted in the FY22 Annual Report, document the risk to the warfighter associated with incomplete component shock qualification and lack of full-ship shock trial prior to deployment.
5. Update the LFT&E strategy to include evaluation of the as-built survivability of the *Zumwalt* class and submit it for DOT&E approval with the TEMP update.
6. Plan and resource within the TEMP update a full ship shock trial of the first available *Zumwalt*-class ship with CPS installation.
7. As recommended in the FY22 Annual Report, sufficiently fund modernization and sustainment of the DDG 1000 class to include improvements determined from Failure and Recoverability Mode testing, which will be documented in the final survivability assessment report.

Distributed Common Ground System – Navy (DCGS-N)

The Program Office for Battlespace Awareness and Information Operations (PMW 120) and the Navy's Operational Test and Evaluation Force (OPTEVFOR) are using the level of test determination process to conduct testing of Distributed Common Ground System – Navy (DCGS-N) enhancements. OPTEVFOR is providing timely information to PMW 120, and the program has made acquisition and deployment decisions consistent with OPTEVFOR's evaluations. DOT&E agrees with this approach as documented in the DOT&E-approved Test and Evaluation Master Plan (TEMP).

SYSTEM DESCRIPTION

DCGS-N is the Navy Service component of the DoD DCGS family of systems, which provides multi-Service integration of intelligence, surveillance, reconnaissance, and targeting capabilities. DCGS-N Increment 1 is fielded to the Force-level ships and shore sites. The Navy is updating DCGS-N by incrementally adding mature commercial and government applications.

Current upgrades include the addition of the Fusion Analysis and Development Effort (FADE) desktop application and Track Management Display System (TMDS). FADE is a government off-the-shelf application from National Reconnaissance Office. It is accessible via both a website and the new desktop application, which allows users to download the data so that they can continue to use the FADE application when the network is disconnected. TMDS is an enhancement to a deployed application.

MISSION

Operational commanders use DCGS-N to participate in the joint task force-level targeting and planning processes and to share and provide Navy-organic intelligence, reconnaissance, surveillance, and targeting data to joint forces.

Units equipped with DCGS-N will:

- Identify, locate, and confirm targets through multi-source intelligence feeds.
- Update enemy track locations and provide situational awareness to the joint force maritime component commander by processing data drawn from available sensors.

PROGRAM

The Assistant Secretary of the Navy for Research, Development, and Acquisition approved transition of DCGS-N Increment 2 to the DoD Instruction 5000.02's adaptive acquisition framework, software acquisition pathway in January 2021. DCGS-N Increment 2 brings in incremental upgrades, using commercial and government applications whenever possible. DOT&E approved the updated TEMP for the software acquisition pathway approach in August 2022. The TEMP describes a process for tailoring test and evaluation in accordance with the potential risks associated with the upcoming incremental changes. OPTEVFOR conducts level of test determinations in cooperation with the program office and submits a recommendation to DOT&E for approval. The level of test ranges from observing developmental tests (DTs) to conducting a full scoped operational test.

» MAJOR CONTRACTOR

- CACI International, Inc. – Denver, Colorado

TEST ADEQUACY

In accordance with the DOT&E-approved TEMP, the program office conducts Application Integration System Integration Tests (AI SITs) for each new release to evaluate whether the new or enhanced applications and services work with other interfacing systems. OPTEVFOR observes AI SITs to gain knowledge about the updates and uses that knowledge, along with information on the scope of the new release, to conduct a level of test determination.

Based on the level of test determination results, OPTEVFOR observed DTs for two versions of DCGS-N in FY23.

- V4.0.2/4.5.2: OPTEVFOR observed AI SIT 22-2 conducted by PMW 120 in March 2023.
- V4.0.1.0/4.5.1.1: The main upgrade for this version was addition of the FADE desktop application and TMDS. OPTEVFOR observed the DT conducted by PMW 120 aboard USS *Theodore Roosevelt* (CVN 71) in May 2023 based on the level of test approval after the AI SIT 22-1. OPTEVFOR published a Letter of Observation in July 2023.

Both DT events accomplished their objectives. The program office coordinated closely with DOT&E and OPTEVFOR in their DT planning, conduct, and reporting process to provide input for the risk assessment leading to a determination of appropriate

level of test. The program office invites DOT&E and OPTEVFOR for engineering review boards where shortfalls identified during the test are scored, and mitigation measured are discussed. The resulting deployment decisions have been consistent with the evaluation results. The program office only deployed applications or services that were tested and evaluated to be effective and suitable by OPTEVFOR.

The Naval Sea Systems Command Red Team conducted penetration testing in a laboratory setting to evaluate the cyber survivability posture of DCGS-N in March 2023. The assessment was conducted using an insider threat/assumed compromise methodology. It was part of a series of cyber survivability test events to get ready for the future cooperative vulnerability and penetration assessment and the adversarial assessment. The location and timing of these cyber assessments are under discussion.

PERFORMANCE

There is not enough data available for DOT&E to make an operational effectiveness, suitability, or survivability determination. The following is provided based on testing observed by OPTEVFOR.

» EFFECTIVENESS

The testing involving FADE showed that users receive the same information on the desktop as the website.

The test also demonstrated that intelligence analysts can use TDMS to add, modify, and delete track information, and pass information between common intelligence picture from DCGS-N and common operational picture on Global Command and Control System – Maritime.

» SUITABILITY

PMW 120 is developing a formal training guide. The training for FADE was only provided to the cryptology technicians and not for the intelligence specialists. Users expressed satisfaction with the training they received for the TMDS. OPTEVFOR will continue to monitor the FADE training in future iterations.

» SURVIVABILITY

During the laboratory-based developmental testing in preparation for the eventual operational test, testers with unauthenticated and user-level access to the environment found several vulnerabilities specific to DCGS-N and made general security posture recommendations.

RECOMMENDATIONS

None.

E-2D Advanced Hawkeye

In FY23, the Navy conducted integrated testing (IT) and operational testing (OT) on E-2D Delta System Software Configuration Build 4 (DSSC-4). DSSC-4 improves the Advanced Hawkeye's command and control capability and is the fourth in a series of biennial hardware and software upgrades to the E-2D. The Navy expects to complete DSSC-4 OT in 2QFY24. The Navy began upgrading fleet aircraft to the DSSC-4 configuration in 3QFY23 to support an FY24 operational deployment.

SYSTEM DESCRIPTION

The E-2D Advanced Hawkeye is a carrier-based, airborne tactical command and control platform that enables offensive and defensive carrier strike group tactics including airborne early warning. Its sensors and communications systems are designed to detect, track, and identify air and surface targets in blue-water, littoral, and overland environments. The following subsystems and capabilities enable the Advanced Hawkeye to perform its mission:

- AN/APY-9 phased array radar that combines mechanical and electronic scan modes
- Tactical Targeting Network Technology (TTNT) data link
- Multifunctional Information Distribution System (MIDS)
- Cooperative Engagement Capability (CEC)
- Communications suite
- Electronic support measures
- Electronic protection
- Aerial refueling

The E-2D Advanced Hawkeye Program also includes all simulators, interactive computer media, and documentation to conduct maintenance, as well as aircrew initial and follow-on training.

MISSION

The E-2D Advanced Hawkeye provides all-weather, airborne early warning, airborne battle management, and command and control functions, and supports Naval 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 counterair 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 it incorporates the TTNT data link. During OT-D4, the Navy is assessing DSSC-4 upgrades and the Hawkeye Integrated Training System. DSSC-4 serves as the baseline integration of capabilities that the Navy plans to fully deliver in DSSC-5 and later upgrades.

IT, which started in FY22, continued through the first half of FY23. The Navy conducted a DSSC-4 operational test readiness review in January 2023 but delayed the start of OT to correct critical software deficiencies. OT commenced in May 2023. The Navy began upgrading fleet aircraft to the DSSC-4 configuration in 3QFY23 to support an FY24 operational deployment.

The current Test and Evaluation Master Plan (TEMP) Revision F covers DSSC-4 and the follow-on upgrade, DSSC-5. The Navy is working on a TEMP update to address changes in the planned capabilities of DSSC-5, which is scheduled to begin OT in 4QFY24.

The TEMP presents a modeling and simulation (M&S) framework for developing and testing DSSC capabilities using the E-2D Systems Test and Evaluation Laboratory (ESTEL). The Navy intends to certify ESTEL capabilities in an incremental fashion; however, as of this writing, the ESTEL is not accredited for use during OT.

» MAJOR CONTRACTOR

- Northrop Grumman Aeronautics Systems – Melbourne, Florida

TEST ADEQUACY

The evaluation of DSSC-4 will occur through a cumulative collection of IT and OT data. The evaluation will determine fielding risks and delivered capabilities for DSSC-4.

In FY23, the Navy conducted DSSC-4 IT and OT in accordance with DOT&E-approved data collection and operational test plans; DOT&E observed the testing. To maximize data collection opportunities in operationally representative environments, the Navy largely

used an enterprise testing approach that incorporated test events from other programs. IT and OT leveraged two Aegis Combat Systems Ship's Qualification Trials (CSSQT) at the Point Mugu Sea Range, California; an Aegis CSSQT at the Atlantic Test Ranges, Maryland; and the joint force, GRAY FLAG exercise at Point Mugu, California. In addition, the Navy conducted dedicated OT flights on the Atlantic Test Ranges using an Aegis land-based test site at Wallops Island, Virginia.

In December 2022, the Navy conducted a DSSC-4 cyber survivability test at Patuxent River, Maryland. That test included a cooperative vulnerability and penetration assessment (CVPA) and an adversarial assessment (AA).

In 4QFY23, the Navy conducted DT on the DSSC-4 Hawkeye Integrated Training System in Sterling, Virginia. OT for this system is expected to take place in 2QFY24.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Not enough data are yet available to evaluate DSSC-4's operational effectiveness and suitability. Shortfalls in DSSC-4 systems maturity, aircraft availability, and test resource availability have slowed the collection of adequate data during OT-D4. Although reliability, maintainability, logistics, and availability data collection is still in progress, DOT&E observed that the overall rate at which DSSC-4 test aircraft were available and capable of executing IT and OT was lower than that required to execute the test schedule in the data collection and test plans. As the E-2D's OT environment often requires large, complex test events incorporating external systems of systems, the Navy should address E-2D availability and reliability challenges to maximize the efficiency of these events.

Data analyses from the cyber survivability CVPA and AA tests are ongoing.

DOT&E will provide an assessment of DSSC-4 after OT is complete.

RECOMMENDATIONS

The Navy should:

1. Continue to leverage large-force exercises and Navy Aegis test events to maximize E-2D OT data collection opportunities in operationally representative environments.
2. Increase aircraft availability and reliability in operational test to facilitate efficient execution of large, complex test events.
3. Develop a TEMP update to address planned DSSC-5 capabilities not covered in the current TEMP Revision F.
4. Accredit the ESTEL for use during OT of future DSSC builds.

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

F/A-18 Infrared Search and Track (IRST) Block II is on track to begin operational testing in 2QFY24 as stated in the DOT&E FY22 Annual Report. During FY23, the IRST Block II program made strides towards resolving open deficiencies from previous versions throughout the developmental test (DT) phase. Additionally, updated pod software fixed outstanding anomalies that affected operational suitability. To be operationally effective, the IRST Block II program needs to continue to discover and fix deficiencies during Block II DT in order to produce the intended fleet-releasable software and hardware to begin IOT&E. The proposed schedule allows minimal time for problem discovery and deficiency resolution prior to the planned start of IOT&E in 2QFY24. The Navy did not conduct operational test events during FY23.

SYSTEM DESCRIPTION

The ASG-34A(V)1 F/A-18E/F IRST is a centerline-mounted pod with a long-wave infrared sensor that provides a passive fire-control system intended to search, detect, track, and engage airborne targets at long range. The IRST sensor assembly integrates onto the front of the redesigned FPU-13/A centerline fuel tank assembly. The fuel capacity of the FPU-13/A is 340 gallons compared to the 480-gallon FPU-12/A centerline fuel tank it replaces. The IRST acts as a complementary sensor to the aircraft's AN/APG-79 fire control radar in a heavy electronic attack or radar-denied environment. It operates autonomously, or in combination with other sensors, to support the guidance of beyond-visual-range air-to-air missiles.

MISSION

The F/A-18E/F Super Hornet will employ the IRST Block II as a complementary long-wave infrared sensor to the AN/APG-79 fire control radar in a heavy electronic attack or radar-denied environment. IRST Block II provides passive search, detect, track, and engage capabilities against airborne targets at long range and will support the guidance of beyond-visual-range air-to-air missiles, including the AIM-120 Advanced Medium-Range Air-to-Air Missile and AIM-9X Sidewinder Block II.

PROGRAM

The F/A-18 IRST Block II is an Acquisition Category IC program. DOT&E approved the Milestone C Test and Evaluation Master Plan in May 2021. DT was conducted during FY23, and 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
- Boeing Defense, Space & Security – St. Louis, Missouri

TEST ADEQUACY

The Navy plans to conduct IOT&E between January and July 2024 and has not yet submitted the IOT&E plan to DOT&E for approval. An operational test readiness review is expected in 1QFY24.

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 discovered during Block II DT of prototype systems. Additionally, the Navy must improve the F/A-18E/F Super Hornet's operating software and correct existing deficiencies to enable IRST to be an effective contributor to aircraft fire control solutions. During FY23, IRST Block II developmental flight test events demonstrated tactically relevant detection ranges against operationally relevant targets and upgraded F/A-18E/F software demonstrated the ability to translate these long-range target detections into stable system tracks to facilitate weapons employment. The ability of the Navy to continue to fix outstanding critical issues on schedule is the most significant performance risk towards achieving an adequate IOT&E.

» SUITABILITY

IRST Block II demonstrated reliability issues below the Navy's requirements early in DT, but software improvements have increased pod reliability during FY23 DT events. Production-representative versions of the system are slated to be delivered prior to the start of IOT&E to determine system suitability. DOT&E will assess suitability based on operational test data at the completion of IOT&E in FY24.

» 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 operationally representative threat environment.

Cyber survivability testing is slated for 1QFY24.

RECOMMENDATIONS

The Navy should:

1. Continue to address the known IRST Block II and Super Hornet operating software deficiencies.
2. Continue to test unproven Block II DT system capabilities to support an adequate assessment of operational effectiveness, suitability, and survivability during IOT&E.
3. Develop and submit an adequate IOT&E test plan to accommodate a 1QFY24 operational test readiness review with DOT&E.

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

Both the F/A-18E/F Super Hornet and EA-18G Growler programs continue to experience development challenges in the latest software configuration set (SCS) updates. The Navy stopped SCS H16 operational testing during 4QFY22 due to severe software deficiencies, but still fielded the system to the operational fleet in FY23 without completing the DOT&E-approved FOT&E test plan. The Navy completed integrated test events for SCS H18, which provided relevant findings, but no significant data were provided. The Navy did not conduct SCS H18 FOT&E as planned in FY23. In March 2023, the Navy decided to test and issue SCS H18 in three releases. Release 1 was released to the fleet in April 2023 without conducting operational test events. The Navy fielded SCS H18 Release 1 prior to conducting FOT&E to support Long Range Anti-Ship Missile (LRASM) 1.1 capabilities. DOT&E provided early fielding reports (EFRs) for SCS H16 and H18 in response to the Navy's fielding decisions. In August 2023, the Navy conducted an operational test readiness review (OTRR) for SCS H18 Release 2, which is designed to enable Next-Generation Jammer–Mid Band capability in the EA-18G Growler, but it was not approved to conduct FOT&E due to severe software deficiencies. SCS H18 Release 3 is scheduled for OTRR and FOT&E in 3QFY24.

SYSTEM DESCRIPTION

The F/A-18E/F Super Hornet is a twin-engine, supersonic, all-weather, carrier-capable, multirole combat aircraft performing a variety of roles, including air superiority, fighter escort, suppression of enemy air defenses, reconnaissance, forward air control, close and deep air support, day and night strike, and aerial refueling. The F/A-18E/F Super Hornet is the replacement for the F/A-18A through D and the F-14, and it complements the F-35C in a carrier environment. The F/A-18E/F Block III Super Hornet aircraft leverages ongoing production of the Kuwaiti Super Hornet; it is also available as a Block II aircraft retrofit. F/A-

18E/F Block III Super Hornets include upgraded hardware, advanced cockpit displays, and improved networking capability.

The EA-18G Growler is a two-seat, electronic attack variant of the F/A-18E/F Super Hornet that can provide standoff, escort, and self-protection jamming using both noise and deception techniques against land/surface-based and airborne radar systems. The EA-18G Growler carries up to five AN/ALQ-99 tactical jammer system pods mounted under the wings and fuselage, which integrate with the internal AN/ALQ-218 electronic warfare (EW) 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 (NGJ-MB) 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 a mix of SCS H14, H16, and the most recent H18. SCS H18 brings improved capabilities to the APG-79 radar for both aircraft, 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 Electronic Attack 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-18 Super Hornet and EA-18G Growler now share the same acquisition strategy for SCS H18. The F/A-18E/F Super Hornet is an Acquisition Category IC program and the EA-18G Growler is an Acquisition Category ID program. Urgent fleet capability needs are driving the Navy's acquisition strategy for tactical aircraft SCS.

In the FY22 Annual Report, DOT&E stated that the Navy was conducting SCS H16 operational testing. Due to severe software deficiencies, operational testing of SCS H16 stopped, and the Navy began to develop urgent F/A-18E/F and EA-18G SCS capabilities for follow-on SCS releases. Although the program completed two more SCS H16 integrated test events to prove system stability, the Navy still fielded SCS H16 in FY23 without completing FOT&E per the DOT&E-approved Test and Evaluation Master Plan (TEMP) and the FOT&E test plan. DOT&E published an SCS H16 EFR in response to the Navy's fielding decision in September 2023.

In the FY22 Annual Report, DOT&E stated that SCS H18 FOT&E was scheduled to begin during 3QFY23, but system deficiencies caused program delays. The Navy's acquisition strategy for SCS H18 is an incremental three-part test-and-release plan to support the urgent fleet needs for the LRASM 1.1 on the F/A-18E/F Super Hornet and NGJ-MB on the EA-18G Growler. In February 2023, the Navy completed integrated test events for SCS H18 Release 1, but no significant data were generated for DOT&E assessment. In April 2023, the Navy fielded SCS H18 Release 1 to support LRASM 1.1 fielding without a DOT&E-approved TEMP, FOT&E test plan, and without conducting operational test events. In August 2023, DOT&E provided an SCS H18 Release 1 EFR in response to the Navy's fielding decision. DOT&E received and approved the SCS H18 TEMP in June 2023. DOT&E has not yet approved an SCS H18 operational test plan for Release 2 due to concerns about severe system deficiencies that will affect operational test adequacy. The Navy plans to test and field SCS H18 Release 3 in FY24.

SCS H18 includes EW and radar enhancements from SCS H16,

along with weapons integration software for LRASM 1.1, Small Diameter Bomb II, Advanced Anti-Radiation Guided Missile-Extended Range, and Joint Advanced Tactical Missile for the F/A-18E/F Super Hornet.

» MAJOR CONTRACTORS

- Boeing Defense, Space & Security – St. Louis, Missouri
- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Forest, Mississippi
- GE Aerospace, a subsidiary of General Electric – Evendale, Ohio
- Northrop Grumman Aeronautics Systems – Bethpage, New York
- Lockheed Martin Missiles and Fire Control – Orlando, Florida

TEST ADEQUACY

SCS H16 operational testing with the F/A-18E/F Super Hornet and EA-18G Growler was inadequate. The DOT&E-approved operational test plan was not completed prior to fielding the system in FY23; therefore, DOT&E was unable to assess the operational effectiveness, suitability, and survivability of SCS H16.

SCS H18 Release 1 operational testing was also inadequate. The program submitted a limited scope TEMP in January 2023, which DOT&E did not approve because it did not outline the overall H18 test strategy. DOT&E received and approved an updated TEMP in June 2023, but the Navy had already fielded SCS H18 Release 1 after conducting integrated test events. The Navy fielded Release 1 to operational fleet squadrons in April 2023 without a DOT&E-approved TEMP, FOT&E test plan, or conducting dedicated operational testing.

The F/A-18E/F Super Hornet and EA-18G Growler programs conducted an OTRR in August 2023 for SCS H18 Release 2. The OTRR revealed severe system deficiencies that could impact operational test adequacy and DOT&E did not approve the program to conduct FOT&E. The Navy completed several SCS H18 Release 2 integrated test events in August 2023 after DOT&E required the program to correct the severe system deficiencies and conduct a Delta-OTRR to show system maturity for FOT&E approval. However, the Delta-OTRR was not conducted and SCS H18 FOT&E was not conducted during FY23. The Navy plans to make the SCS H18 Release 2 fielding decision in October 2023.

The Navy plans to test and field SCS H18 Release 3 during FY24 as part of the incremental release plan. DOT&E received an FOT&E test plan for Release 3 but did not approve the test plan due to the same severe system deficiencies affecting previous SCS versions that could affect test adequacy. The program intends to conduct an H18 Release 3 OTRR in FY24 as the system matures.

The Navy has not yet submitted an H18 cyber survivability test plan to DOT&E.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

The Navy did not complete the DOT&E-approved SCS H16 FOT&E test plan and operational test data were not provided to DOT&E. Therefore, DOT&E did not assess SCS H16 effectiveness, suitability or survivability for the F/A-18E/F or EA-18G in FY23 as planned.

Although the program did complete integrated test events for SCS H18 Release 1, no significant data was generated for analysis and SCS H18 Release 1 FOT&E was not conducted. SCS H18 Release 2 OTRR revealed severe system deficiencies that could impact operational test adequacy as an outcome. DOT&E did not approve the program to conduct FOT&E, but the Navy did conduct integrated test events for SCS H18 Release 2. No significant data were generated by the integrated test events for analysis; therefore, DOT&E will provide an assessment of SCS H18 operational effectiveness, suitability, and survivability at the conclusion of an approved SCS H18 Release 3 FOT&E.

RECOMMENDATIONS

The Navy should:

1. Cease fielding subsequent versions of SCS H18 until all severe deficiencies, which are a risk to adequate operational test, aircrew safety, and aircrew ability to perform assigned missions, are remedied.
2. Conduct an OTRR of SCS H18 after developmental testing verifies corrections to severe software deficiencies that may affect operational test.
3. Complete dedicated operational testing of SCS H18 to assess operational effectiveness, suitability, and survivability prior to fielding subsequent versions.
4. Submit an H18 cyber survivability test plan to DOT&E for approval.
5. Address the two recommendations from the FY22 DOT&E Annual Report that are still outstanding.
6. Improve the reliability of the APG-79 Active Electronically Scanned Array (AESA) radar, as recommended in the FY22 Annual Report.
7. Continue to incorporate Open Air Battle Shaping and high-fidelity AESA threat radar emulators into SCS H18 FOT&E.

FFG 62 *Constellation*-Class Guided-Missile Frigate

In March 2023, DOT&E published a classified early operational assessment (EOA) report for the FFG 62 *Constellation*-class guided-missile frigate. The report identifies FFG 62 design risks to operational effectiveness and opportunities for design changes to mitigate the associated risks in the delivered ship. The FFG 62 Program expects delivery of the lead ship in 1QFY27.

SYSTEM DESCRIPTION

The FFG 62 class 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 the FFG 62 class include:

- Aegis Combat System
- AN/SPY-6(V)3F Enterprise Air Surveillance Radar
- AN/SLQ-32(V)6 Surface Electronic Warfare Improvement Program Block 2
- 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

- Thales Combined Active Passive Towed Array Sonar-4 (CAPTAS-4), a variable depth sonar not previously used by U.S. ships
- 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 FFG 62-class ships 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

FFG 62 is an Acquisition Category IB major capability 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 10 additional ships, and entry into the detail design and construction (production) phase with a low-rate initial production quantity of 20 ships. The FFG 62 Program intends to deliver the lead ship by December 2026.

In June 2020, DOT&E approved the FFG 62 Test and Evaluation Master Plan (TEMP), except for the strategy for testing its anti-air warfare (AAW) mission capability. DOT&E agreed to provide the Navy opportunity to show the adequacy of their proposed AAW test strategy. The Navy is in the process of collecting data that they believe supports this proposed strategy.

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 – Marinette, Wisconsin

TEST ADEQUACY

In March 2023, DOT&E published a classified FFG 62 EOA report based on evaluations conducted between February 2022 and July 2022 and detailed in the FY22 Annual Report. Evaluations were adequate to determine potential FFG 62 design risks that could affect operational effectiveness and suitability of the delivered ship. The EOA provides the FFG 62 Program with an opportunity to consider modifications to the ship design. The FFG 62 Program will also use the EOA to inform development of the next TEMP revision expected to be completed in FY25. The Navy conducted the EOA in accordance with a DOT&E-approved test plan, and it was observed by DOT&E.

In FY23, the Navy conducted testing against a large scale-model of a generic ship incorporating characteristics typical of Navy standard ship structure and a responding mid-deck plate to generate response data for underbottom explosions. This test was similar to the test detailed in the FY22 Annual Report but focused on different structure response. Data from these tests provide validation data for survivability models used to predict the magnitude and extent of damage from underwater threat weapons. The Navy conducted this test in accordance with the DOT&E-approved test plan, and it was observed by DOT&E.

In FY23, the FFG 62 Program approved the FFG 62 Verification, Validation, and Accreditation (VV&A) Plans for the Advanced

Survivability Assessment Program (ASAP) and Navy Enhanced Sierra Mechanics (NESM) M&S tools. These plans are adequate to determine the sufficiency of these M&S within the LFT&E test strategy. Further, the Navy continued M&S modification that incorporates new capabilities, including improvements in the blast and whipping codes. The Navy is working closely with DOT&E on the development of M&S plans to support the Detail Design Survivability Assessment Report that the FFG 62 Program expects to publish in FY26.

PERFORMANCE

» EFFECTIVENESS

No data are available to determine FFG 62 operational effectiveness due to FFG 62 being in development. However, the FFG 62 design presents risks to operational effectiveness in each of its primary mission areas: air warfare, anti-submarine warfare, and surface warfare. Classified risks to operational effectiveness are in the FFG 62 EOA report. Unclassified risks to operational effectiveness include that the FFG 62 design does not have a tracker illuminator system, which is typically installed on other Aegis platforms, and that the design crew size will be highly reliant on currently unproven system automation and human system interfaces. The Navy acknowledges the risk of the current crewing strategy for FFG 62 and is working with the appropriate stakeholders to mitigate and eliminate the associated risk to mission performance. Further, the FFG 62 Program reports that they currently have sufficient access to technical information on the Thales CAPTAS-4 needed to effectively integrate it with the AN/SQQ-89(V)16 system.

» SUITABILITY

No data are available to determine FFG 62 operational suitability due to FFG 62 being in development. Further, reliability, maintainability, and availability data for hull, mechanical, and electrical systems are not yet available to identify associated risk in the FFG 62 design.

» SURVIVABILITY

No data are available to determine the cyber survivability of FFG 62 due to its early stage of development. Cyber survivability was not assessed during the EOA.

Insufficient data are available to determine FFG 62 survivability due to ongoing LFT&E. The Navy continued to close outstanding vulnerability knowledge gaps and support validation of survivability M&S through additional large-scale underwater explosion testing in FY23.

RECOMMENDATIONS

The Navy should:

1. Provide an update to the FFG 62 TEMP that includes the strategy to test anti-air warfare mission capability.
2. Continue to monitor the development of the mission system autonomy/ automation components in the ship design to minimize risk to mission performance and system maintenance capability, and if necessary, complete a reassessment of the adequacy of crew sizing to allow opportunity to incorporate modifications of the ship design, should additional crewing be required to support all intended missions.

LHA 6 Flight 0/Flight 1 Amphibious Assault Ship

In February 2023, DOT&E published an FOT&E report on the LHA 6 Flight 0 Amphibious Assault Ship. The report details LHA 6 Flight 0 capability to support Marine Corps aviation operations with 20 F-35Bs embarked in the F-35B-heavy configuration. LHA 6 Flight 0 remains operationally suitable for amphibious warfare and standard Aviation Combat Element (ACE) operations. As stated in the last two Annual Reports, the LHA 6 program still needs to provide an updated LFT&E strategy for LHA 6 Flight 1.

SYSTEM DESCRIPTION

The LHA 6 class are large-deck amphibious assault ships intended to provide transportation and operational support for deployed Marine Corps forces, aircraft squadrons (including F-35B, AV-8B, MV-22, CH-53, AH-1, UH-1, and H-60 squadrons), and the Marine Air Ground Task Force. The class has two variants, referred to as Flights. The LHA 6 Flight 0, commencing with USS *America* (LHA 6), maximizes aviation capability (i.e., flight deck and hangar deck) and includes no well deck. The LHA 6 Flight 1, commencing with USS *Bougainville* (LHA 8), reduces aviation capability to support a well deck capable of deploying two Landing Craft Air Cushion hovercraft. The LHA 6 class (both

Flights) 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 LHA 6-class ships as the primary command ship and aviation platform for an Amphibious Ready Group or Expeditionary Strike Group and associated Marine Expeditionary Unit/Marine Air-Ground Task Force.

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 FOT&E in FY22, and DOT&E submitted the reports in April 2019 and February 2023, respectively. The Navy completed an operational assessment of the LHA 6 Flight 1 design, and DOT&E submitted a report in September 2021. The Navy continues to revise the Test and Evaluation Master Plan (TEMP) to include the test strategy and resources for OT&E and LFT&E of LHA 6 Flight 1 and now expects to deliver it to DOT&E for approval in FY24. The LHA 6 program expects to deliver USS *Bougainville* (LHA 8) in FY26 and subsequently conduct FOT&E and LFT&E.

» MAJOR CONTRACTOR

- Ingalls Shipbuilding, a division of HII (formerly Huntington Ingalls Industries) – Pascagoula, Mississippi

TEST ADEQUACY

In February 2023, DOT&E published an LHA 6 Flight 0 FOT&E report based on evaluation conducted between March and April 2022 on USS *Tripoli* (LHA 7), as detailed in the FY22 Annual Report. Testing was adequate to demonstrate LHA 6 Flight 0 capability to support Marine Corps aviation operations in the F-35B-heavy configuration consisting of 20 F-35B 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 LHA 6 program 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. The LHA 6 program plans to use test observations to inform future F-35B-heavy operational concepts and tactics, techniques, and procedures.

As first reported in the FY21 Annual Report, DOT&E and the LHA 6 program have yet to agree on an LHA Flight 1 LFT&E strategy to evaluate the survivability of the LHA 6 Flight 1 against air-delivered or underwater kinetic threats. Specific DOT&E concerns are the lack of fire testing for embarked vehicle spaces and the lack of a Full Ship Shock Trial.

PERFORMANCE

» EFFECTIVENESS

LHA 6 Flight 0 ships are operationally effective in supporting Marine Corps aviation operations in the F-35B-heavy configuration. USS *Tripoli* demonstrated the capability to conduct representative flight operations with 20 embarked F-35Bs throughout two days of mission exercises. USS *Tripoli* supported reliable launch and recovery of the F-35B. The Navy also demonstrated sufficient capability to conduct casualty control in the F-35B-heavy configuration during the simulated events of an aircraft fire on the flight deck and in the hangar of an LHA Flight 0 ship.

LHA 6 Flight 0 ships have limited special access program facility (SAPF) capacity, degrading the planning and execution of real-world missions with sustained operations in the F-35B-heavy configuration. Full details are in the LHA 6 Flight 0 FOT&E report.

» SUITABILITY

LHA 6 Flight 0 is operationally suitable for amphibious warfare and standard ACE operations. USS *Tripoli* experienced no material issues and demonstrated sufficient reliability to support strike and defensive counter air missions in the F-35B-heavy configuration.

Additionally, the ship's command, control, and communications systems were sufficient to support the demonstrated missions. Full details are in the LHA 6 Flight 0 FOT&E report.

The embarkation of an F-35B-heavy ACE created crewing requirements that exceeded the 12-hour routine operations. The Navy will likely need to develop a crewing plan for supplementing the ship's crew when operations exceed 12 hours with the embarkation of an F-35B-heavy ACE.

» SURVIVABILITY

No data are available to change the survivability assessment of LHA 6 Flight 0 from IOT&E or assess survivability of LHA 6 Flight 1.

RECOMMENDATIONS

The Navy should:

1. Investigate SAPF space options that support sustained operations with an F-35B-heavy ACE embarked. If SAPF space cannot be increased to support mission requirements, the Navy and Marine Corps should investigate the feasibility of relaxing the requirement for the SAPF as necessary to support F-35B operations.
2. Investigate supplemental crewing options for sustained LHA 6 Flight 0 operations with an F-35B-heavy ACE embarked.
3. As recommended in the last two Annual Reports, deliver the LHA 6 Flight 1 LFT&E strategy for DOT&E approval in FY24. Identify funding in the updated TEMP for embarked vehicle fire testing and a Full Ship Shock Trial.

USS America *(LHA 6) in the Coral Sea during Exercise TALISMAN SABRE, July 2023*

Littoral Combat Ship (LCS)

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

In March 2023, the Navy declared initial operational capability of the *Independence*-class Littoral Combat Ship (LCS) Mine Countermeasures (MCM) Mission Package (MP); however, IOT&E is not complete. In June 2023, DOT&E released a classified cyber addendum to its published *Freedom*-class LCS Surface Warfare (SUW) MP Increment 3 IOT&E report from July 2020.

SYSTEM DESCRIPTION

The LCS is a small surface combatant designed for littoral operations and capable of executing open ocean missions. The LCS comprises two seaframe variants: the *Freedom* variant (odd-numbered) and the *Independence* variant (even-numbered). The *Freedom* variant is a monohull design constructed of steel (hull) and aluminum (deckhouse) with two steerable and two fixed-boost waterjets driven by a combined diesel and gas turbine main propulsion system. The *Independence* variant is an aluminum trimaran with two steerable waterjets driven by diesel engines and two steerable waterjets driven by gas turbine engines. LCS seaframes host and derive mission capability from the SUW and MCM MPs.

The SUW MP is now scheduled to deploy only on the *Freedom*

class and derives its capability from the following components:

- Two Mk 46 30mm guns
- MH-60R or MH-60S helicopter
- MQ-8 Fire Scout Vertical takeoff and landing Tactical Unmanned Aerial Vehicle
- Two 11-meter rigid-hull inflatable boats
- Surface-to-Surface Missile Module with 24 Longbow Hellfire missiles

The MCM MP is now scheduled to deploy only on the *Independence* class and derives its capability from the following baseline components:

- AN/ASQ-235 Airborne Laser Mine Detection System (ALMDS) employed from an MH-60S helicopter
- Airborne Mine Neutralization System (AMNS) employed from an MH-60S helicopter
- MCM Unmanned Surface Vehicle (USV) with Minehunt Payload (MCM USV and Minehunt) and the AN/AQS-20C sonar
- Unmanned Influence Sweep System (UISS)

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 I system employed from an MQ-8C Fire Scout
- Barracuda Mine Neutralization System employed from MCM USV

MISSION

The maritime component commander will employ LCS alone, or within a group of ships, to prepare the environment for joint forces access to littoral regions by conducting MCM or SUW operations, possibly under an air defense umbrella. Because of capabilities inherent to both seaframes, commanders can also employ LCS in a maritime presence role and support deterrence operations. Further, the Maritime Security Module of the SUW MP enables the *Freedom* class to conduct Maritime Security Operations including visit, board, search, and seizure of ships suspected of transporting contraband.

PROGRAM

The LCS seaframes and the combined MPs are each Acquisition Category IC programs. Additionally, several components within the MPs are themselves individual programs of record. In FY23, one *Independence*-class ship and one *Freedom*-class ship were delivered. The Navy expects the remaining two *Independence*-class and three *Freedom*-class ships to deliver between FY24 and FY25. In FY23, 3 MCM MPs and 3 SUW MPs were delivered with the remaining 21 MCM MPs expected between FY24 and FY33 and the remaining 5 SUW MPs expected in FY24.

In March 2023, the Navy declared initial operational capability of the MCM MP and the AN/AQS-20C sonar. The Navy intends to make a full-rate production decision on AN/AQS-20C in FY24 after the completion of IOT&E and then begin deployment of the MCM MP.

In 2018, DOT&E approved an update to the LCS Test and Evaluation Master Plan (TEMP) that accounted for changes in the test designs for evaluating the MPs on the two seaframe variants. In FY23, the Navy intended to update the LCS TEMP to address additional changes in the test program for the LCS MCM MP and for the Navy's divestment in the LCS Anti-Submarine Warfare (ASW) MP. However, the Navy delayed the update to FY24.

In January 2023, DOT&E approved the MCM USV and Minehunt TEMP. MCM USV and Minehunt are detailed in the AN/AQS-20X Minehunt Sonar and Tow Vehicle article of this Annual Report.

» MAJOR CONTRACTORS

- Lockheed Martin Corporation and Fincantieri Marinette Marine team – Marinette, Wisconsin
- Austal USA – Mobile, Alabama
- Northrop Grumman Corporation – Falls Church, Virginia

TEST ADEQUACY

The Navy conducted no operational testing on the *Freedom* class with the SUW MP Increment 3 in FY23. DOT&E completed analysis of cyber test events reported in the FY22 Annual Report

in June 2023 and submitted a classified cyber addendum to the IOT&E report for the *Freedom* class with the LCS SUW MP Increment 3. Testing was adequate to determine cyber survivability. The Navy has no follow-on testing planned for the *Freedom* class with the LCS SUW MP Increment 3.

The Navy conducted no operational testing on the *Independence* class with the LCS MCM MP in FY23. Testing remains inadequate to determine operational effectiveness because the Navy has yet to provide required data to determine the performance of the AMNS and ALMDS components of the LCS MCM MP. DOT&E cannot provide an IOT&E report without these data as they are primary contributors to the MCM mission.

The Navy scheduled evaluation of the cyber survivability of the *Independence* class with LCS MCM MP for FY24, a one-year delay from what was reported in last year's Annual Report. This test and sufficient data on the AMNS and ALMDS are needed to complete IOT&E.

PERFORMANCE

» EFFECTIVENESS

DOT&E's classified July 2020 LCS with Increment 3 SUW MP IOT&E report contains details on effectiveness of the *Freedom*-class LCS with the SUW MP Increment 3.

No determination of the operational effectiveness of the *Independence* class with the LCS MCM MP can be made due to the IOT&E not being complete.

» SUITABILITY

DOT&E's classified July 2020 LCS with Increment 3 SUW MP IOT&E report contains details on suitability of the *Freedom*-class LCS with the SUW MP Increment 3.

No determination of the operational suitability of the *Independence* class with the LCS MCM MP can be made due to the IOT&E not being complete. However, analysis of the available data on baseline components suggests that:

- UISS is not operationally suitable, as documented in the UISS IOT&E report dated June 2022. UISS's reliability and availability do not support sustained mine sweeping operations.
- AMNS and ALMDS are unlikely to have sufficient reliability. This assessment is based on limited data available for the classified DOT&E LCS MCM MP Early Fielding Report from June 2016, as no additional data are available.

» SURVIVABILITY

Cyber survivability of the *Freedom* class with LCS SUW MP to a nearsider or insider threat is classified and is detailed in the June 2023 DOT&E cyber addendum to the IOT&E report.

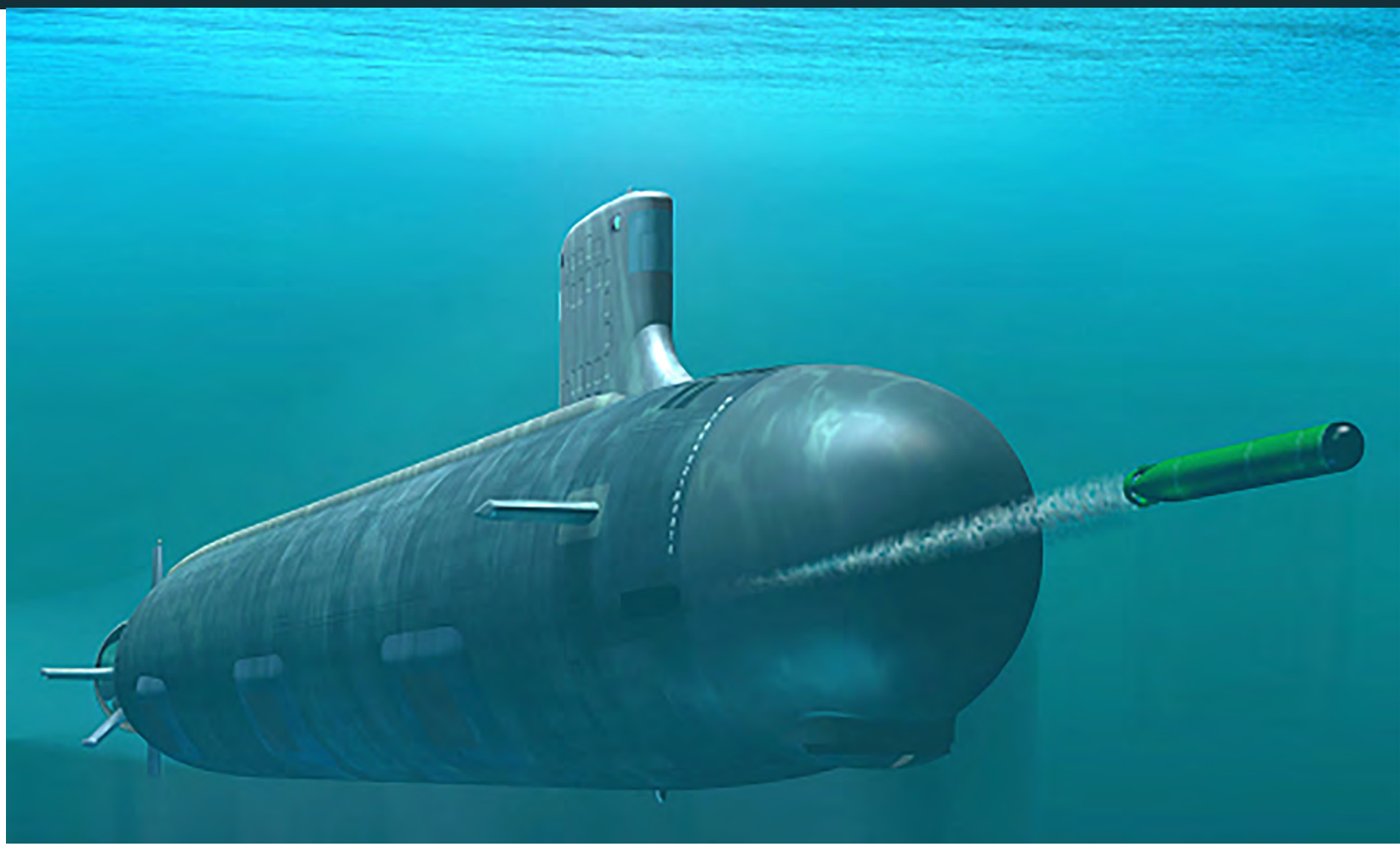
No data are available to determine cyber survivability of the *Independence* class with LCS MCM MP as the evaluation is scheduled for FY24.

RECOMMENDATIONS

The Navy should:

1. Submit an update to the *Independence*-class LCS MCM MP TEMP for DOT&E approval by 2QFY24 to support the Navy's planned cyber test in 4QFY24.
2. Complete operational testing of the *Independence*-class LCS MCM MP.
3. Provide data from fleet events to characterize performance of ALMDS and AMNS. If data are not available, plan additional test to obtain these data, as data are required to adequately test the LCS MCM MP capability.
4. Improve resilience of the *Freedom* class with the LCS SUW MP to cyberattack by addressing recommendations in the June 2023 DOT&E classified cyber addendum to the July 2020 IOT&E report.

Mk 48 Torpedo Modifications



The Navy ended operational test of the Mk 48 Mod 7 torpedo with Advanced Processor Build (APB) 5+ in May 2023. In August 2023, DOT&E submitted a classified FOT&E report that determined APB 5+ is operationally effective and suitable, though Mk 48 Mod 7 torpedo reliability has degraded below Navy-defined requirements. In FY23, the Navy commenced evaluation of an urgent software build for the APB 5 and APB 5+ torpedoes for which findings are expected in mid-FY24.

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 Mk 48 torpedo has hardware variants referred to as Mods. Each Mod represents a step improvement in capability, integrating upgraded sensors, guidance and control (G&C), and propulsion system hardware. Three Mods are in use in the fleet:

- Mod 6 integrated noise quieting in the propulsion section and commercial-off-the-shelf (COTS) electronics in the G&C section.
- Mod 6 Advanced Common Torpedo (ACOT) integrated additional COTS electronics in the G&C section.
- Mod 7 Common Broadband Advanced Sonar System upgraded the Mod 6 ACOT with a new sonar receiver.

The Mk 48 torpedo undergoes regular software updates referred to as APBs. APBs include modifications (e.g., tactics, classification algorithms, operator interface) intended to improve torpedo performance or simplify the operator interface. APBs can operate on various torpedo Mods with some variance in performance based on Mod hardware:

- APB 5 modifications focused on detection and discrimination of target submarines and surface ships. It also provided an alternative tactic against surface ships.
- APB 5+ modifications focused on simplifying the interface between the submarine's combat system and the torpedo. APB 5+ is limited to Mod 7 torpedo hardware and requires the employing submarine to have the AN/BYG-1 combat control system version APB-18/TI-19 or beyond.
- APB 6 is in development for delivery in FY26 with modifications that are focused on target detection and classification. APB 6 will support an upgraded sonar array being delivered in a Mk 48 Mod 8 variant that the Navy expects to deliver in FY28.

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 APB 5/5+, is an Acquisition Category III program and a shared development effort with the Royal Australian Navy.

The Navy completed operational testing in May 2023 and fielded APB 5+ in FY23. DOT&E submitted a classified FOT&E report in August 2023.

In 1QFY23, the Navy requested a software update for APB 5 and APB 5+ to address an urgent need torpedo capability, referred to as the Shallow Water Urgent Build (SWUB). The Navy conducted a limited in-water test in July and August 2023. DOT&E expects to submit a classified SWUB Early Fielding Report in mid-FY24.

The Navy is in engineering testing for APB 6 software and expects to begin operational testing in FY25 on the Mk 48 Mod 7 variant. APB 6 is being designed to support the future Mk 48 Mod 8 variant.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

The Navy completed operational test of APB 5+ in May 2023 with DOT&E concurrence. APB 5+ testing was adequate to assess operational effectiveness and suitability. Cyber survivability was not evaluated due to no expected change from the previous test on APB 5. The Navy executed all tests in accordance with DOT&E-

approved test plans; DOT&E attended most but not all test events due to COVID-19 travel restrictions. Assessment included the following tests detailed in the FY21 and FY22 Annual Reports:

- Live Virtual Construct testing that incorporated fleet operators, a representative combat system, and the Navy's Environment Centric Weapon Analysis Facility (ECWAF). This test characterized the warfighter utility of operational interface improvements.
- Modeling and simulation data using the ECWAF confirmed that APB 5+ modifications did not degrade its effectiveness against submarines when compared to APB 5.

The Navy completed in-water evaluation of APB 5+ in February 2023. Data were collected from 8 antisubmarine and 12 anti-surface warfare scenarios that occurred in one dedicated test event and three fleet training events. Data were sufficient to evaluate torpedo effectiveness and suitability.

The Navy conducted a test event in July 2023 that consisted of seven torpedo firings to evaluate the SWUB on APB 5 torpedoes. The Navy conducted a follow-on test event in August 2023 consisting of 11 torpedo firings with SWUB on APB 5 torpedoes. SWUB testing was adequate to evaluate a new feature provided by SWUB, but testing was not adequate to assess end-to-end performance of the intended mission because of limited threat representation.

Test adequacy of future APBs depends upon representative threats and threat capability surrogates. In August 2020, the Navy commenced development of the Towed Array Threat Emulator (TATE) that the Navy intends to use to improve the threat representation of the current surrogate for a mobile countermeasure, the Submarine Launched Acoustic Countermeasure Emulator (SLACE). In July 2023, the Navy commenced development of the Modular Threat Countermeasure Emulator (MOTCE) that the Navy intends to use to improve the threat representation for static countermeasures. The Navy plans to use the TATE and MOTCE in operational tests of future Mk 48 torpedoes in FY28.

The Navy intends to accredit the ECWAF to evaluate the effectiveness of Mk 48 Mod 7 APB 6 against both submarines and surface ships and reduce live tests by approximately half compared to the Mk 48 Mod 7 APB 5 live fire test shots that were part of IOT&E. Limited test in some ocean environments during recent torpedo variant testing may require fleet training and certification events to include these environments to provide sufficient live data for verification and validation. Additionally, the Navy must complete development of some surface ship and reverberation models intended for use in anti-surface warfare scenarios in the ECWAF.

PERFORMANCE

» EFFECTIVENESS

APB 5+ is operationally effective and provides an improvement in the operator interface between the combat system and torpedo. APB 5+ simplifies operator guidance provided to the torpedo prior to launch (i.e., torpedo presets) to include more intuitive safety features that protect ownship from the torpedo, and operator updates to the torpedo after launch. The Navy determined that some new features were less useful than those included in APB 5 and adjusted tactical guidance appropriately. Classified details are in the August 2023 FOT&E report.

Testing demonstrated that a specific SWUB feature operates as designed and that SWUB can improve single torpedo performance in the intended scenario given equivalent crew targeting. However, testing does not support comparison of performance to the legacy torpedo for an overall scenario with multiple torpedoes employed. DOT&E expects to submit a classified early fielding report in FY24.

» SUITABILITY

APB 5+ is operationally suitable. However, reliability of the Mk 48 Mod 7 torpedo is now below the Navy-defined requirement. Failure to correct reliability issues will lead to the Mk 48 Mod 7 torpedo (all APB variants) becoming not operationally suitable.

» SURVIVABILITY

The Navy did not complete a cyber survivability assessment of APB 5+ because results are unchanged from APB 5. APB 5+ remains not survivable to cyberattack with details in the classified April 2022 APB 5 IOT&E report.

RECOMMENDATIONS

The Navy should:

1. Address all recommendations in the classified April 2022 APB 5 IOT&E report and August 2023 APB 5+ FOT&E report.
2. Determine and correct causes of degraded reliability of the Mk 48 Mod 7 torpedo.
3. As recommended in FY22, 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.
4. Complete development and validation of surface ship models and reverberation models in the ECWAF and validate their intended use in Mod 8 APB 6 IOT&E.
5. Complete development of the TATE and MOTCE prior to Mod 8 IOT&E.
6. Continue to evaluate SWUB performance in FOT&E with a combination of in-water testing and modeling and simulation.

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

The Navy ended the Mk 54 Mod 1 Increment 1 IOT&E in October 2022 without completing many tests in the DOT&E-approved test plan. In April 2023, DOT&E published a classified IOT&E report that assessed the Mk 54 Mod 1 Increment 1 as operationally effective with no apparent degradation from the Mk 54 Mod 0 variant, but no assessment could be made about its performance in an acoustically challenging environment. The Mk 54 Mod 1 is not operationally suitable due to low reliability and availability.

The Navy conducted no operational test of the High Altitude Anti-Submarine Warfare (ASW) Weapon Capability (HAAWC) in FY23.

SYSTEM DESCRIPTION

The Mk 54 lightweight torpedo is the primary anti-submarine weapon employed from U.S. surface ships, aircraft, and helicopters. Navy convention is to designate the Mk 54 with Mods when significant changes are made to the Mk 54 hardware:

- Mod 0 is being phased out of existing inventories as they are converted to Mod 1.
- Mod 1 adds a new sonar array and processing hardware. Mod 1 has two increments:
  - Increment 1 incorporates Advanced Processor Build 5 software from the Mk 48 heavyweight torpedo program to improve target detection and discrimination.
  - Increment 2 will include additional updates focused on improving performance within a classified set of scenarios. Increment 2 has two phases of delivery:
    - Phase 1 introduces Advanced Processor Build 6 software to enable multi-band sonar processing.
    - Phase 2 includes hardware obsolescence upgrades needed to optimize performance with the new software.
- Mod 2 will incorporate a new warhead and engine to improve lethality, speed, endurance, and operating depth.

HAAWC is a combined Mk 54 torpedo and Air Launch Accessory

wing kit. P-8A aircraft operators can employ HAAWC from much higher altitudes than conventionally 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.

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 release or firing the Vertical Launch Anti-Submarine Rocket (VLA) 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 first fielded in 2004. Mk 54 Mod 1 is an Acquisition Category (ACAT) III program and Increment 1 entered full-rate production in April 2023. The Navy plans to submit a Test and Evaluation Master Plan (TEMP) update for Mod 1 Increment 2 in 2QFY25 and commence FOT&E in 1QFY26.

Mk 54 Mod 2 is an ACAT IB program and a joint development effort with Australia. DOT&E approved the Mod 2 Milestone B Joint TEMP in January 2023. The Joint TEMP requires set-to-hit in-water tests, but the Navy has yet to approve a method to conduct this testing. The Navy plans to begin IOT&E of Mod 2 in FY27.

The Navy has not approved the Mod 1 Increment 1 or Mod 1 Increment 2 for VLA missile applications.

The HAAWC is an ACAT III program and entered full-rate production in August 2022. DOT&E submitted classified IOT&E and FOT&E reports in June 2021 and July 2022, respectively. The HAAWC Air Launch Accessory and VLA missile will require redesigns to integrate the Mk 54 Mod 2 torpedo. The Navy requested proposals for a new HAAWC design from industry, with selection planned for late FY24.

» MAJOR CONTRACTORS

- Aerojet Rocketdyne, a subsidiary of L3Harris Technologies, Inc. – Huntsville, Alabama
- Boeing Defense, Space & Security – St. Charles, Missouri
- Northrop Grumman Corporation – Minneapolis, Minnesota
- Progeny Systems LLC, a subsidiary of General Dynamics Mission Systems – Manassas, Virginia
- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Portsmouth, Rhode Island

TEST ADEQUACY

The Navy ended the Mod 1 Increment 1 IOT&E in October 2022 without completing the DOT&E-approved test plan. IOT&E was adequate to evaluate performance in a limited set of scenarios, but not in the acoustically challenging environment of shallow water for which improvements were expected to have the greatest effect on torpedo performance. DOT&E observed the IOT&E test events and submitted a classified IOT&E report for Mod 1 Increment 1 in April 2023.

The Navy conducted two live fire tests between February and May 2023 to characterize the Mod 2 warhead performance and both were observed by DOT&E. Testing was planned and conducted as proof-of-design tests by the warhead design contractor.

Test adequacy of Mk 54 Mod 2 depends upon representative threats and threat capability surrogates. In August 2020, the Navy commenced development of the Towed Array Threat Emulator (TATE) that the Navy intends to use to improve the threat representation of the current surrogate for a mobile countermeasure, the Submarine Launched Acoustic Countermeasure Emulator

(SLACE). In July 2023, the Navy commenced development of the Modular Threat Countermeasure Emulator (MOTCE) that the Navy intends to use to improve the threat representation for static countermeasures. The Navy plans to use the TATE and MOTCE in operational tests of the Mk 54 Mod 2.

PERFORMANCE

» EFFECTIVENESS

The Mod 1 Increment 1 torpedo is operationally effective and showed no degradation in torpedo effectiveness from Mod 0. However, no assessment of performance could be made for the Mod 1 Increment 1 torpedo operating in an acoustically challenging environment. A detailed assessment is in the classified IOT&E report for Mod 1 Increment 1 dated April 2023.

» LETHALITY

Mod 1 torpedo lethality is addressed in the classified IOT&E report for Mod 1 Increment 1 dated April 2023. No assessment of Mod 2 warhead lethality can be made due to ongoing analysis.

» SUITABILITY

The Mod 1 Increment 1 torpedo is not operationally suitable due to low availability and reliability. Mod 1 torpedoes are more likely to shut down early compared to Mod 0. A detailed assessment is in the classified IOT&E report for Mod 1 Increment 1 dated April 2023.

» SURVIVABILITY

Assessment of cyber survivability of the Mod 1 Increment 1 torpedo is classified; details are in the classified IOT&E report for Mod 1 Increment 1 dated April 2023.

RECOMMENDATIONS

The Navy should:

1. Continue to address all recommendations in the classified FOT&E report for HAAWC and the classified IOT&E report for Mk 54 Mod 1 Increment 1.
2. Prioritize opportunities to test the Mod 1 Increment 2 torpedo in an acoustically challenging shallow water environment to estimate torpedo performance.
3. Identify and approve a method to conduct Mod 2 set-to-hit testing that supports the required determination of torpedo lethality and effectiveness in the Mod 2 IOT&E.

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

Since achieving Milestone B (MS B) in August 2018, a series of programmatic and technical delays led the MQ-25 program to request fiscal reprogramming in FY23. If the reprogramming request is granted, the Navy will update the MQ-25 acquisition strategy and submit an update of the MS B Test and Evaluation Master Plan (TEMP) to DOT&E.

SYSTEM DESCRIPTION

The MQ-25 Stingray Carrier-Based Unmanned Aerial System (CBUAS) is composed of the MQ-25A Stingray air vehicle (Group 5 unmanned aircraft system (UAS)) and the MD-5 Unmanned Carrier Aviation Mission Control System (UMCS). It is intended to enhance carrier air wing (CVW) warfighting capabilities as an organic, carrier-based mission and recovery tanker with a secondary maritime intelligence, surveillance, and reconnaissance (ISR) capability. MQ-25 will assume the organic tanking mission currently performed by the F/A-18E/F. MQ-25 is intended to integrate manned and unmanned operation and mature complex sea-based command, control, communication, computers, and intelligence UAS technologies to support future UAS development to pace emerging threats.

MISSION

Commanders will utilize the MQ-25 to provide tanking and ISR capabilities to the carrier strike group, extending CVW strike range and alleviating the persistent, sea-based ISR gap, while introducing and integrating organic unmanned aviation into the CVW.

PROGRAM

The MQ-25 CBUAS is composed of the MQ-25A Stingray air vehicle, an Acquisition Category IB program; the MD-5 UMCS, an Acquisition Category II program; and additional systems, capabilities, and facilities needed to enable operations. The MQ-25 will be the first operational, carrier-based, fixed-wing, catapult-launched UAS.

The MQ-25 MS B TEMP called for the MS C decision in FY23 to be informed by an operational assessment based on testing up to and including initial sea trials. In December 2022, based on production delays, the Navy issued an updated Acquisition Decision Memorandum which revised the MS C criteria to use information from an Early Operational Assessment (EOA) that would be based on data collected between June 2019 and December 2021 that utilized a Boeing-owned, -operated, and -funded MQ-25A Stingray prototype (pictured above).

The prototype test program was a 30-month, risk-reduction effort with ground and flight events executed at Mid-America Airport in Mascoutah, Illinois; ground events at Naval Air Station Norfolk, Virginia; and an underway (non-flight) deck-handling demonstration onboard USS *George H. W. Bush* (CVN 77) in December 2021 which concluded the program. While the prototype demonstrated in-flight refueling capability and was taxied under its own power on the flight deck, there are significant differences between the prototype and the MQ-25A Engineering Development Model design. These differences include internal structures, fuel system design, communications and network architecture, and for later test articles, obsolesce updates for some internal hardware that need to be incorporated before production model delivery. Additionally, the prototype was flown with a Boeing ground station, not the Lockheed Martin MD-5 UMCS ground station planned for use with fleet aircraft. At the time of testing, the Navy did not intend the prototype test program to inform an EOA, and DOT&E did not observe the testing. Developmental risk reduction activities are in progress at both Boeing-owned and government-owned software and hardware integration labs.

The Navy's Operational Test and Evaluation Force sent an EOA strategy to DOT&E which it assessed as inadequate. MS C did not occur in FY23 due to delays with MQ-25A Stingray production.

As a result of the design, production, and testing delays, the MQ-25 program is currently in the process of fiscal reprogramming to extend the engineering and manufacturing development phase of the program by approximately 24 months. Once reprogramming is approved and completed, the Navy will update the acquisition strategy and submit an update of the MS B TEMP to DOT&E. As of the end of FY23, the draft financial reprogramming plan and related budget marks did not meet the program's full RDT&E funding request, which adds risk to an aggressive test schedule.

» MAJOR CONTRACTORS

- Boeing Defense, Space & Security – St. Louis, Missouri (MQ-25A Stingray)
- Lockheed Martin Corporation – Marietta, Georgia (MD-5 UMCS)

TEST ADEQUACY

DOT&E has not approved any operational test plans for MQ-25.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

Not enough data are currently available to evaluate the MQ-25 operational effectiveness, suitability, and survivability.

RECOMMENDATION

The Navy should:

1. Submit an update to the MS B TEMP for DOT&E approval upon completion of an updated acquisition strategy.

MQ-4C Triton

In August 2023, DOT&E published a classified early fielding report (EFR) on the MQ-4C Triton to support a Navy fielding decision, also in August 2023. While the Navy conducted integrated testing of some capabilities to inform that decision, the MQ-4C Triton program did not enter IOT&E in FY23 due to immature systems that precluded operationally representative testing for the primary missions. The Navy fielded two aircraft and declared initial operational capability in July 2023, despite these immature systems.

SYSTEM DESCRIPTION

The MQ-4C Triton is a high-altitude, long-endurance intelligence, surveillance, and reconnaissance (ISR) unmanned aircraft intended to support global naval and joint operations by collecting, processing, and distributing geospatial intelligence (GEOINT), including imagery and track data, and signals intelligence (SIGINT) data to tactical and information operations centers.

MISSION

Commanders will employ the MQ-4C to provide persistent, broad-area ISR to detect, classify, identify, track, and assess maritime and littoral targets in support of surface warfare, intelligence operations, strike warfare, maritime interdiction, amphibious warfare, homeland defense, and search and rescue missions.

PROGRAM

The MQ-4C Triton is an Acquisition Category IC program and a critical component, along with the P-8A Poseidon, of the Navy's maritime ISR transition plan to retire the EP-3E Aries II. Section 112 of the FY11 National Defense Authorization Act prohibits the Navy from retiring or preparing to retire the EP-3E until it fields one or more platforms that, in the aggregate, provide an equivalent or superior capability.

The program is following an incremental development approach after restructuring in 2021. The first increment is designed for the Navy to deliver SIGINT capabilities sufficient to support the MQ-4C's portion of the maritime ISR transition plan. DOT&E approved Revision E of the Test and Evaluation Master Plan in January 2023. The Navy approved an updated acquisition strategy in August 2023. Operational Test and Evaluation Force (OPTEVFOR) published a classified interim report in July 2023. The Navy fielded two aircraft and declared initial operational capability in July 2023. DOT&E published a classified EFR in August 2023.

» MAJOR CONTRACTOR

- Northrop Grumman Corporation Aeronautics Sector – Rancho Bernardo, California

TEST ADEQUACY

As stated in the FY22 Annual Report, the Navy intended to enter IOT&E in January 2023. However, due to deficiencies in the SIGINT systems that precluded a stable configuration and operationally realistic testing, DOT&E did not approve the IOT&E plan in FY23. However, DOT&E did approve conduct of the GEOINT and cyber survivability portions of the test plan for integrated testing. OPTEVFOR conducted, and DOT&E observed, testing of the radar and electro-optical/infrared camera GEOINT sensors between January and June 2023 in accordance with the approved portions of the test plan.

As discussed in the FY22 Annual Report, the Navy does not have a method to extract all types of data from the Minotaur mission management system the operators use to control MQ-4C sensors, view sensor data, and build the common operating picture. OPTEVFOR was able to collect sufficient data to support a preliminary assessment of the operational effectiveness and suitability of the MQ-4C for GEOINT missions. However, immature systems prevented useful assessments of SIGINT capabilities and the Navy does not yet have a reliable method to collect SIGINT data from the Minotaur system. Also, the Navy has not yet fully implemented their tasking, collection, processing, exploitation, and dissemination plan for GEOINT and SIGINT data.

The program conducted contractor and developmental testing in the anechoic chamber at the Air Combat Environment Test and Evaluation Facility in July 2023. Analyses are in progress, including the analysis required to support the degraded or denied GPS testing discussed in the FY22 Annual Report.

OPTEVFOR has not yet conducted the approved cyber survivability assessment, which is scheduled for October 2023.

PERFORMANCE

» EFFECTIVENESS

The operational effectiveness of the MQ-4C for its primary SIGINT missions is unknown. The

system's GEOINT performance was qualitatively comparable to a previous configuration fielded as an early operational capability. Details are provided in DOT&E's classified MQ-4C EFR.

» SUITABILITY

The reliability, availability, and maintainability observed during integrated testing are not likely to sustain the planned operational tempo. Details are provided in DOT&E's classified MQ-4C EFR.

» SURVIVABILITY

The survivability of the MQ-4C in contested cyberspace is unknown; testing is planned to begin in October 2023.

RECOMMENDATIONS

The Navy should:

1. Develop a method to extract mission data from the Minotaur system, particularly for SIGINT mission data.
2. Complete the integrated test program and correct major deficiencies prior to proceeding into IOT&E.
3. Complete IOT&E to evaluate the operational effectiveness, suitability, and survivability of the system.
4. Complete development and implementation of the tasking, collection, processing, exploitation, and dissemination plan for MQ-4C mission data.

MQ-8C Fire Scout

The Navy conducted FOT&E of the MQ-8C Surface Warfare (SUW) Increment that included an interoperability test onboard a littoral combat ship (LCS) and a land-based radar characterization test during FY23. The Navy expects to complete FOT&E in FY24 following completion of cyber survivability evaluation. No preliminary assessment of operational effectiveness, suitability, and cyber survivability can be made due to ongoing test and analysis.

SYSTEM DESCRIPTION

The MQ-8C is a helicopter-based tactical unmanned aerial system designed to support intelligence, surveillance, and reconnaissance; surface warfare; and mine countermeasures payloads. The basic airframe is known as the Endurance Baseline Increment and is equipped with the AN/AAQ-22D BRITE Star II multi-sensor imaging system with Electro-Optic/Infrared cameras and laser range finding and target designation. The air vehicle is a modified Bell 407 airframe intended to support LCS missions.

The MQ-8C SUW Increment integrates the AN/ZPY-8 multi-mode active electronically scanned array (AESA) radar into the airframe, Minotaur software, and supporting air vehicle (AV) and mission control systems software. The AESA radar has maritime search, inverse synthetic aperture radar and synthetic aperture radar imagery capability.

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 MQ-8C 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 shipboard weapon systems as well as remote target designation for MH-60R/S helicopters.

PROGRAM

The MQ-8C Fire Scout is an Acquisition Category IC program that received Milestone C approval in FY17. The MQ-8C has three expected increments of capability: the Endurance Baseline Increment, the SUW Increment, and the Mine Countermeasure Increment. The current inventory is 36 aircraft with no additional procurement planned. DOT&E approved the Test and Evaluation Master Plan (TEMP) in February 2022.

President's Budget 2023 included a significant divestment within the MQ-8 program, resulting in the removal of all MQ-8B AVs from inventory and reduction of the MQ-8C AV active operational inventory. Currently there are 11 aircraft dedicated to operational employment with 3 allocated to test and training, an increase of 1 from last year's Annual Report. Projections for FY24 will increase the operational employment number to 15. The remainder are in a preservation status and are planned to be used for maintenance parts as necessary to support the pool of operational aircraft.

The Coastal Battlefield Reconnaissance and Analysis (COBRA) airborne mine detection system is currently in development for integration into the MQ-8C and requires a test strategy and associated test resources update to the MQ-8C TEMP.

» MAJOR CONTRACTOR

- Northrop Grumman Aeronautics Systems – San Diego, California

TEST ADEQUACY

The DOT&E-approved test plan includes two components: an at-sea component and a land-based component.

The Navy completed the at-sea component of the MQ-8C SUW Increment FOT&E in July 2023 in accordance with the DOT&E-approved test plan. Shipboard operations were conducted from an operational LCS during multiple embarkations. Test data are being evaluated to determine sufficiency for assessing interoperability of the MQ-8C SUW Increment with the LCS.

The Navy has yet to complete land-based testing necessary to characterize radar performance against maritime targets. The Navy expects to complete land-based testing in 1QFY24 at the Atlantic Test Range (ATR) facility using dedicated surface testing targets in the Chesapeake Bay.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Not enough data are available to provide an assessment of the

operational effectiveness and suitability of the MQ-8C SUW Increment due to ongoing testing.

» 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 will conduct a cooperative vulnerability and penetration assessment and an adversarial assessment after release of the final intended software release expected in mid to late FY24, which is a one-year slip from what was reported in last year's Annual Report.

RECOMMENDATIONS

The Navy should:

1. Complete cyber survivability assessments and remaining radar evaluation no later than FY24.
2. Correct remaining deficiencies identified during IOT&E of the Endurance Baseline and verify correction through FOT&E.
3. Update the MQ-8C TEMP revision for evaluation of COBRA and future capabilities in FY24.

Next Generation Jammer Mid-Band (NGJ-MB)

The Next Generation Jammer Mid-Band (NGJ-MB) did not conduct IOT&E in FY23 as planned. In April 2023, the NGJ-MB program conducted an Operational Test Readiness Review (OTRR) and was certified ready for operational test by the Program Executive Office for Tactical Aircraft Programs, but DOT&E did not clear the program to conduct IOT&E due to system immaturity. The Navy has since conducted integrated test events focused on resolving identified deficiencies and collecting data for modeling and simulation (M&S) while demonstrating the system has matured enough to conduct operationally relevant test flights. Hardware reliability issues and a lack of validated or accredited digital models, which are derived from operational test data and are required to supplement NGJ-MB operational flight test evaluation, present a significant risk to NGJ-MB IOT&E.

SYSTEM DESCRIPTION

The NGJ-MB is an airborne electronic attack (EA) 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-MB is designed to improve EA-18G capabilities against modern, advanced RF threats, communications, datalinks, and non-traditional RF targets.

The NGJ-MB has four EA mission profiles: standoff, modified escort, penetrating escort, and stand-in jamming. Navy aircrews will primarily fly the standoff and modified escort profiles. The Navy will use the NGJ-MB to deny, degrade, or deceive the enemy's use of the electromagnetic spectrum by 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 Navy approved the NGJ-MB program to move past Milestone C and enter the production and deployment phase by authorizing procurement of low-rate initial production (LRIP) pods. In the FY22 Annual Report, DOT&E reported that LRIP pods were undergoing integrated testing, and operational testing was scheduled to begin in May 2023, but system immaturity delayed operational testing indefinitely.

Using results from the April 2023 OTRR, DOT&E did not approve the program to enter IOT&E due to system deficiencies causing ongoing configuration changes and the lack of an IOT&E test plan. DOT&E conveyed these concerns in a memo to the Navy Operational Test and Evaluation Force, stating that the program needed to correct system deficiencies to ensure NGJ-MB used under test is operationally representative and then conduct a follow-up OTRR to receive approval to begin IOT&E. The program then submitted a combined SCS H18 and NGJ-MB IOT&E test plan in May 2023, but has yet to conduct the follow-up OTRR after addressing deficiency corrections.

Per the DOT&E-approved Test and Evaluation Master Plan, NGJ-MB was originally slated to integrate as part of the Software Configuration Set (SCS) H16 upgrade, which is the currently fielded SCS on EA-18G aircraft. However, delays in the NGJ-MB program caused SCS integration to be deferred to the SCS H18 upgrade. The SCS upgrades, labeled in numeric order, were a separate but parallel flight test for the EA-18 Growler program. In FY23, the program decided to combine EA-18G Growler SCS H18 and NGJ-MB into one operational test plan for fiscal efficiency but has yet to conduct operational test as DOT&E awaits the follow-up OTRR. NGJ-MB will replace the ALQ-99 Tactical Jammer System pods that were developed and fielded in 1971.

» MAJOR CONTRACTORS

- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – El Segundo, California
- Boeing Defense, Space & Security – St. Louis, Missouri
- Northrop Grumman Mission Systems – Linthicum, Maryland

TEST ADEQUACY

Due to system immaturity, NGJ-MB did not conduct operational test during FY23 as planned. 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 IOT&E. 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. These integrated test events include large-force exercises in a threat-representative environment and serve as risk-reduction for planned EA-18G H18 SCS test flights with NGJ-MB. In July 2023, NGJ-MB was scheduled to conduct an integrated test event in the operationally representative environment provided by the Nevada Test and Training Range at Nellis AFB. However, the program did not execute the event as scheduled due to system immaturity. Both NGJ-MB hardware and software, along with the EA-18G SCS H18, require significant maturation and removal of high priority problems to support future NGJ-MB operational test.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E will provide an assessment of NGJ-MB operational effectiveness, suitability, and survivability at the conclusion of an approved, adequate IOT&E.

RECOMMENDATIONS

The Navy should:

1. Submit an adequate NGJ-MB IOT&E Test Plan for DOT&E approval.
2. Improve system maturity, stability, availability, and reliability of operational test-ready LRIP pods and EA-18G Growler SCS H18 to support IOT&E as soon as practical.
3. Continue to develop and assess digital models of integrated test events in an operationally representative environment to ensure necessary data are available for M&S verification, validation, and accreditation.
4. Utilize data from NGJ-MB SCS H18 integrated test events to demonstrate system maturity and conduct the follow-up OTRR.

Offensive Anti-Surface Warfare (OASuW) Increment 1

The Offensive Anti-Surface Warfare (OASuW) Increment 1 program continued the development of missile hardware and software to increase targeting capabilities and employment range over the currently fielded air-to-ground missile (AGM)-158C Long Range Anti-Ship Missile (LRASM 1.0). The Navy decided to field LRASM 1.1, the first incremental upgrade to LRASM 1.0, in FY23 following the LRASM 1.1 quick reaction assessment (QRA) in 4QFY22. The Navy also utilized QRA data for modeling and simulation (M&S) verification, validation, and accreditation (VV&A). LRASM 1.1 was slated to conduct dedicated operational test events during FY23, but hardware production delays forced LRASM 1.1 IOT&E into FY24. During FY23, the Navy completed one LRASM 1.1 integrated test event to inform M&S and aircraft carrier suitability flights in accordance with the DOT&E-approved master test strategy (MTS). The Navy is currently developing the next missile upgrade, LRASM C-3, which brings an upgraded threat target library, greater employment range, and Beyond Line-of-Sight communication capability.

SYSTEM DESCRIPTION

The OASuW Increment 1 is the first weapon of an incremental approach to produce an OASuW capability in response to a U.S. Pacific Fleet urgent operational need generated in 2008. AGM-158C LRASM, the weapon system for the OASuW Increment 1, is a long-range, conventional, air-to-surface, precision-standoff weapon intended to be launched from the Navy's F/A-18E/F and the Air Force's B-1B aircraft. Once launched, LRASM guides to an initial point using a GPS guidance system and employs onboard sensors to locate, identify, and provide terminal guidance to the target.

To date, there are three LRASM variants which comprise the OASuW Increment 1 program, designated LRASM 1.0, LRASM 1.1, and LRASM C-3. In FY22, the Navy began development of LRASM C-3, which added extended range capability. The FY22 DOT&E Annual Report stated that a land strike capability was part of the LRASM C-3 upgrade, but the program has since decided to remain focused on surface warfare capabilities, including employment range and threat target library improvements instead of land-strike. The Navy continues to work through the details required to plan and execute test events to meet the LRASM C-3 early operational capability (EOC), which has been rescheduled for 4QFY26 due to expanded program scope.

MISSION

Combatant commanders will use units equipped with LRASM to destroy adversary ships from standoff ranges.

PROGRAM

OASuW Increment 1 began as an accelerated acquisition program to procure a limited number of air-launched missiles in response to a U.S. Pacific Fleet urgent operational need generated in 2008. The program leveraged the near-term Defense Advanced Research Projects Agency's LRASM initiative as the weapon system for OASuW Increment 1. DOT&E approved the LRASM 1.1 MTS in January 2020, in lieu of a test and evaluation master plan. In 2QFY23, the Navy decided to field LRASM 1.1. The fielding decision followed FY22 integrated test events but was made without conducting the IOT&E that was scheduled in FY23. DOT&E provided a classified early fielding report in April 2023. DOT&E will write an IOT&E report at the completion of operational test flights, M&S, and cyber survivability testing in FY25.

In the FY22 Annual Report, DOT&E stated that the Navy planned to conduct a LRASM C-3 integrated test shot during 1QFY24. However, the LRASM C-3 program was delayed by expanded program scope and does not plan to conduct integrated or operational test until FY26 with EOC planned for 4QFY26.

A new program, OASuW Increment 2, which is not yet on DOT&E oversight, is intended to deliver 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, with EOC anticipated in FY29 and initial operational capability anticipated in FY31. The Navy funded LRASM C-3 to bridge the gap until an OASuW Increment 2 program of record is established. This upgrade is intended to incorporate missile hardware and software improvements to address component obsolescence and increase missile range and targeting capabilities. The Navy plans to reach LRASM C-3 EOC in 4QFY26, but has not yet provided a test and evaluation master plan, MTS or IOT&E plan to DOT&E.

» MAJOR CONTRACTOR

- Lockheed Martin Missiles and Fire Control – Orlando, Florida

TEST ADEQUACY

Despite the LRASM 1.1 MTS being approved in January 2020, LRASM 1.1 dedicated operational test activity still has not occurred due to hardware production delays. However, the Navy proceeded with integrated test events in accordance with the DOT&E-approved MTS. In FY23, the program completed one integrated test event to support VV&A of M&S and live-flight aircraft carrier suitability with captive carry free-flight evaluation missiles (FFEMs).

The carrier-tested FFEMs will be employed in an integrated test event in FY24 to support IOT&E.

The Navy plans to increase operational realism in LRASM 1.1 IOT&E through replication of an operationally representative environment. LRASM 1.1 will also undergo cyber survivability testing using a signal processor-in-the-loop lab environment. IOT&E is composed of FFEM shots, including one with a live warhead, M&S-based test events, and cyber survivability test events. DOT&E will write an IOT&E report in FY25 after operational flight, cyber, and M&S tests are complete. IOT&E is scheduled to begin in FY24 and continue into early FY25, but the Navy has not yet submitted an IOT&E plan for DOT&E approval.

In the FY22 Annual Report, DOT&E stated that LRASM C-3 would reach EOC in FY24, however the program has updated the planned fielding decision to 4QFY26. The Navy continues to develop the LRASM C-3 MTS and operational test plan. The missile concept of operations and system requirements were completed during FY23 by shifting from land-strike capability to focusing on anti-surface warfare employment range and updating the missile target threat library compared to LRASM 1.1. The Navy should continue to work with DOT&E to develop and execute an adequate operational test plan to support full-rate production and EOC in 4QFY26.

PERFORMANCE

» EFFECTIVENESS, LETHALITY, SUITABILITY, AND SURVIVABILITY

Operational effectiveness, lethality, suitability, and survivability assessments will be addressed in the FY25 IOT&E report, once testing and analysis are complete.

RECOMMENDATIONS

The Navy should:

1. Submit an adequate LRASM 1.1 IOT&E plan for DOT&E review and approval.
2. Complete development and validation of the M&S environment to facilitate the evaluation of LRASM 1.1.
3. Complete LRASM 1.1 IOT&E before full-rate production of LRASM 1.1 weapons.
4. Ensure an operationally representative open-air environment is available for LRASM 1.1 IOT&E.
5. Complete development of the LRASM C-3 MTS and operational test plan for DOT&E approval.

Ship Self-Defense System (SSDS) Mk 2 Integrated Combat Systems

Clockwise from top left: SSDS Mk 2 Mod 3 on LHD 8; Mod 6 on CVN 78; Mod 5 on LSD 51; Mod 2 on LPD 20; Mod 4 on LHA 6; and Mod 1 on CVN 68

DOT&E published a classified early fielding report for the CVN 78 *Gerald R. Ford*-Class Nuclear Aircraft Carrier program in April 2023 in advance of the ship's initial deployment. The report addresses performance shortfalls observed to date on the Ship Self-Defense System (SSDS) Mk 2 Mod 6 with Baseline 10. The Navy began the cybersecurity evaluation of SSDS Mk 2 Mod 6 with Baseline 10 (CVN 78 configuration) in July 2023 at the Surface Combat Systems Center land-based test facility in Wallops Island, Virginia. At the same facility, the Navy started land-based developmental testing of SSDS Mk 2 Mods 2 and 6 with Baseline 12. Operational tests of SSDS Mk 2 Mod 6 with Baseline 10 aboard CVN 78 are planned in 1QFY25.

SYSTEM DESCRIPTION

SSDS Mk 2 is the command and control system aboard amphibious ships and aircraft carriers. It comprises a local area network with processors that host tactical programs, and interfaces to external systems. SSDS Mk 2 integrates the following systems: horizon search radars (i.e., SPQ-9B and SPY-3), volume search radars (i.e., SPS-48, SPS-49, SPY-4 and SPY-6), MK 9 tracker illuminator system for Evolved Sea Sparrow Missile (ESSM), SLQ-32 electronic warfare system, Cooperative Engagement Capability (CEC) sensor fusion and netting system, ESSM and Rolling Airframe Missile (RAM) launchers, and Close-In Weapon System 20mm Gatling gun. SSDS includes operator workstations that display real-time tactical information.

SSDS Mk 2 has six variants referred to as mods. Each mod represents the integration of a unique set of sensors and self-defense weapon systems for a specific ship class.

- 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 dock landing ships (LSD 41 and LSD 49 classes)
- Mod 6 on *Ford*-class aircraft carriers (CVN 78 class)

SSDS Mk 2 capability improvements are delivered via software and hardware baselines within each mod. Individual ships in a class may have different SSDS software baselines, but they have the same SSDS mod. Most SSDS-based commissioned ships have baselines up to and including SSDS Mk 2 Baseline 10. The Navy is developing SSDS Mk 2 Baseline 12, which includes major changes to engagement doctrine and weapon scheduling algorithms intended to improve ship survivability.

MISSION

Navy commanders use SSDS Mk 2 for timely engagement of anti-ship cruise missile (ASCM) threats to their ship. Further, SSDS Mk 2 contributes to the commander's tactical picture during air, surface, amphibious, and undersea warfare missions by combining participating units' sensor data into a real-time composite target track picture of the battlespace.

PROGRAM

SSDS Mk 1 achieved Milestone C in 1998. In 2005, the Navy transitioned to SSDS Mk 2. SSDS Mk 2 is an Acquisition Category IC program. The Navy completed testing of the SSDS Mk 2 Mods 2 and 3 prior to May 2018, when DOT&E approved Revision C of the SSDS Mk 2 TEMP. That revision included operational tests of SSDS Mk 2 Mod 1, SSDS Mod 4 with Baseline 9 on the LHA 6 class, SSDS Mk 2 Mod 5 with Baseline 9 on LSD 41 and LSD 49 classes, and SSDS Mk 2 Mod 6 with Baseline 10 on CVN 78.

The Navy continued to develop an Air Warfare Ship Self-Defense Enterprise TEMP that includes FOT&E of SSDS Mk 2 with Baseline 12 (all mods). Testing planned in this TEMP will assess performance of updates to SSDS Mk 2 mods to address significant changes to the systems on each ship class and will include testing on new construction ships: SSDS Mk 2 Mod 4 with Baseline 12 will be tested on *Bougainville* (LHA 8), SSDS Mk 2 Mod 2 with Baseline 12 on *Harrisburg* (LPD 30), and SSDS Mk 2 Mod 6 with Baseline 12 on *John F. Kennedy* (CVN 79). Testing will also address the back-fit of Baseline 12 on existing ships. The Navy plans to start operational testing in FY27 aboard the Navy's Self-Defense Test Ship (SDTS).

» MAJOR CONTRACTORS

- Lockheed Martin Corporation – Bethesda, Maryland
- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Arlington, Virginia

TEST ADEQUACY

The Navy has yet to execute the SSDS Mk 2 Mod 1 testing outlined in the 2018 SSDS Mk 2 TEMP to assess force-level interoperability when integrated into a carrier strike group.

The Navy completed operational test on SSDS Mk 2 Mod 4 in 1QFY18 during the IOT&E of USS *America* (LHA 6). Results are documented in the USS *America* (LHA 6) Combined IOT&E and LFT&E Report of April 2019.

The Navy conducted one operational test on SSDS Mk 2 Mod 5 in 2016, The results were documented in the Ship Self-Defense of LSD 41/49-Class Ships Equipped with the Ship Self-Defense System Mk 2 Mod 5 Early Fielding Report of November 2017. The Navy plans to keep four LSD 49-class ships until FY33 but does not plan to execute the remaining eight SSDS Mk 2 Mod 5 test events for LSD ships outlined in the 2018 SSDS TEMP.

There were several operational tests of SSDS Mk 2 Mod 6 with Baseline 10 since 2019. Results were documented in the USS *Gerald R. Ford* (CVN 78) – Air Warfare Self-Defense Interim Assessment of April 2022. In April 2023, prior to the deployment of CVN 78 with SSDS Mk 2 Mod 6, DOT&E published a classified early fielding report which detailed the combat system's performance from completed test events in previous years. Only a limited assessment of the combat system's effectiveness aboard CVN 78 was possible due to the low number of anti-air warfare (AAW) test events against ASCM surrogates. The Navy must complete development and accreditation of the Probability of Raid Annihilation modeling and simulation (M&S) suite to support the full evaluation of SSDS Mk 2 Mod 6 for ASCM defense. The remaining live tests for SSDS Mk 2 Mod 6 that the Navy intends to complete in FY24 are needed to expand demonstration of AAW capabilities and to provide data for verification and validation of the M&S suite.

The Navy conducted two land-based developmental test (LBDT) events of SSDS Mk 2 Baseline 12 in the Mod 2 and Mod 6 configurations at the Surface Combat Systems Center (SCSC) in Wallops Island, Virginia in 3QFY23. The Navy intends to conduct several more LBDT events in support of SSDS Mk 2 Baseline 12. The next LBDT is scheduled for 2QFY24.

The Navy began cybersecurity evaluation of CVN 78, which included SSDS Mk 2 Mod 6 Baseline 10, at the SCSC in July 2023. The test was conducted in accordance with a DOT&E-approved test plan and observed by DOT&E. The Navy plans cybersecurity evaluation aboard CVN 78 in 2QFY24.

PERFORMANCE

» EFFECTIVENESS

No data were collected in FY23 that would change previously provided assessment of effectiveness for SSDS Mk 2 Mods 1, 4, and 5.

Insufficient data are available to determine the operational effectiveness of SSDS Mk 2 Mod 6 with Baseline 10 against ASCMs. Remaining test events will provide more data, but 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 CVN 78 IOT&E. The Navy planned to use ten live operational firing events from the DDG 1000 *Zumwalt*-Class IOT&E, but modifications to the DDG 1000 combat system no longer support the use of the DDG 1000 test data for validation of the Probability of Raid Annihilation (PRA) test bed M&S suite for the combat system. SSDS Mk 2 Mod 6 tracking capability of small boats and unmanned aerial vehicles from the July 2022 event are included in this year's Annual Report entry for the CVN 78 program. Performance shortfalls identified to date are in the classified USS *Gerald R. Ford* (CVN 78) – Air Warfare Self-Defense Interim Assessment of April 2022 and the classified USS *Gerald R. Ford* (CVN 78) Early Fielding Report of April 2023.

Early developmental testing does not provide sufficient data to assess the risks to operational

effectiveness of SSDS Mk 2 Baseline 12 Mods 2 and 6. Testing at Wallops Island is typical of early developmental testing with the system still in the problem discovery phase. Many test-analyze-fix cycles are likely to be needed before the integrated SSDS Mk 2 Baseline 12 combat systems can properly perform their air warfare mission.

» SUITABILITY

No data were collected in FY23 that would change the previously provided assessment of suitability for SSDS Mk 2 Mods 1, 4, and 5. Insufficient data are available to determine the operational suitability of SSDS Mk 2 Mod 6, as reported in the classified USS *Gerald R. Ford* (CVN 78) Early Fielding Report of April 2023.

No data are available to assess the suitability of SSDS Mk 2 Baseline 12 combat systems as they are in early developmental testing and additional modifications are expected.

» SURVIVABILITY

Data are not yet available to assess cyber survivability for SSDS Mk 2 Mod 6 on CVN 78. The determination will depend on data from the FY23 land-based test and the data yet to be collected during CVN 78 shipboard operational cyber survivability testing scheduled for FY24. The shipboard data is necessary to validate the data collected at the land-based test facility.

RECOMMENDATIONS

The Navy should:

1. Complete remaining AAW testing on CVN 78 to support demonstration of SSDS Mk 2 Mod 6 capability against surrogate threat ASCMs and validate M&S for operational assessment.
2. Complete development of the CVN 78 Probability of Raid Annihilation M&S suite in FY24 and conduct verification and validation of its accuracy to support assessment of the SSDS Mk 2 Mod 6 combat systems performance.
3. Conduct SSDS Mk 2 Mod 1 testing outlined in the 2018 SSDS Mk 2 TEMP to assess force-level interoperability when integrated into a carrier strike group.
4. Complete cybersecurity evaluation onboard CVN 78 in FY24 to assess SSDS Mk 2 Mod 6 resilience to cyberattack.
5. Address all recommendations for SSDS Mk 2 Mod 6 performance in the classified USS *Gerald R. Ford* (CVN 78) – Air Warfare Self-Defense Interim Assessment and the classified USS *Gerald R. Ford* (CVN 78) Early Fielding Report.
6. Continue to develop the Air Warfare Ship Self-Defense Enterprise TEMP in support of SSDS Mk 2 Baseline 12 platforms and submit for DOT&E approval in FY24.
7. Complete SSDS Mk 2 Mod 5 testing to characterize ship self-defense performance of LSD 49 ship class.
8. Validate with operational testing the correction of SSDS Mk 2 Mods 1 and 3 with Baseline 10 integration issues discussed in the FY22 Annual Report.

Ship to Shore Connector (SSC)

In December 2022, the Ship to Shore Connector (SSC) program postponed IOT&E due to low reliability exhibited in pre-test SSC operations. Operational testing of the SSC is expected to recommence in 3QFY24 after modifications for reliability improvement are made. The SSC program intends to complete verification, validation, and accreditation (VV&A) of vulnerability assessment models in parallel with the final survivability assessment report in FY24.

SYSTEM DESCRIPTION

The SSC is a fully amphibious air cushion vehicle similar to the currently in-service Landing Craft, Air Cushion (LCAC). Compared to the LCAC, the SSC is intended to have increased payload, 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 capability acquisition program. The Navy approved Milestone C in July 2015. The SSC program took delivery of the first test and training craft in February 2020. DOT&E approved the SSC program Test and Evaluation Master Plan in November 2021.

» MAJOR CONTRACTOR

- Textron Systems – New Orleans, Louisiana

TEST ADEQUACY

In December 2022, the SSC program attempted to commence IOT&E to assess operational effectiveness and suitability but subsequently postponed the testing. Despite the SSC program's determination that the SSC was ready to commence operational test, the three SSCs exhibited poor operational availability during pre-test operations. The SSCs experienced a high rate of failures/faults and repairs significantly depleted available repair parts. The SSC program assessed that the SSCs would not be able to complete the DOT&E-approved test plan and canceled the planned operational test. The SSC program expects to be ready to recommence IOT&E in 3QFY24.

In FY23, the SSC program completed underwater signature testing of a LCAC in loaded and unloaded conditions as a surrogate for the SSC. The test was conducted in accordance with DOT&E-approved test plan, but mechanical issues with the test article prevented the SSC program from conducting three of the twelve planned test runs. The reduced set of test runs remained adequate for the purpose of bounding the underwater signatures of loaded and unloaded SSC. Testing was observed by DOT&E. This testing supports analysis of SSC survivability in the presence of threat mines that the SSC program expects to complete in FY24 using mine susceptibility modeling and simulation.

Testing associated with cyber and LFT&E survivability addressed in the FY22 Annual Report will be reviewed and assessed for possible regression testing following the implementation of potential changes that the SSC program is making to improve SSC reliability.

PERFORMANCE

» EFFECTIVENESS

No data are available to determine operational effectiveness of the SSC.

» SUITABILITY

Insufficient data are available to determine operational suitability of the SSC due to potential changes that the SSC program is making to improve SSC reliability. Existing SSC reliability did not support conducting the planned operational test.

» SURVIVABILITY

The SSC cyber survivability assessment is classified and will be included in the SSC IOT&E report. DOT&E now expects to release this report in late FY24 or early FY25 due to the delay in commencing SSC IOT&E.

In FY23, the SSC program collected the required acoustic and magnetic data from completed underwater signature testing for assessing mine susceptibility, building off data provided from testing of SSC completed in FY22. However, the

SSC program remains behind in the VV&A of the supporting vulnerability assessment models that were previously expected to complete in FY23. The SSC program now intends to complete VV&A in parallel with a final survivability assessment report in FY24. The final survivability assessment report will also include the final predictions for the probability of kill given hit to the SSC by threat weapons.

RECOMMENDATIONS

The Navy should:

1. Sufficiently improve SSC reliability prior to commencing IOT&E. Correction of reliability issues should be confirmed with representative SSC operations.
2. Complete VV&A of SSC vulnerability assessment models in early FY24 to support timely completion of the final survivability assessment report.

Standard Missile 2 (SM-2) Block IIIC and Block IIICU

In FY23, the Navy completed a quick reaction assessment (QRA) to provide an operational demonstration of the Standard Missile 2 (SM-2) Block IIIC prototype. In addition to the live missile firing event reported in the FY22 Annual Report, the Navy completed a modeling and simulation (M&S) study and cyber tabletop assessment. Analysis is in progress and DOT&E plans to deliver an early fielding report (EFR) for SM-2 Block IIIC in 2QFY24 to support a fielding decision in the same quarter. The Navy plans IOT&E of the next missile variant, SM-2 Block IIICU, in FY27.

SYSTEM DESCRIPTION

The SM-2 Block IIIC and Block IIICU are medium-range, surface-to-air missiles with active radio frequency seekers. Both missiles are modifications to legacy SM-2 Block III/IIIA/IIIB missiles. The most significant modification is replacement of the legacy semi-active missile seeker with a dual-mode semi-active and active missile seeker based on SM-6 Block I technology. The SM-2 Block IIIC and Block IIICU additionally have a new dorsal fin design and a thrust vectoring jet tab assembly to control trajectory as the missile egresses the launcher.

The Navy's Guidance Section Electronics Unit (GS EU) replacement program is making hardware changes to the SM-6 Block IA Guidance Section and Target Detection Device to address obsolescence issues. The upgraded GS EU will be qualified on the SM-6 Block IA missile as the SM-6 Block IAU. Integration of the upgraded GS EU on the SM-2 Block IIIC results in the SM-2 Block IIICU.

MISSION

The joint force commander will use SM-2 Block IIIC and Block IIICU missiles from *Arleigh Burke*-class and *Constellation*-class ships to provide medium-range air defense, both self-defense and area air defense, against anti-ship cruise missiles and tactical aircraft. The joint force commander will use SM-2 Block IIIC and Block IIICU missiles in Naval Integrated Fire Control – Counter Air engagements from ships with this capability.

PROGRAM

The SM-2 Block IIIC was developed as a Middle Tier of Acquisition program for rapid prototyping. The Navy declared interim capability for SM-2 Block IIIC in November 2022 and expects to field the missile in 2QFY24.

The Navy declared SM-2 Block IIICU an Acquisition Category II program on the major capability acquisition pathway in an acquisition decision memorandum in April 2022, pending acquisition program baseline approval, anticipated in 1QFY25. The program was approved to enter at Milestone B in April 2023, also pending the acquisition program baseline approval. DOT&E approved the SM-2 Block IIICU Milestone B Test and Evaluation Master Plan (TEMP) in 1QFY24.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Tucson, Arizona

TEST ADEQUACY

In February 2023, the Navy completed an M&S study and the Navy's Operational Test Force (OPTEVFOR) conducted a cyber tabletop assessment of the SM-2 Block IIIC. These evaluations were conducted as part of a QRA to inform SM-2 Block IIIC fielding and supplement the live missile firing event reported in the FY22 Annual Report. OPTEVFOR intends to accredit the M&S for operational assessment in 1QFY24. The cyber tabletop will inform cyber threat vectors and areas of focus for future cyber vulnerability assessment but is not sufficient to determine cyber vulnerability of the SM-2 Block IIIC. DOT&E expects to complete review of the OPTEVFOR cyber vulnerability assessment and the Navy's M&S study of SM-2 Block IIIC in 1QFY24.

DOT&E deferred the EFR for SM-2 Block IIIC identified in the FY22 Annual Report. DOT&E will submit this report in 2QFY24 to include additional analysis from the cyber tabletop evaluation and M&S study conducted in FY23 and inform the Navy's planned fielding decision in the same quarter. Test were intended to demonstrate limited capability of the SM-2 Block IIIC prototype but not to determine operational effectiveness, suitability, or cyber survivability.

No SM-2 Block IIICU operational testing has occurred. SM-2 Block IIICU IOT&E is planned for FY27. The Navy is in development of the SM-2 Block IIICU Milestone C TEMP.

There are no changes to the legacy warhead or fusing method used on the SM-2 Block IIIC and Block IIICU missile. However, the packaging of the warhead within a modified airframe may affect the missile's lethality and should be assessed by the Navy with analysis provided to DOT&E.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

No assessments of operational effectiveness, suitability, or cyber survivability of SM-2 Block IIIC are available due to ongoing analysis. DOT&E will submit a classified EFR of SM-2 Block IIIC in 2QFY24.

» LETHALITY

No data are available to assess potential changes in lethality of the SM-2 Block IIIC and Block

IIICU missiles from the legacy SM-2 Block III and IIIA missiles.

RECOMMENDATION

The Navy should:

1. Assess the effect of missile airframe modifications on SM-2 Block IIICU lethality and provide associated analysis to DOT&E.

Surface Electronic Warfare Improvement Program (SEWIP) Block 2

The Navy's Operational Test and Evaluation Force (OPTEVFOR) commenced cyber survivability evaluation of Surface Electronic Warfare Improvement Program (SEWIP) Block 2 in FY23 with testing on the SLQ-32A(V)6 variant aboard USS *Zumwalt* (DDG 1000) and the SLQ-32B(V)6 variant in a laboratory-based test facility representing the USS *Gerald R. Ford* (CVN 78) configuration. OPTEVFOR conducted no operational testing of effectiveness and suitability in FY23 but plans completion of SEWIP Block 2 FOT&E in FY24. In the FY21 Annual Report, operational effectiveness and suitability testing was expected to be accomplished in FY22; this testing has been delayed two years due to ship and other test resource availability. DOT&E expects to publish a classified report in FY25 upon completion of FOT&E.

SYSTEM DESCRIPTION

SEWIP is an electromagnetic warfare system that detects, identifies, and tracks threat anti-ship cruise missiles and targeting radars. SEWIP Block 2 incorporates a new antenna system, enhanced processing capabilities, and a High Gain High Sensitivity subsystem to improve battlefield situational awareness. Some variants of SEWIP Block 2 incorporate additional software, known as the Soft Kill Coordination Subsystem, to improve combat system integration with non-kinetic effects, such as decoys, to defeat aerial threats.

MISSION

Navy commanders have used the SLQ-32 electronic warfare system to perform anti-ship missile defense (ASMD), counter-targeting, and counter-surveillance since the 1970s. SEWIP Block 2 upgrades the electromagnetic support capabilities and integrates more closely with the combat system to improve ASMD against emerging threats.

PROGRAM

SEWIP Block 2 is an Acquisition Category II program that entered Milestone C in January 2013. SEWIP Block 2 completed IOT&E in FY16 and the Navy approved full-rate production in September 2016.

SEWIP Block 2 has three variants, each of which have distinct hardware and software suites:

- SLQ-32(V)6 on *Arleigh Burke*-class destroyers with the Aegis combat system
- SLQ-32A(V)6 on *Zumwalt*-class destroyers
- SLQ-32B(V)6 on *Gerald R. Ford*-class aircraft carriers

SEWIP Block 2's FOT&E assesses the following:

- System upgrades since IOT&E
- Combat system integration and decoy integration capabilities of the Soft Kill Coordination Subsystem for the variant fielded on Aegis destroyers
- Integration of each SEWIP Block 2 variant with its corresponding combat system: the Aegis Combat System on the *Arleigh Burke* class, the Total Ship Computing Environment (TSCE) combat system on the *Zumwalt* class, and the Ship Self-Defense Combat System (SSDS) on the *Gerald R. Ford* class

DOT&E expects to submit a classified FOT&E report in FY25 after completion of SEWIP Block 2 FOT&E.

» MAJOR CONTRACTOR

- Lockheed Martin Corporation – Syracuse, New York

TEST ADEQUACY

OPTEVFOR evaluated the cyber survivability of SLQ-32A(V)6 aboard USS *Zumwalt* (DDG 1000) in February 2023 and SLQ-32B(V)6 in a laboratory-based test facility configured for the *Gerald R. Ford* class in July 2023. The Navy conducted both test events in accordance with DOT&E-approved test plans and with observation by DOT&E. The DDG 1000 test supports evaluation of SLQ-32A(V)6 integration with the TSCE combat system. Although the laboratory test should support evaluation of SLQ-32B(V)6 integration with the SSDS combat system, OPTEVFOR has not yet accredited the laboratory version of SLQ-32B(V)6 as representative of the *Gerald R. Ford*-class configuration due to pending data from evaluation on USS *Gerald R. Ford* (CVN 78) scheduled in 3QFY24. OPTEVFOR plans to conduct SLQ-32(V)6 system scans during *Arleigh Burke*-class destroyer platform testing in 3QFY24 to support its cyber survivability assessment and is in development of the test plan. As documented in the FY21 Annual Report, this cyber survivability testing was expected to be accomplished in 1QFY23, but it has since been delayed due to ship and other test resource availability.

OPTEVFOR conducted no testing for assessing effectiveness and suitability of SLQ-32(V)6 in FY23 but expects to conduct this evaluation in FY24. DOT&E approved a test plan for assessing effectiveness and suitability

of SLQ-32A(V)6 in July 2023. However, the scheduled test was postponed due to pilot training and safety concerns associated with the aircraft supporting tracking events and the resultant inability to conduct the test as planned. The Navy is working through these concerns and now plans to execute this test of SLQ-32A(V)6 in FY24. No additional test for assessing effectiveness and suitability of SLQ-32B(V)6 is planned.

While SEWIP Block 2 FOT&E has included additional threat emulations from those available in IOT&E, several stressing threats that the system could encounter are not available for test. Models for several of these threats are developed but the Navy has yet to fund required programming of these threats within threat emulators for test. Additionally, adequate evaluation of SEWIP Block 2 depends upon data from SLQ-32(V)6 (*Arleigh Burke*-class destroyers) and SLQ-32A(V)6 (*Zumwalt*-class destroyers) test events in a more comprehensive and complex electromagnetic spectrum environment.

PERFORMANCE

» EFFECTIVENESS

Not enough data are yet available to determine operational effectiveness of SEWIP Block 2 due to remaining test requirements and ongoing data analysis. DOT&E expects to deliver a classified report for SEWIP Block 2 in FY25 after completion of remaining FOT&E.

» SUITABILITY

Not enough data are yet available to determine operational suitability of SEWIP Block 2. However, preliminary data indicate SEWIP Block 2 fails to meet its reliability and operational availability requirements. SEWIP Block 2 reliability failure rates are similar to those reported in the SEWIP Block 2 IOT&E Report of September 2016. DOT&E expects to deliver a classified report for SEWIP Block 2 in FY25 after completion of remaining FOT&E.

» SURVIVABILITY

Not enough data are yet available to determine cyber survivability of SEWIP Block 2 due to remaining tests on SLQ-32(V)6 and SLQ-32B(V)6. DOT&E expects to deliver a classified report for SEWIP Block 2 in FY25 after completion of remaining FOT&E.

RECOMMENDATIONS

The Navy should:

1. Fund the programming of more stressing threats within threat emulators and incorporate into remaining SEWIP Block 2 test events as the emulations become available.
2. Include a complex electromagnetic environment in remaining SEWIP Block 2 test events as previously recommended in the FY21 Annual Report.
3. Identify availability of USS *Gerald R. Ford* in FY24 to complete cyber survivability evaluation of SLQ-32B(V)6 and accredit its representation during the laboratory-based test event in FY23.
4. Identify and schedule test assets to complete remaining tests on SLQ-32(V)6 and SLQ-32A(V)6.

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

The Navy commenced IOT&E and LFT&E to support assessment of T-AO 205 capabilities in FY23. However, the Navy did not complete IOT&E due to the lack of ships available to support several required test events. DOT&E will report on T-AO 205 operational effectiveness, suitability, and survivability in FY24 upon completion of IOT&E.

SYSTEM DESCRIPTION

The T-AO 205 *John Lewis*-class of fleet replenishment oilers replaces the 15 ships in the T-AO 187 *Henry J. Kaiser* class. The T-AO 205 is 746 feet long, has a full load displacement of 49,850 metric tons, and can attain a maximum speed of 20 knots. T-AO 205 has eight connected refueling stations (three delivery to port, two delivery and three receiving to starboard), one astern fuel delivery station, two connected cargo transfer stations (one to port and one to starboard), and a vertical replenishment station from the flight deck.

The T-AO 205 has an advanced degaussing system, the Nixie torpedo countermeasure system, and nine mounts for an embarked security team to mount their machine guns. The ship has the space and weight reservations for, but no installed defensive weapons systems. The T-AO 205 is designed to commercial standards for a crew of 95 civilian mariners with additional accommodations for up to 34 personnel.

MISSION

Combatant commanders will use T-AO 205 to replenish ships within carrier strike groups and expeditionary strike groups during peacetime and combat operations. T-AO 205 will serve as the primary logistics platform linking Navy ships and embarked aircraft with logistics nodes ashore. T-AO 205 delivers fuel, food, supplies, and spare parts.

PROGRAM

The T-AO 205 is an Acquisition Category IB program and achieved Milestone B/C in September 2017. The FY19 Annual Long-Range Plan for Construction of Naval Vessels increased the T-AO 205 class to 20 ships. Assistant Secretary of the Navy for Research, Development, and Acquisition increased low-rate initial production (LRIP) to 12 ships in June 2022.

General Dynamics, National Steel and Shipbuilding Company (NASSCO) delivered T-AO 205 in July 2022 and T-AO 206 in July 2023. Four ships (T-AO 207 through T-AO 210) are under construction.

DOT&E approved the Test and Evaluation Master Plan Revision 1 in September 2021.

» MAJOR CONTRACTOR

- General Dynamics NASSCO – San Diego, California

TEST ADEQUACY

The Navy commenced IOT&E in 3QFY23 aboard USNS *John Lewis (*T-AO 205) during its post-delivery test and trials period. Testing was in accordance with DOT&E-approved test plans but was incomplete due to unavailability of all ship types that the T-AO 205 is designed to replenish and reduced crew manning. The Navy demonstrated 8 of 23 replenishment events in the operational test design and repeated several of these events for seven supplemental events. The Navy has yet to demonstrate replenishment of amphibious-class ships including LHDs, LHAs, LPDs, and LSDs.

Tests focused on the delivery of fuel and cargo, as well as communications, damage control, mobility, replenishment, self-defense, and system reliability. The Navy has yet to demonstrate simultaneous operation of five connected replenishment stations and conduct operationally relevant vertical replenishment of dry cargo onboard the T-AO 205 class.

The Navy evaluated cyber survivability of T-AO 205 in 3QFY23. Testing to assess T-AO 205's cyber survivability posture and the crew's ability to conduct their mission in a cyber-contested environment was conducted in accordance with the DOT&E-approved test plan and observed by DOT&E.

The Navy completed acoustic trials in January 2023 and underwater electromagnetic trials in March 2023 on USNS *John Lewis* as part of developmental testing. Data from this testing will be leveraged to support LFT&E assessment of the likelihood that the class will set off naval mines as well as determining safe passage depths for unswept routes.

As part of LFT&E assessment of the class, the Navy completed Total Ship Survivability Trials (TSST) in July 2023 aboard USNS *John Lewis*. The TSST

simulated three different weapon hits against USNS *John Lewis* to exercise the ship's damage control and recoverability capabilities to combat primary and secondary damage.

The results from TSST will be used to assess ship recoverability and update modeling and simulation (M&S) to reflect observed functionality of T-AO 205 systems. Completion of the LFT&E survivability assessment of the class requires the Navy to complete verification, validation, and accreditation (VV&A) of the survivability M&S, including the Advanced Survivability Assessment Program (ASAP).

PERFORMANCE

» EFFECTIVENESS

Insufficient data are available to determine operational effectiveness of T-AO 205 due to testing being incomplete. To date, the T-AO 205 has demonstrated the ability to deliver fuel and cargo to several ship classes including the CVN 68 class, DDG 51 class, CG 47 class, DDG 1000 class, and LCS 2 class and also demonstrated the ability to deliver and receive fuel from another combat logistics ship during consolidation operations. Ship propulsion, damage control, communications, and auxiliary systems supported all observed operations.

» SUITABILITY

Insufficient data are available to determine operational suitability of T-AO 205 due to testing being incomplete. However, USNS *John Lewis* could not support scheduled test events on five occasions due to equipment failures.

» SURVIVABILITY

DOT&E is conducting analysis of the cyber survivability data collected on T-AO 205 and will provide a classified report in FY24.

Because the Navy has yet to complete LFT&E analyses, survivability assessment of T-AO 205 is not yet possible. DOT&E expects sufficient data to be collected by 2QFY24, but the Navy must complete VV&A of survivability M&S to support assessment. The T-AO 205 TSST identified findings previously not determined through survivability M&S. The Navy expects to deliver a TSST report and a Final Survivability Assessment Report in FY24.

RECOMMENDATIONS

The Navy should:

1. Complete the remaining IOT&E events to include simultaneous vertical and underway replenishment and simultaneous operation of five connected replenishment stations.
2. Complete the VV&A of the survivability M&S to support the Final Survivability Assessment Report.
3. Evaluate and correct causes of system reliability failures on T-AO 205 ships.
4. Complete the T-AO 205 TSST Report and Final Survivability Assessment Report.

Tomahawk Weapon System (TWS)

In February 2023, the Navy's Operational Test and Evaluation Force (OPTEVFOR) commenced operational testing of modifications to Tactical Tomahawk (TACTOM) that were developed to enable future upgrades to the Tomahawk missile, including capability to strike adversary ships at sea. In FY23, the TACTOM program additionally continued its live fire test campaign to assess lethality of the Joint Multiple Effects Warhead System (JMEWS) that the Navy intends to improve missile performance against hardened targets. DOT&E expects to publish a classified FOT&E report on the operational effectiveness and suitability of TACTOM modifications with a classified cyber survivability annex in 4QFY24 and after completion of remaining test events.

SYSTEM DESCRIPTION

The TWS consists of three segments intended to provide surface combatants and submarines with long-range, precision-guided, land attack cruise missile capability. The three major components of the system include the all-up round (AUR) missile, the Theater Mission Planning Center (TMPC), and the Tactical Tomahawk Weapon Control System (TTWCS).

- AUR: Block IV and Block V AURs are conventional Tomahawk missiles with both surface and submarine vertical launch capabilities.
- TTWCS: Provides for the initialization, preparation, launch, and post launch control of the Tomahawk missile.
- TMPC: A shore-based or sea-based mission planning center that develops and distributes missions; provides command information services for all variants of the Tomahawk missile; provides strike planning, execution, coordination, control, and reporting; and provides maritime component commanders the capability to plan or modify conventional TWS missions.

MISSION

The joint force commander employs naval units equipped with the Tomahawk Weapon System (TWS) for long-range, precision strikes against land targets. Maritime Strike Tomahawk (MST) upgrades are designed to enable the joint force commander to employ the TWS in anti-surface warfare.

PROGRAM

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

- TTWCS v5.6.1 upgrades support future AUR changes and GPS Military Code (M-code) capability, as well as SSN *Virginia*-class Payload Module implementation.
- TMPC 6.0.2/7.0.x supports AUR land attack capability changes.

Revision I of the TWS TEMP additionally documents the Navy's enduring flight test program that includes up to four test flights per year for monitoring missile flight reliability.

In April 2023, the Navy designated MST as a subprogram of the TACTOM program. The resultant TWS Block Va variant will add a surface warfare capability to the legacy TWS Block V. The Navy intends TWS Block Va initial operational capability in 2025 but has yet to develop program requirements or provide a TEMP update for DOT&E approval. DOT&E approved the MST LFT&E Strategy in December 2019.

The Navy is developing the JMEWS to improve lethality against hardened targets. The JMEWS commenced lethality evaluation in FY09 and fuze risk reduction efforts in FY19. The Navy intends integration of the JMEWS onto the Block V AUR in 1QFY27 with designation as the Block Vb variant. DOT&E approved the JMEWS LFT&E Strategy in January 2021.

» MAJOR CONTRACTORS

- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Tucson, Arizona (AUR)
- Lockheed Martin Rotary and Mission Systems – King of Prussia, Pennsylvania (TTWCS)
- Peraton, Inc. – Santa Clara, California (TMPC)
- Vencore, Inc. – San Jose, California (TMPC)
- Tapestry Solutions – St. Louis, Missouri (TMPC)
- BAE Systems – San Diego, California (Targeting Navigation)

TEST ADEQUACY

In February 2023, OPTEVFOR commenced operational testing of TTWCS v5.6.1 and TMPC 6.0.2/7.0.X in accordance with a DOT&E-approved test plan and

with observation by DOT&E, and OPTEVFOR expects it to complete in 1QFY24. The Navy intends to validate the modifications to TTWCS and TMPC will support future AUR capability and did not degrade legacy land attack functionality. Testing consists of simulated strike group scenario events in laboratory and shipboard environments, a maintenance demonstration, simulated flight tests, cyber survivability testing, and one flight test of a Block V missile launched from a surface ship.

OPTEVFOR scheduled cyber survivability evaluation of the TMPC 6.0.2/7.0 in 1QFY24. OPTEVFOR intends cyber survivability evaluation TTWCS v5.6.1 in FY24 but has not scheduled the event.

Between October and November 2022, the Navy's TWS office conducted two JMEWS arena tests in accordance with a DOT&E-approved plan and with observation by DOT&E. The Navy's TWS office plans to complete the JMEWS live fire test campaign in 4QFY26.

The Navy has yet to fund or schedule warhead characterization arena tests or lethality simulations for threat-representative maritime targets in the MST LFT&E Strategy.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Not enough data are yet available to determine operational effectiveness and suitability of TACTOM upgrades, TTWCS v5.6.1 and TMPC 6.0.2/7.0.X, due to remaining test requirements and ongoing data analysis. DOT&E expects to deliver a classified report for TACTOM upgrades in FY24 after completion of remaining FOT&E.

No data are available to assess operational effectiveness and suitability of the TWS Block Va MST AUR against maritime targets.

» LETHALITY

Not enough data are yet available to determine lethality of JMEWS due to remaining test requirements and ongoing data analysis. DOT&E expects to deliver a classified LFT&E report for JMEWS lethality in FY27 after completion of the JMEWS live fire test campaign.

No data are available to assess lethality of the TWS Block Va MST AUR against maritime targets.

» SURVIVABILITY

No data are available to assess cyber survivability of the TACTOM upgrades, TTWCS v5.6.1 and TMPC 6.0.2/7.0.X. DOT&E expects to report on TTWCS v5.6.1 and TMPC 6.0.2/7.0.X cyber survivability in FY24 after completion of their cyber assessments as an annex to the FOT&E report.

RECOMMENDATIONS

The Navy should:

1. Conduct cyber survivability evaluation of TTWCS v5.6.1 as soon as feasible.
2. Submit for DOT&E approval a TEMP update that details the test strategy and resources for TWS Block Va MST. Develop and approve requirements for the MST capability that are necessary to complete the TEMP update.
3. Fund and schedule warhead characterization testing for threat-representative maritime targets agreed to in the MST LFT&E strategy.
4. Continue to resolve the major deficiencies identified during the TWS Block V FOT&E and address recommendations in the classified TWS FOT&E report of October 2021.

Trident II (D-5) Sea-Launched Ballistic Missile – Life Extension Program Variant

The Navy's Strategic Systems Program (SSP) Office concluded operational test for the Trident-II (D-5) Life Extension Program (LEP) following 23 missile flights between 2018 and 2022. In July 2023, DOT&E submitted the IOT&E report that states the Trident-II (D-5) remains operationally effective and suitable with the LEP modifications.

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 by the inertial measurement unit. LEP modifications provide missile component refresh, including an updated guidance system and flight control electronics. The Navy plans for the Trident II (D-5) to be available through at least 2042.

MISSION

The Navy deploys the Trident II (D-5) aboard nuclear ballistic missile submarines as the sea-based leg of the U.S. nuclear triad. 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) can attack the entire range of enemy targets and supports termination of 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 Trident II (D-5) with LEP modifications 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. The Navy executes a Follow-on Commander's Evaluation Test program that conducts additional Trident II (D-5) flight tests each year to monitor missile reliability and performance.

» MAJOR CONTRACTORS

- Lockheed Martin Space Systems – Titusville, Florida
- Charles Stark Draper Laboratory – Cambridge, Massachusetts

TEST ADEQUACY

The Navy's SSP Office concluded operational testing following 23 flights of the Trident II (D5) LEP missiles between 2018 and 2022. Missile flights were in accordance with DOT&E-approved flight test support plans and were adequate to determine operational effectiveness and suitability. DOT&E submitted an IOT&E report in July 2023.

PERFORMANCE

» EFFECTIVENESS

Trident II (D-5) remains operationally effective with the LEP modifications. Classified details are in the DOT&E IOT&E report.

» SUITABILITY

Trident II (D-5) remains operationally suitable with the LEP modifications. Trident II (D-5) showed no degradation in missile reliability or availability. Classified details are in the DOT&E IOT&E report.

» SURVIVABILITY

DOT&E will continue to monitor the cyber survivability of Trident II (D-5) through annual reviews of the system's cyber postures and the program's processes to manage cyber improvements against current and future threats.

RECOMMENDATIONS

The Navy should:

1. Use its Follow-on Commander's Evaluation Test program to further characterize Trident II (D-5) performance throughout the operational space.
2. Address classified recommendations in the IOT&E report.

VH-92A® Patriot® Presidential Helicopter

The VH-92A began supporting White House Military Office (WHMO) tasking in FY23. DOT&E published an FOT&E report in January 2023 that assessed the VH-92A as operationally effective and suitable for all missions. The Navy is working to upgrade the Mission Communication System (MCS) to further improve performance and capability. VH-92A® and Patriot® are registered trademarks of the Department of the Navy.

SYSTEM DESCRIPTION

The VH-92A is a four-bladed, dual-piloted, twin-engine helicopter based on the Sikorsky S-92A medium lift helicopter. VH-92A replaces the legacy fleet of VH-3D and VH-60N aircraft flown by Marine Helicopter Squadron One (HMX-1) to perform the Presidential Transport mission. The VH-92A is transportable via a single Air Force C-17 cargo aircraft to worldwide locations. The aircraft is equipped with the MCS that can provide simultaneous line-of-sight and beyond-line-of-sight, non-secure and secure, voice and data communications to the passengers to carry out senior leader duties. MCS performance is critical to mission success.

MISSION

HMX-1 will use the VH-92A aircraft to conduct administrative lift and contingency operation missions intended to provide pre-planned and unscheduled transport of the President of the United States, cabinet members, heads-of-state and other parties as directed by the WHMO. HMX-1 will operate the VH-92A from the White House South Lawn, commercial airports, military airfields, Navy ships, and austere sites throughout the world.

Additional missions include transportation within the National Capital Region for the Vice President of the United States and visiting heads-of-state.

PROGRAM

VH-92A is an Acquisition Category IC program. The Navy procured 23 aircraft: 21 operational aircraft and 2 dedicated engineering development model test aircraft. The program acquisition strategy does not require a full-rate production decision. The U.S. Marine Corps declared initial operational capability for the VH-92A in December 2021, and the VH-92A is now supporting the WHMO Transition Plan assigned tasking. The WHMO Transition Plan stipulates an event-driven, multi-phased approach to replace legacy helicopters with the VH-92A. DOT&E published an FOT&E report in January 2023, based upon FOT&E completed in 4QFY22, that assesses effectiveness, suitability and cyber survivability, and verifies the correction of deficiencies identified during IOT&E conducted in FY21. The Navy has yet to schedule any additional FOT&E to test planned future capability upgrades.

» MAJOR CONTRACTOR

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

TEST ADEQUACY

HMX-1, under the auspices of Navy's Operational Test and Evaluation Force (OPTEVFOR), completed a first period of FOT&E and verification of correction of deficiencies in September 2022. Operational testing, conducted in accordance with a DOT&E-approved test plan and observed by DOT&E representatives, was adequate to evaluate effectiveness and suitability. HMX-1 flew nearly 40 flight hours in the National Capitol Region assessing the contingency mission and verifying the correction of deficiencies. DOT&E observed a developmental test cyber event to verify correction of deficiencies identified during IOT&E conducted in FY21. DOT&E published the results of this testing in the January 2023 FOT&E report.

PERFORMANCE

» EFFECTIVENESS

VH-92A is operationally effective for all operations. During IOT&E, VH-92A demonstrated it is operationally effective for administrative lift missions, and during FOT&E, DOT&E determined that VH-92A is also operationally effective for contingency operations missions. Performance of VH-92A voice communications, the primary means of contingency mission communications, improved significantly from IOT&E. MCS supported high call connection rates across all required voice communication pathways, but user experiences for additional off-board data services do not support fast and reliable data exchanges. Incremental improvements to the MCS are a U.S. Marine Corps and WHMO priority.

» SUITABILITY

VH-92A is operationally suitable. Improved MCS stability, modifications to the rear air-stair door actuators and increased spare parts availability have improved the aircraft's reliability and availability, and reduced maintenance times as compared to IOT&E. MCS improvements have decreased communications system operator workload. The logistics supportability concept has sufficient breadth and depth of spare parts to support HMX-1 operations. VH-92A maintenance hours per flight hour (MH/FH) are less than the legacy aircraft, and MH/FH decreased by almost 50 percent from IOT&E to FOT&E. The VH-92A remains a maintenance-intensive aircraft. Maintenance inspections account for the majority of maintenance hours.

» SURVIVABILITY

DOT&E's assessment of the VH-92A's cyber survivability is detailed in the classified annex to the January 2023 FOT&E report.

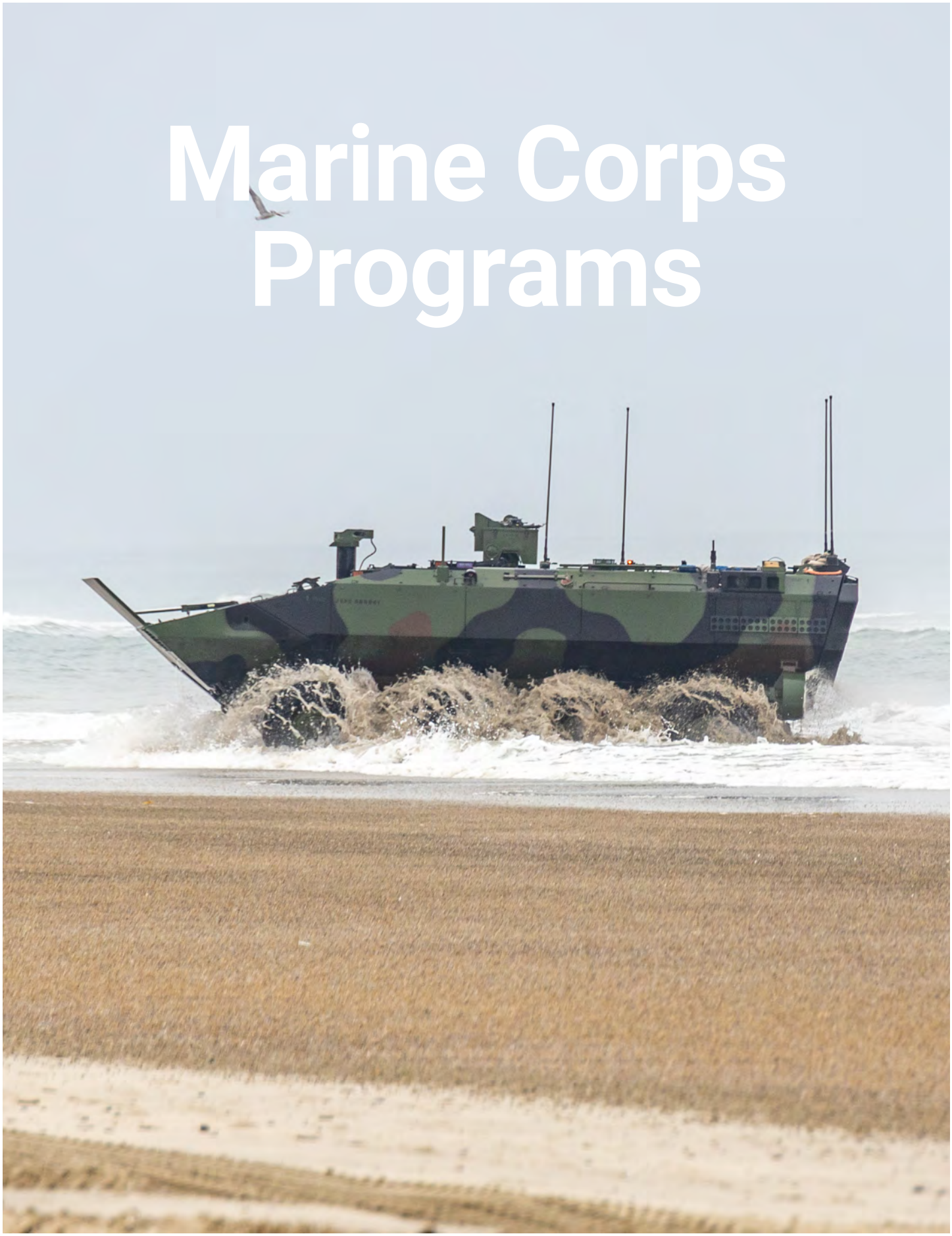
RECOMMENDATIONS

The Navy should:

1. Continue to improve user experiences with additional off-board data services and conduct an additional period of FOT&E to assess future MCS upgrades.
2. Continue to investigate options to improve MH/FH.
3. Address the cyber survivability recommendations from the classified annex to the January 2023 FOT&E report.

This page intentionally left blank.

Marine Corps Programs



This page intentionally left blank.

Long Range Unmanned Surface Vessel (LRUSV)

In FY23, the Long Range Unmanned Surface Vessel (LRUSV) Program conducted an early operational assessment (EOA) of the LRUSV prototype. No preliminary assessment of performance attributes can be made from the EOA as analysis remains in progress. DOT&E expects to deliver an EOA report in 2QFY24.

SYSTEM DESCRIPTION

The LRUSV prototype is an unmanned platform capable of traveling semi-autonomously to and from a designated patrol area where it can then loiter indefinitely (dependent on fuel state) and launch loitering munitions (LMs) and other payloads to strike maritime targets. The LRUSV rapid prototyping program consisted of the following five major sub-systems:

- Unmanned Surface Vessel (USV): powered vessel that can maneuver autonomously, or as directed by a pilot, with capability to launch LMs or small, unmanned surface vessels (sUSVs).
- LM System: organic precision fires-mounted (OPF-M) loitering munition system with a munition control interface to launch an all-up round against designated maritime targets.

- sUSV: a small USV that can be carried on the rear deck of the LRUSV to provide extended reach to deliver kinetic and non-kinetic effects.
- Command, Control, Communications, and Computers (C4) System: integrates the functions of the other required subsystems, enabling USV autonomy and deployment of LMs or sUSVs.
- Contact Vessel (CV): a manned version of the USV that provides sustainment.

MISSION

The Marine Corps and joint force commanders will employ the LRUSV to enhance maritime reconnaissance in support of sea denial and sea control operations. LRUSV supports implementation of the Littoral Operations in a Contested Environment concept, the Expeditionary Advanced Base Operations concept, and emerging doctrine defined by the Marine Corp's Force Design 2030.

PROGRAM

The LRUSV was established as a Middle Tier of Acquisition rapid prototyping program, designated by the Marine Corps in May 2021. The Marine Corps approved the LRUSV Master Test Strategy in November 2021 prior to the program being put on DOT&E oversight. In July 2023, the Marine Corps directed a capability requirement change to refine direction for the next phase of acquisition of the LRUSV. The Marine Corps intends future development of the LRUSV to focus on multi-domain sensor collections in support of the Maritime Reconnaissance Company. In September 2023, the Marine Corps directed the termination of the LRUSV Middle Tier of Acquisition program. The Marine Corps intends to transition the LRUSV to the major capability acquisition pathway at Milestone B in 2QFY27. The LRUSV program was placed on DOT&E oversight in February 2023.

» MAJOR CONTRACTORS

- Metal Shark – Jeanerette, Louisiana (LRUSV)
- HII (formerly Huntington Ingalls Industries) – Newport News, Virginia (autonomy systems)

TEST ADEQUACY

Between April and May 2023, the Marine Corps conducted an EOA with five prototype LRUSVs in accordance with a Marine Corps Operational Test and Evaluation Activity-approved test plan. DOT&E reviewed the test plan, subsequently agreed with it, and observed the test events. Testing was sufficient for operational demonstration of capability of the LRUSV prototype to direct itself to a designated patrol area and fire munitions against simulated maritime targets. The EOA also demonstrated LRUSV capability to autonomously maneuver safely in various navigational scenarios when encountering another surface vessel during transit operations.

The LRUSV Master Test Strategy did not require a cyber survivability evaluation of the LRUSV prototype.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

DOT&E's analysis is ongoing to determine the potential for LRUSV operational effectiveness and suitability. DOT&E expects to deliver an EOA report in 2QFY24.

» SURVIVABILITY

No data were collected to assess LRUSV cyber survivability.

RECOMMENDATIONS

The Marine Corps should:

1. Conduct cyber survivability testing of the LRUSV prototype prior to its use in operations and to support development of the LRUSV and assure its mission survivability.
2. Start development of a Test and Evaluation Master Plan to support entry into Milestone B.

DEPARTMENT OF THE AIR FORCE PROGRAMS

This page intentionally left blank.

Air Force Programs

This page intentionally left blank.

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

DOT&E approved the Integrated Master Test Plan that governs the remaining testing for the AGM-183A ARRW program. The Air-launched Rapid Response Weapon (ARRW) program continues to develop and mature the ARRW prototype design and conduct testing to demonstrate the required warfighting capability. The program continues to show progress and has demonstrated safe separation from the platform, proper function of the solid rocket motor, shroud separation, glide vehicle separation and flight and warhead detonation. Activities continued in preparation for an operational demonstration is FY24.

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 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 rapid prototyping Middle Tier of Acquisition program leveraging technology and lessons learned from the Defense Advanced Research Projects Agency's Tactical Boost Glide vehicle program. In August 2023, the ARRW program completed an Integrated Master Test Plan and continues to develop an Operational Demonstration Plan for DOT&E approval. Having concluded a series of booster rocket flight tests in FY21–22, the program progressed into all-up round (AUR) testing with live warheads in FY23. Because of test range availability conflicts, the two ARRW AUR flight tests conducted in FY23 targeted broad ocean areas. The Air Force intends to conduct land impacts for the last two AUR flight tests scheduled for FY24. The Air Force currently is producing a limited number of ARRWs. The Air Force will use the AUR flight test results to inform their production decision upon conclusion of the current test series.

» MAJOR CONTRACTOR

- Lockheed Martin Missiles and Fire Control – Orlando, Florida

TEST ADEQUACY

The program's flight test schedule is continually challenged due to the limited availability and numbers of hypersonic flight corridors, target areas, and test support assets. To continue system development efforts, the Air Force has conducted flight tests to date using broad ocean area impacts, which limited the amount of data collection for terminal flight and measurement of effects (i.e., lethality evaluation). The program continues to compete for limited flight test resources with other hypersonic programs, including those being developed by the Navy, Army, and Missile Defense Agency.

In December 2022, DOT&E observed the first AUR flight test. This test demonstrated proper function of the ARRW throughout all phases of flight that were measured, to include release from the B-52H platform, boost and ascent, booster-glide vehicle separation, glide, and terminal maneuver. The Air Force experienced difficulties with the terminal phase telemetry and imagery, which prevented measurement of warhead function and effects.

In March and August of 2023, DOT&E observed two AUR test flights that demonstrated proper release of the ARRW from the B-52H platform and boost/ascent. Final data analysis is ongoing at this time; however, quick look data indicate nominal conditions, including flight of the glide vehicle and warhead detonation, were achieved.

The program intends to conduct additional testing in FY24. These flights will validate the envelope of the launch conditions as well as the ARRW's flight characteristics. AUR test flights will impact land targets.

The Air Force plans to conduct an operational demonstration to assess the operational capabilities and limitations of the system. The program is working with DOT&E to develop an Operational Demonstration Plan that governs the execution of the demonstration.

The Air Force continues to conduct analysis of test data that captures missile and glide vehicle flight characteristics, and warhead performance, and comparing the observed results to modeling and simulation (M&S) results. The various M&S tools that will be used to assess lethality against the full target set continue to be validated.

The Air Force plans to use engagement-level and mission-level M&S to assess ARRW

survivability against surface-to-air missile systems and anti-aircraft-artillery batteries.

PERFORMANCE

» LETHALITY

The ARRW program has shown preliminary indications that it could become an operationally lethal weapon; however, the lack of terminal characterization data to date does not yet allow for a full assessment.

In the December 2022 flight test, the AUR performed nominally in all aspects of flight. The lack of data regarding terminal conditions was not a fault with the ARRW itself, but rather a technical failure of the test range sensor systems used during the test. Due to these sensor system failures, it is unknown if the glide vehicle and warhead functioned as desired in the final phase of flight.

In the March 2023 flight test, the AUR incurred a failure when the shrouds failed to fully eject properly during booster-glide vehicle separation, as one of two shroud ejector motors appears to have not fired. Due to that failure, the Air Force could not obtain data for the glide and terminal phases of flight. The program instituted additional continuity verification to the ejector motors to avoid a similar failure in the future. Initial quick look data analysis indicates the flight test in August 2023 achieved nominal conditions, to include proper glide vehicle flight as well as warhead detonation.

The lethality evaluation will mainly rely on the data collected during the remaining AUR test flights, which are anticipated to terminate at land targets. Given the limited number of planned test events, there is a risk that the test program will not be able to demonstrate the ARRW lethal effects against the required tactical and strategic targets.

» SUITABILITY

The limited number of planned flight hours and test assets (e.g., booster and AUR) will preclude an adequate assessment of all operational suitability metrics for the ARRW system during this phase of testing. For example, the various intermittent failures within the overall weapon system are not currently meeting system specifications, but the Air Force continues to improve reliability with software and hardware fixes, along with process improvements in manufacturing.

» SURVIVABILITY

The Air Force conducted engagement-level and mission-level simulations to assess ARRW survivability in a contested environment. The survivability assessment estimates the probability that a single ARRW will complete its mission, given the capabilities of various early warning radars, surface-to-air missile systems, and anti-aircraft-artillery batteries to detect and engage ARRW in various one-on-one scenarios. Simulations to date indicate that ARRW will meet its survivability requirements.

RECOMMENDATIONS

The Air Force should:

1. Before the next flight test, adjudicate the DOT&E comments on the Operational Demonstration Plan and submit for DOT&E approval.
2. Verify, validate, and accredit all M&S tools intended for use to enable an adequate assessment of ARRW performance.

AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM)

The Advanced Medium-Range Air-to-Air Missile (AMRAAM) Air Intercept Missile (AIM)-120D3 System Improvement Program (SIP)-3F finished integrated testing in May 2023 and the fielding recommendation is pending Service-level approval as of 4QFY23. Test analysis is ongoing and will inform the FOT&E report planned for 1QFY24.

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-120D3 is the newest variant in the AMRAAM family of missiles and incorporates a form-fit-function hardware refresh to replace obsolete components and re-hosts the SIP-3 operational flight software as SIP-3F. Multiple planned follow-on SIPs will provide updates to the AIM-120D3 to enhance missile performance and resolve previous deficiencies.

Additional software updates to the legacy AIM-120D variant are planned under the SIP-3 Tape X designation. These updates will enhance performance and resolve previous deficiencies for legacy AIM-120D hardware.

MISSION

The Air Force, Navy, and several foreign militaries employ various versions of the AIM-120 AMRAAM to conduct air-to-air combat missions. All U.S. fighter aircraft use the AMRAAM as their primary beyond-visual-range, air-to-air weapon.

PROGRAM

The AMRAAM SIP-3F upgrade is an Air Force-led project under the Acquisition Category IC AMRAAM program. DOT&E approved the SIP-3F test plan in June 2022. The Air Force and Navy completed SIP-3F integrated testing in May 2023, and fielding is pending Service-level approval. The Services are also in the process of operational test planning for the next set of AIM-120 updates: SIP-3 Tape 2 for AIM-120D and SIP-4 for AIM-120D3 variants. Operational testing on these upgrades is planned to begin in 4QFY24.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX (formerly Raytheon Technology) – Tucson, Arizona

TEST ADEQUACY

In May 2023, the Air Force and Navy completed SIP-3F integrated testing in accordance with the DOT&E approved test plan and DOT&E observed the testing. Discoveries during testing led to multiple missile software and firmware changes. As a result of these changes, some of the early tests were not of the final production-representative version of the missile. Analysis is still ongoing and test adequacy, along with effectiveness and suitability will be included in the DOT&E classified test report expected in 1QFY24.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Details on SIP-3F operational effectiveness and suitability will be available in the classified DOT&E test report, expected in 1QFY24.

» LETHALITY

SIP-3F is lethal based on previous test results from SIP-3. Details are available in the classified SIP-3 test report of November 2022.

» SURVIVABILITY

SIP-3F cyber survivability is based on previous test results from SIP-3. Details are available in the classified SIP-3 test report of November 2022.

RECOMMENDATION

The Air Force should:

1. Review SIP-3F test results to determine if regression testing and/or additional missile shots are required prior to fielding due to software and firmware changes during testing.

Air Operations Center – Weapon System (AOC-WS)

DOT&E has determined that annual functional and cyber survivability OT&E events, at a fielded Air Operations Center (AOC) site, are required to assess progress toward Block 20 system maturity, and to characterize the risks to the warfighter as the hybrid system evolves from the AOC–Weapons System (AOC-WS) 10.1 increment to the intended Block 20 end state. The Air Force delivered two capability modernization upgrades in FY23 to the fielded AOC-WS 10.1 increment. The Air Force found that AOC-WS 10.1 Agile Release Event (ARE) 23-04 was operationally effective and suitable and 23-08 needs regression testing to determine operational effectiveness and suitability; however, DOT&E will not provide an independent assessment based on the relatively minor capability delivery of the AREs. The Air Force continues to develop and deploy AOC-WS Block 20 software and has decided to delay operational testing until improved capabilities are released.

SYSTEM DESCRIPTION

The AOC-WS is a system of systems that incorporates numerous third party, commercial off-the-shelf, and Agile-developed software applications. The AOC-WS consists of two instantiations:

- The AOC-WS 10.1 increment (AN/USQ-163 Falconer) is the currently fielded backbone system for the AOC.
- AOC-WS Block 20 consists of software-based upgrades that are delivered incrementally to enhance warfighter capability.

The 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 the Air Force develops more Block 20 capabilities, 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 modernize AOC-WS 10.1 capabilities with Block 20 as the delivered software capabilities mature.

MISSION

The AOC-WS provides the Commander, Air Force Forces, or the Joint/Combined Forces Air Component Commander, the capability to exercise command and control of joint (or combined) air forces. This includes planning, directing, and assessing air, space, and cyberspace operations; air defense; airspace control; and coordination of space and mission support operations not resident within the theater of operations.

PROGRAM

The AOC-WS 10.1 increment began as an Acquisition Category III program when it entered sustainment in FY12. Block 20 began as a Defense Innovation Unit Experimental Pathfinder effort in 2017 and transitioned to six Middle Tier of Acquisition programs in FY19. In October 2021, the Assistant Secretary of the Air Force for Acquisition, Technology and Logistics designated both AOC-WS 10.1 and Block 20 as software acquisition pathway (SWP) programs, merged them, and authorized them to enter the execution phase of development. To comply with DoD Instruction 5000.87, the programs require a DOT&E-approved test strategy prior to entry into the execution phase of development. AOC-WS 10.1 has a DOT&E-approved test strategy, but there is still no DOT&E-approved test and evaluation master plan or test strategy that covers Block 20.

The Air Force submitted a revised test strategy for the merged AOC-WS 10.1 and Block 20 program in June 2023, which DOT&E returned with critical comments, including concerns about the roles, responsibilities, and authorities for the two independent Air Force operational test organizations that will both be testing AOC-WS. The program office continues to deliver incremental capability updates and maintenance software revisions to AOC-WS 10.1 via periodic AREs. The Air Force delivered and fielded ARE 23-04 in FY23 based on results from operational testing at the Ryan Center, Joint Base Langley-Eustis, Virginia.

To address one of DOT&E's critical comments discussed above, the Air Force submitted a revised 10.1 Overarching Test Plan in August 2023, which DOT&E approved with caveats. Block 20 capabilities are developed and fielded following Agile software development and continuous integration and deployment principles. Block 20 continues to undergo iterative development following the deployment of a Minimum Viable Capability Release; however, no dedicated OT&E was conducted in FY23.

DOT&E has determined that annual, independent, dedicated OT&E of both AOC-WS 10.1 and Block 20 efforts are required to assess the evolving hybrid system and Block 20's progress toward system maturity, which could be satisfied by a single test at an operational site that has both AOC-WS 10.1 and Block 20. However, AOC-WS 10.1 is the only configuration currently ready for operational testing; Block 20 will begin operational test once the capabilities are ready.

» MAJOR CONTRACTORS

- RTX (formerly Raytheon Technologies) – Dulles, Virginia
- Science Applications International Corporation, Inc. – Reston, Virginia

TEST ADEQUACY

The Air Force is conducting planned system upgrades via AREs, in accordance with the DOT&E-approved test strategy. DOT&E monitors the releases, observes the testing, and reports on more significant capability releases. The Air Force conducted integrated tests on AOC-WS 10.1 upgrades, ARE 23-04 and ARE 23-08, in accordance with a DOT&E-approved test plan, and DOT&E observed testing of both upgrades. ARE 23-04 underwent integrated testing in April 2023 and was subsequently deployed to the field. The integrated test of ARE 23-08 required additional testing of both functionality and deployability, which began in October 2023 and is expected to complete in FY24.

The Air Force is planning a Block 20 software supply chain test in FY24.

Following DOT&E approval of the test plan, the Air Force plans to conduct a cooperative vulnerability and penetration assessment (CVPA) at a functional AOC-WS in FY24. This test is consistent with DOT&E's determination that CVPAs are required annually to characterize the risk of the evolving system. The Air Force intends to submit a test plan for an AA at a functional AOC-WS site in FY24.

The Air Force did not conduct operational testing of Block 20 in FY23. Air Force operational testers observed three program office-led usability assessments (UAs) of Block 20 at operational AOC sites. However, none of these events were intended to provide adequate data to draw OT&E conclusions. Block 20 capabilities continue to be deployed incrementally through an Agile release capabilities model. Capabilities are released to the field, then feedback is obtained from the users, and the capability is refined to fit warfighter needs. DOT&E has determined that annual operational assessments are required to monitor progress toward meeting Air Combat Command's Capability Needs Statements, replacing AOC-WS 10.1, and assessing the evolving risk that is being imposed on the warfighters; each operational assessment will be followed by a DOT&E report.

PERFORMANCE

DOT&E published a classified report on AOC-WS 10.1 in May 2019. Due to the minor nature of the AREs since then, DOT&E has not issued a follow-on assessment.

» EFFECTIVENESS

The Air Force found that AOC-WS 10.1 ARE 23-04 is operationally effective and ARE 23-08 needs regression testing to determine effectiveness. The Air Force conducted capability/limitation assessments, provided operational progress report observations on operational effectiveness, and completed formal reports on the Block 20 MVCR, but the data were insufficient for DOT&E to evaluate and comment on its effectiveness.

» SUITABILITY

The Air Force found that AOC-WS 10.1 ARE 23-04 is operationally suitable. The test data from ARE 23-08 are still being analyzed to determine operational suitability. Since there has been no operational suitability testing of Block 20, there are insufficient data for DOT&E to evaluate the sustainment, maintenance, and training processes.

» SURVIVABILITY

DOT&E still does not have sufficient data on the survivability of the AOC-WS 10.1, Block 20, or the hybrid configuration. Moreover, the Air Force has not provided sufficient data on a critical portion of the software supply chain and the unclassified development environments to enable adequate OT&E planning. The AA planned for FY24, primarily focusing on AOC-WS 10.1, in conjunction with the CVPA planned for FY24, should provide adequate data to support conclusions about AOC-WS 10.1 survivability. DOT&E intends to submit a cyber survivability assessment following the completion of testing.

RECOMMENDATIONS

The Air Force should:

1. As recommended in the FY22 Annual Report, 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. Complete the revision of the consolidated test strategy covering 10.1 and Block 20 that provides for adequate, periodic evaluations of operational effectiveness, operational suitability, and cyber survivability.
3. As recommended in the FY22 Annual Report, conduct a cyber survivability assessment of the Block 20 software supply chain to include the unclassified development environment and distribution environments, and to adequately inform subsequent OT&E.
4. Complete the AA at a fielded AOC to characterize the mission survivability of the system in a realistic, cyber-contested environment.
5. As recommended in the FY22 Annual Report, implement a solution to meet the long-standing requirement to collect and report stability, reliability, availability, and maintainability data for the AOC-WS.

B-52 Radar Modernization Program (RMP)

Modification of B-52 Radar Modernization Program (RMP) test aircraft and development of initial system flight software began in FY23. Developmental and integrated flight testing is planned to begin in FY25 leading to IOT&E, full-rate production, and operational fielding in FY27.

SYSTEM DESCRIPTION

The B-52 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 high-resolution ground mapping capabilities to improve target location accuracy and capabilities to track moving surface and air targets.

MISSION

Theater Commanders use units equipped with the B-52 to conduct long-range, all-weather conventional and nuclear strike operations that employ a wide range of munitions against ground and maritime targets in low-to-medium adversary threat environments. B-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-52 RMP is an Acquisition Category IB Major Defense Acquisition Program. DOT&E approved the B-52 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 and manufacturing development contract to Boeing. A two-part Milestone C decision is planned in 2QFY25 and 4QFY25 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. The Air Force continues to refine the system design to address emerging aircraft integration issues. Modification of test aircraft and development of initial system flight software began in FY23. Developmental and integrated flight testing is planned to begin in FY25 leading to IOT&E, full-rate production, and operational fielding in FY27.

Installation of the Tactical Data Link communication system upgrade necessary to complete RMP operational test requirements may not be available until just prior to IOT&E. Delayed integration of this related system upgrade increases the risk of late deficiency discovery.

The Air Force successfully leveraged DOT&E-sponsored funding to modernize B-52 test data collection and processing infrastructure. New B-52 data acquisition technologies have been successfully paired with a government-owned Knowledge Management (KM) system to implement cutting-edge data collection, management, and processing capabilities. Application of big data analytics has improved the quality, depth, and speed of post-mission data processing for current B-52 upgrade programs and hypersonic weapon testing. As the KM system continues to mature, it is expected to accelerate data analysis for all B-52 test programs.

DOT&E approved the B-52 Cybersecurity T&E Strategy in September 2023. This strategy defines a comprehensive, integrated cybersecurity test approach across all planned modernization programs, including Commercial Engine Replacement Program, RMP, and multiple communication system upgrade programs.

» MAJOR CONTRACTORS

- The Boeing Company – Oklahoma City, Oklahoma
- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Arlington, Virginia

TEST ADEQUACY

DOT&E approved the B-52 RMP TEMP in April 2021. The TEMP defines an adequate operational test strategy and necessary resources for integrated testing and IOT&E. The B-52 Cybersecurity T&E 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 began in FY23. Developmental and integrated flight testing is scheduled to begin in 2QFY25. IOT&E will assess operational effectiveness, suitability, and survivability in FY27.

RECOMMENDATIONS

The Air Force should:

1. Continue to evaluate opportunities to accelerate Tactical Data Link integration on test aircraft to avoid late

deficiency discovery for this key supporting system.

2. Evaluate and implement system design changes necessary to manage simultaneous operation of radar and electronic warfare systems.
3. Evaluate system changes to optimize radar field-of-view in the air-to-air target mode.
4. Continue to mature and improve the B-52 KM system to accelerate the application of big data analytic techniques for B-52 modernization programs.

B-52J Commercial Engine Replacement Program (CERP)

The B-52J Commercial Engine Replacement Program (CERP) completed initial Middle Tier of Acquisition (MTA) rapid prototyping efforts with delivery of Virtual System Prototype digital models in FY23. At Air Force Acquisition Executive direction, the program is transitioning to the Major Capability Acquisition pathway with a planned Milestone B decision in FY24.

SYSTEM DESCRIPTION

The B-52J CERP is the final phase of a multi-year, multi-program modernization effort that will produce the B-52J aircraft configuration. B-52J CERP replaces legacy TF33 engines with Rolls Royce F130 commercial derivative engines to increase system reliability and reduce sustainment costs. This upgrade will also increase fuel efficiency and electrical power generation capacity and provide modern digital engine controls and displays.

MISSION

Theater Commanders will use units equipped with the B-52J to conduct long-range, all-weather, conventional and nuclear strike operations that employ a wide range of munitions against ground and maritime targets in low-to-medium adversary threat environments. B-52 theater mission tasks will include strategic attack, time-sensitive targeting, air interdiction, close air support, suppression/destruction of enemy air defenses, maritime mining, and nuclear deterrence.

PROGRAM

The B-52J CERP completed initial MTA rapid prototyping efforts with delivery of Virtual System Prototype digital models in FY23. These models support initial system performance analysis, production planning, system support analysis, and early training activities. Digital models developed during the MTA phase will require extensive ground and flight test validation to enable their use as primary program data sources.

At Air Force Acquisition Executive direction, the program is transitioning to the major capability acquisition pathway with a planned Milestone B decision in FY24. The proposed acquisition strategy extends system development until FY31 to better integrate with preceding modernization upgrades, to include the radar modernization and communication system upgrades, along with ongoing aircraft sustainment programs. The proposed program schedule includes system-level Critical Design Review in FY25 followed by modification of two test aircraft. Developmental and integrated flight testing would begin in FY28 leading to IOT&E in FY31. The proposed production program would award low-rate initial production (LRIP) contracts to procure engines and modify 70 percent (52 of 74) of B-52 fleet aircraft prior to the completion of IOT&E in FY31. A full-rate production decision for the remaining 22 aircraft is planned for FY32. IOT&E will be conducted with two fully modernized B-52J LRIP aircraft.

Integration of new engines on a legacy aircraft is a major design change. B-52J commercial engine integration will require extensive flight tests to evaluate safety and performance in the areas of aircraft structures, wing flutter, propulsion system compatibility, aerodynamic performance, and aircraft flying qualities in critical phases of flight. Changes in aircraft performance and flight characteristics require recertification of air refueling compatibility with all supporting tanker aircraft and recertification of all weapons employed from external wing stations. Based on results from previous flight test programs, the risk of deficiency discovery in one or more of these areas is high.

The proposed Air Force acquisition strategy implements a highly concurrent flight test and production program with LRIP contracts awarded for 70 percent of fleet aircraft prior to IOT&E. Contracts for the first two LRIP lots totaling 20 aircraft would be awarded prior to the start of the flight test program. Two additional LRIP contracts for 32 more aircraft would be awarded prior to completion of the developmental flight test program and IOT&E. Previous aircraft development programs with highly concurrent flight test and production schedules of this kind have frequently incurred significant cost increases and schedule delays driven by deficiency discoveries. To minimize concurrency risks, section 4231 of title 10, U.S. Code limits LRIP quantities to the minimum necessary to provide production representative articles for operational test, to establish an initial production base for the system, and to permit an orderly increase in the production rate. Air Force rationale for establishing 70 percent of fleet aircraft as the

minimum LRIP quantity necessary for these limited purposes is based on a 2017 Business Case Analysis. That analysis projected significant cost savings from procurement of a commercial engine replacement in fewer and larger lots with installation schedules aligned with existing B-52 periodic depot maintenance schedules.

DOT&E is coordinating with the Air Force to develop the B-52J CERP Milestone B Test and Evaluation Master Plan. DOT&E approved the B-52J Cybersecurity T&E Strategy in September 2023. The strategy defines a comprehensive cybersecurity test approach across all planned modernization programs, including CERP, radar modernization, multiple communication system upgrades and system sustainment programs.

» MAJOR CONTRACTORS

- The Boeing Company – Oklahoma City, Oklahoma
- Rolls-Royce North America – Indianapolis, Indiana

TEST ADEQUACY

DOT&E is coordinating with the Air Force to develop the B-52J CERP Milestone B Test and Evaluation Master Plan. It will define an adequate operational test strategy for the modernized B-52J aircraft configuration.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

The B-52J CERP is still in the system design phase. Developmental and integrated flight testing is proposed to begin in FY28. IOT&E will assess operational effectiveness, suitability, and survivability in FY31.

RECOMMENDATIONS

The Air Force should:

1. Continue to develop verification and validation plans for digital models developed during the MTA phase to enable future use as primary engineering decision tools.
2. Mitigate concurrent flight test and production risks by establishing clear, data-driven exit criteria based on flight test results for each of the four LRIP contract award decision points.

Defense Enterprise Accounting and Management System (DEAMS)

The Defense Enterprise Accounting and Management System (DEAMS) program continues to refine their implementation of the Scaled Agile Framework (SAFe) to improve the delivery of accounting management software in support of the warfighter, but the operational test strategy is out-of-date and DEAMS's current operational effectiveness, suitability and survivability have not been fully assessed since FY16. The Air Force should perform a DEAMS verification, validation, and accreditation (VV&A) of the DEAMS integrated test environment to determine its level of operational representativeness. The results should be used to develop a more operationally representative test strategy to guide Agile development and fielding of new capabilities and software fixes.

SYSTEM DESCRIPTION

DEAMS is a defense business system that uses commercial off-the-shelf enterprise resource planning software to provide accounting and financial management services.

The DEAMS Program Management Office (PMO) is following an Agile acquisition strategy that adds capabilities and users incrementally. DEAMS serves a user base of up to 16,600 end-users at approximately 170 locations worldwide.

MISSION

DEAMS is intended to deliver accurate, reliable, timely, and auditable financial management information compliant with governing laws, regulations, and policies. DEAMS performs the following core accounting functions:

- Financial System Management
- General Ledger Management
- Funds Management
- Payment Management
- Receivable Management
- Cost Management
- Reporting

Air Force financial managers and tenant organizations use DEAMS to do the following across the U.S. Air Force, the U.S. Space Force, and their supported combatant and field commands:

- Compile and share accurate, up-to-the-minute financial management data and information
- Satisfy congressional and DoD requirements for auditing of funds, standardizing of financial ledgers, timely reporting, and reduction of costly rework

PROGRAM

DEAMS is a Business Acquisition Category I program of record. The PMO submitted for approval a Test and Evaluation Master Plan (TEMP) to DOT&E, which was approved in FY18. DEAMS was designated as an Agile software development pilot program in the FY19 National Defense Authorization Act. In FY20, the DEAMS PMO adopted SAFe to facilitate Agile software development. During FY23, DEAMS completed 4 Agile program increments of approximately 12 weeks each, which resulted in deployment of incremental updates to previously fielded capabilities.

» MAJOR CONTRACTOR

- CACI International, Inc. – Dayton, Ohio

TEST ADEQUACY

The DEAMS PMO developed a more operationally representative integrated test environment to support shortened development and deployment cycles enabled by Agile software development methods. Additionally, the DEAMS PMO is executing a cloud migration strategy as well. The DEAMS program intends to deploy new capabilities to new user sets starting in major acquisition commands in FY25, a one-year slip from DOT&E's FY22 Annual Report. The Air Force will conduct a risk assessment in accordance with DOT&E guidance to determine the scope of the FOT&E for this limited deployment planned for FY25.

As reported in the FY22 DOT&E Annual Report, the following problems still need to be addressed as a result of the implementation of the SAFe software development:

- The approved DEAMS TEMP is out of date and requires an update to address future FOT&E of new capabilities being fielded and/or new user deployments.
- The operational representativeness of the DEAMS integrated test environment is unknown because the Air Force has not yet conducted a VV&A of the integrated test environment.
- An Agile Operational Master Test Plan (AOMTP) is needed with sufficient detail to conduct adequate operational tests of the upcoming DEAMS capability deployments.

PERFORMANCE

» EFFECTIVENESS

The FY22 Annual Report noted some areas reducing the operational effectiveness of the DEAMS program identified during previous operational testing. The DEAMS program is using Agile development methods to improve each of those areas:

- Timeliness of displayed information to users has improved due to fixes implemented in performance in data replication to display timely reports to the users.
- Problems resulting from software obsolescence and a major system software upgrade are delivered through the program increment Agile process.

DEAMS implementation of SAFe is facilitating an Agile software development environment that can focus on faster resolution of critical software deficiencies and prioritization of the backlog of software deficiencies, enhancements, and capability development. Limitations in the integrated test environment have precluded discovery of operational software deficiencies prior to deployment. However, the program has limited resources and software deficiencies are placed in the software defect backlog to be fixed based on program priorities.

» SUITABILITY

In FY20, DOT&E recommended that site-specific workflows are needed to improve the usability of DEAMS. The DEAMS AOMTP should then implement a test strategy that will evaluate site-specific operational needs for existing users and future user deployments. No significant progress has been made in this area.

» SURVIVABILITY

DEAMS remains not survivable based upon previous operational tests. In the FY20 Annual Report, DOT&E recommended that the DEAMS PMO address cyber vulnerabilities that present a high risk to DEAMS missions. To measure the program's progress towards cyber survivability, the Air Force should conduct a cooperative vulnerability and penetration assessment and an adversarial assessment.

RECOMMENDATIONS

The Air Force should:

1. Perform a VV&A of the operational representativeness and realism of the DEAMS integrated test environment. The Air Force should provide a report that details any deficiencies in the integrated test environment that would preclude its use for adequate operational testing, prior to FOT&E in FY25 and deployment of new capabilities.
2. Submit an AOMTP and an updated TEMP to DOT&E for approval to support the next planned capability deployment to new users in FY25.
3. Conduct a cooperative vulnerability and penetration assessment and an adversarial assessment to evaluate the progress of DEAMS towards cyber survivability.

F-15 Eagle Passive Active Warning and Survivability System (EPAWSS)

The Air Force continued to integrate software, firmware, and hardware fixes to improve the performance of the F-15 Eagle Passive Active Warning and Survivability System (EPAWSS) and address deficiencies discovered in ground and flight testing in preparation for the start of IOT&E. DOT&E approved the Air Force Operational Test and Evaluation Center (AFOTEC) IOT&E flight test plan in March 2023 and the hardware-in-the-loop test plans in July 2023. Operational testing began in July 2023 and is expected to complete in 2QFY24.

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 Advanced Display Core Processor II 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. It will be flown by active duty and Air National Guard units to perform both offensive and defensive air-to-air missions. EPAWSS provides the primary defensive suite to protect the F-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 the Milestone C DP 1 (Production Decision) in December 2020, authorizing the procurement of low-rate initial production aircraft retrofit kits and installation hardware; and DP 2 (Installation Decision) in June 2022, authorizing the start of fleet aircraft modifications. The first operational aircraft modification began in May 2023; the modified aircraft is due to return to the 48th Fighter Wing in 2QFY24.

Since last year's Annual Report, the Air Force revised its plan and now intends to retrofit 99 F-15Es and equip all 104 F-15EXs with EPAWSS as the aircraft are produced, with fielding due to start in FY24.

» MAJOR CONTRACTORS

- Boeing Defense, Space & Security – St. Louis, Missouri
- BAE Systems, Inc. – Nashua, New Hampshire

TEST ADEQUACY

DOT&E approved the AFOTEC IOT&E flight test plan in March 2023 and the hardware-in-the-loop test plans in July 2023. The Service is planning to submit the cyber test plan in 1QFY24.

During FY23, the Air Force completed a series of ground and flight test events as part of EPAWSS Integrated T&E. All testing was conducted in accordance with the DOT&E-approved Test and Evaluation Master Plan and test plans, and DOT&E observed all testing.

Developmental 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 in the presence of a dense signal environment. The Air Force plans to conduct operationally oriented IDAL testing as part of the IOT&E in 1QFY24. The Air Force previously conducted developmental testing of the jamming effectiveness against a sample of required threats at the Electronic Combat Simulation and Evaluation Laboratory (ECSEL), Point Mugu, California,

and the Wright-Patterson Test Facility at Wright-Patterson AFB. This developmental testing was followed by operationally oriented ECSEL testing as part of IOT&E in July 2023.

The Air Force 96th Test Wing conducted flight testing of the incremental EPAWSS software releases, each integrating new capabilities with the hardware/firmware and correcting deficiencies; operational aircrews and maintainers participated in this testing. Developmental and operational testers also participated in the NORTHERN EDGE 23 multi-national exercise at the Joint Pacific-Alaska Range Complex in May to prepare for IOT&E. AFOTEC commenced IOT&E flight test missions at Nellis AFB, Nevada, in 4QFY23 and plans to complete the open-air missions in 1QFY24.

The Air Force conducted developmental cyber survivability assessments at Boeing's Electronic Systems Integration Laboratory. The Air Force plans to conduct on-aircraft operational cyber survivability testing during IOT&E. Specifically, the Service will conduct a cooperative vulnerability and penetration assessment in 1QFY24 followed by an adversarial assessment in 2QFY24.

Test resource constraints affecting all spectrum warfare systems (especially electromagnetic attack systems) significantly limit the breadth of DOT&E's assessment of EPAWSS effectiveness.

PERFORMANCE

» EFFECTIVENESS

During FY23, the Air Force continued to mature the software and hardware to address the deficiencies identified during developmental testing, prior to initiating IOT&E. DOT&E will continue to observe the IOT&E until testing concludes in 1QFY24 and will publish a classified report on its findings to support the full-rate production decision.

» SUITABILITY

Hardware failures during flight testing to date indicate the system potentially can meet its requirement for mean time between unscheduled maintenance. However, incidence of software-driven built-in test failure indications remains a concern. The rate of software anomalies requiring aircrew intervention is decreasing, but further improvement is still needed. The Air Force prioritized improvements to built-in-test capabilities prior to, and during, IOT&E execution. However, if those improvements do not rectify the inaccurate system status displayed in the cockpit, aircrews may lose confidence in EPAWSS and/or may be unaware of an actual failure. In addition, the inaccurate built-in test indications may drive unnecessary maintenance actions. These aircrew and maintainer problems may negatively affect the operations of F-15 units equipped with EPAWSS. DOT&E will continue to observe the IOT&E; if these suitability problems remain unresolved, subsequent system improvements and an FOT&E might be required.

Air Force aircrews and maintainers are operating and supporting EPAWSS during the ongoing IOT&E using contractor-provided training, preliminary technical orders, and support equipment. Aircrews and maintainers will be surveyed through the end of the IOT&E to identify any areas of improvement. Additionally, AFOTEC plans to conduct an operationally oriented maintenance demonstration as part of the IOT&E.

» SURVIVABILITY

The Air Force completed planned developmental cyber survivability assessments, and the EPAWSS program improved the EPAWSS cyber posture by implementing and validating corrective actions based on the susceptibilities and vulnerabilities found during the developmental cyber assessments. AFOTEC plans to conduct the following on-aircraft operational cyber survivability testing during IOT&E: a cooperative vulnerability and penetration assessment in 1QFY24, followed by an adversarial assessment in 2QFY24.

RECOMMENDATION

The Air Force should:

1. As recommended in the FY22 Annual Report, implement built-in test indication improvements as part of the ongoing F-15 Continuous Development and Integration initiative.

F-15EX Eagle II

The F-15EX Eagle II completed all 19 planned two-ship integrated developmental and operational test missions in FY23. Phase II, which consisted of five four-ship missions, was cancelled due to already having sufficient data to complete an assessment to support the full-rate production (FRP) decision. The cyber survivability evaluation was extended to Lot 2 due to a change in the fielding configuration.

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 and Survivability System for electronic warfare, which is being reported on in a separate article.

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 can employ a full complement of air-to-air weapons and has two additional weapons stations compared to the F-15E. In the near term, the F-15EX will have a very limited capability to employ precision-guided, air-to-surface munitions.

PROGRAM

The F-15EX is an Acquisition Category IB program that transitioned from a rapid fielding Middle Tier of Acquisition program to a major capability acquisition program in September 2022. The Air Force intends to procure 104 F-15EX aircraft, training systems, and support equipment over 6 procurement lots. As part of the transition process, DOT&E approved the OT&E section of the Program Strategy Document in October 2022. DOT&E will provide an IOT&E report in 1QFY24 to support the program's FRP decision in November 2023.

» MAJOR CONTRACTORS

- Boeing Defense, Space & Security – St. Louis, Missouri
- RTX (formally Raytheon Technologies), Agile Radar Solutions – El Segundo, California
- General Electric – Cincinnati, Ohio

TEST ADEQUACY

The Air Force completed integrated testing in August 2023, 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 test missions were flown alongside the F-15C, and other missions were executed by the F-15EX without any F-15Cs participating. While not truly a 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 I of the OT&E.

The Air Force completed all 19 planned Phase I test missions. During the Phase I 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). While the initial Phase I testing was conducted with CFTs, the test data produced is representative of the production aircraft equipped with two external tanks, as now planned. The lack of CFTs will limit the number of external pods and air-to-ground weapons the F-15EX will be able to employ. Until CFTs are procured and provisioned, F-15EX's air-to-ground capabilities will be limited.

F-15EX operational testing requires a real-time, high-fidelity kill-removal system, known as Open Air Battle Shaping (OABS). The Air Force is transitioning the current OABS system 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 subsequent F-15 operational flight program releases, to support future operational test requirements. Utilization of OABS enhances the realism of open-air testing against current and future high-fidelity

active electronically scanned array threat radar emulators, while providing more accurate data including mission-level results for use in verification, validation, and accreditation of modeling and simulation solutions.

The threat levels were limited to predominantly fourth-generation adversaries with commensurate electronic warfare capabilities, with limited testing against fifth-generation adversaries. Subsequent FOT&E testing will be required to assess the system against higher threat levels in more complex mission scenarios. An F-15EX successfully employed three AIM-120s in June 2023 as part of a series of integrated weapons tests. The F-15EX successfully employed the GBU-39 Small Diameter Bomb and GBU-38 Joint Direct Attack Munition in a preplanned attack during Air Combat Command's Combat Hammer weapons evaluation program at Hill AFB, Utah. In addition, the F-15EX demonstrated the ability to launch the AGM-158B Joint Air-to-Surface Standoff Missile.

Due to the planned upgrades in Lot 2 and Lot 3 F-15EX aircraft, the Air Force Operational Test and Evaluation Center (AFOTEC) has eliminated the Phase II IOT&E and is working with the program office and DOT&E to start planning for a FOT&E in FY25 to assess the performance of the predominant operational configuration. The Program Strategy Document does not adequately address the resources and objectives of the FOT&E. The F-15EX Program Office should submit a Test and Evaluation Master Plan (TEMP) to address the requirements for the FOT&E.

In FY23, the Air Force completed vulnerability assessments for ballistic, low-power laser, and air-to-air threat susceptibility studies as part of the F-15EX Alternate LFT&E strategy approved by DOT&E in January 2021. Planned chemical and biological hardness and operational studies are on track to be completed in 2QFY24, as are susceptibility studies that will assess vulnerability to enemy air and surface-to-air defenses given F-15EX performance and countermeasures. DOT&E will provide an addendum to the LFT&E report in 3QFY24.

PERFORMANCE

» EFFECTIVENESS

DOT&E's operational effectiveness assessment is ongoing with the data collected to date. The final assessment of F-15EX operational effectiveness will be published in the classified F-15EX IOT&E report in 1QFY24 to support the FRP decision.

» SUITABILITY

DOT&E's operational suitability assessment is ongoing with the data collected to date. Initial survey data assessing human-systems interactions show the pilots had positive opinions of F-15EX cockpit usability. While training for both pilots and maintainers on new systems is currently lacking, the Air Force plans to have all training available in time for initial operational capability.

As recommended by the FY22 Annual Report, the program chartered and established the Joint Reliability and Maintainability Evaluation Team to review and categorize discrepancies. The F-15EX program office is actively working to resolve an issue with the Technical Orders (T.O.) for the F-15EX, as the current T.O.s are not accurate regarding the production model, impacting pilot and maintenance crews' ability to effectively complete tasks. The final assessment of F-15EX operational suitability will be published in the classified F-15EX IOT&E report in 1QFY24 to support the FRP decision.

» SURVIVABILITY

DOT&E's survivability assessment is ongoing with the data collected to date. The Air Force completed a mission-based risk assessment process for cyber in 2022 and employed the resultant test cases during a developmental cyber survivability assessment in February 2023. The Air Force intends to conduct a cooperative vulnerability and penetration assessment of a Lot 1B F-15EX for insights on the capabilities and limitations of new F-15EX hardware in a cyber-contested environment. AFOTEC intends to complete a nose-to-tail cyber survivability evaluation of Lot 2 F-15EX in FY25.

The Air Force plans to complete Alternate LFT&E assessments and analyses in November 2023,

except for chemical and biological hardness testing, which will be completed in March 2024. DOT&E will submit a report in 1QFY24, to support the FRP decision, and an addendum for the outstanding testing in 3QFY24.

RECOMMENDATIONS

The Air Force should:

1. As recommended in the FY22 Annual Report, ensure the F-15EX test fleet is production representative by modifying test jets to include any configuration or equipment changes that occur in future production lots.
2. Continue to incorporate OABS and high-fidelity, active electronically scanned array, threat radar emulators into the F-15EX FOT&E.
3. Complete all planned LFT&E analyses.
4. Submit a cyber survivability test plan for a nose-to-tail evaluation of Lot 2 aircraft.
5. Submit a TEMP that outlines test events and allocates resources for the period between the FRP decision and the fielding of Lot 6 in FY29.

F-16 Radar Modernization Program (RMP)

The F-16 Radar Modernization Program (RMP) completed IOT&E in 4QFY23. DOT&E is drafting an IOT&E report to inform a full-rate production decision anticipated in 1QFY24.

SYSTEM DESCRIPTION

The APG-83 SABR is a multifunction, active electronically scanned array (AESA) radar intended to replace the F-16's legacy APG-68 radar. It provides F-16 pilots with 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 complete the full kill chain against air, ground, and surface targets, from beyond visual range and in all weather conditions. The APG-83 is an improvement over the legacy system that allows for targeting and engagement from farther ranges with enhanced accuracy and improved combat identification.

PROGRAM

The APG-83 F-16 RMP is an Acquisition Category II program. DOT&E expects to approve the program's updated Test and Evaluation Master Plan (TEMP) in 1QFY24.

The F-16 RMP acquisition approach included two initial phases not under DOT&E oversight. In Phase 1, the Air National Guard tested, acquired, and fielded 24 radars to meet a U.S. Northern Command joint emergent operational need statement requirement for homeland defense. After completing Phase 1 in FY20, 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 1QFY24.

» MAJOR CONTRACTOR

- Northrop Grumman Mission Systems – Linthicum, Maryland

TEST ADEQUACY

F-16 RMP conducted IOT&E in accordance with a test plan approved and observed by DOT&E. IOT&E data collection concluded in May 2023 with over 2,200 flight hours. While data analysis is ongoing, the testing appears to be adequate to assess the radar capabilities currently being delivered to the F-16. However, inconsistent program funding and unexpected engineering challenges have delayed other upgrades to the overall F-16 system, which has prevented full realization of APG-83 capability. Once those components are available, the Air Force should assess all remaining untested radar capabilities in FOT&E.

The program completed three cyber survivability test events as part of developmental testing. In accordance with the approved TEMP, DOT&E observed the events and concurred with using their results for integrated testing purposes. In April 2022, the program office conducted a cooperative vulnerability investigation of the radar installed in an F-16 aircraft at Eglin AFB, Florida. System capabilities that could not be tested on the aircraft were tested in a second cooperative vulnerability investigation in December 2022, and in an adversarial cyber developmental test and evaluation in May 2023. Both subsequent tests were conducted in a laboratory environment at Hill AFB, Utah. The Operational Test Agency (the U.S. Air Force 53d Wing) accredited the laboratory environment for this specific purpose.

PERFORMANCE

» EFFECTIVENESS

Early analysis of the data from the operational testing provides 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 F-16's aging mission computers, obsolete data system, and insufficient network architecture. Upgrades to these systems have been delayed or have failed to meet mission requirements. The most significant pending upgrade is the transition from MIL-STD-1553 data buses to Ethernet, which is part of the high-speed data network project.

» SUITABILITY

Although data analysis is ongoing, the APG-83, as installed on the F-16, has shown vast improvements in overall reliability, maintainability, and availability over the legacy APG-68 and is comparable to other AESA radars in these criteria. Pilots are generally satisfied with the human systems interface, although some limitations and tradeoffs were required to integrate the new radar with legacy F-16 systems. The tradeoffs result in increased pilot workload for some tasks, such as switching between different displays based on the current radar mode and function in use. The Air Force intends to address these interface concerns after the transition to Ethernet.

Pilots noted during IOT&E that training systems have not kept up with APG-83 capabilities. While training systems are not part of the RMP, the Air Force will need to ensure that F-16 training reflects modernized aircraft systems.

» SURVIVABILITY

The survivability of the APG-83 in a cyber-contested environment was assessed during IOT&E. While data analysis is ongoing, testing identified some deficiencies comparable to other AESA radars. Details will be published in DOT&E's classified F-16 RMP IOT&E report in 1QFY24.

RECOMMENDATIONS

The Air Force should:

1. Correct the cyber survivability deficiencies identified during IOT&E.
2. Ensure all remaining expanded radar capabilities are tested via FOT&E after associated aircraft systems, such as the mission computer and data architecture, are modernized.
3. Continue to update supporting training systems to reflect modernized aircraft systems.

F-22A – Raptor Advanced Tactical Fighter Aircraft

In FY23, the F-22A program completed FOT&E on the Release 2 (R2) Operational Flight Program (OFP), their second annual capability release. Operational testing for the next capability release, R3, is planned to begin in 1QFY24. The Federal Aviation Administration (FAA) currently restricts Link 16 transmission, an ongoing issue that has impeded 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 versus threat radars, high maneuverability, sustained supersonic speed, and advanced integrated avionics. The capability release program adds to the F-22A's already significant combat capability via annual increments. The specific capabilities delivered in every two releases are documented in the corresponding Test and Evaluation Master Plan (TEMP).

MISSION

Units equipped with the F-22A conduct offensive counter-air, defensive counter-air, and limited ground attack missions in high-threat environments, delivering air superiority to enable coalition air operations.

PROGRAM

The F-22A Raptor started as a major capability acquisition program, with the first production aircraft fielding in 2003. Since 2019, the Air Force has been implementing hardware and software modernization efforts as capability releases. The Tactical Link 16 and Tactical Mandates TEMPs, approved by DOT&E in 2018, supported testing through the R2 Force Development Evaluation (FDE). Planning for the next F-22A capability release, R3, is ongoing, and operational testing is planned to begin in 1QFY24. The R3 and R4 capstone test strategies and test concepts are covered in a combined R3/R4 TEMP. DOT&E expects incremental updates to the TEMP every two capability releases, beginning with R5, planned for FY25.

» MAJOR CONTRACTOR

- Lockheed Martin Aeronautics Company – Fort Worth, Texas

TEST ADEQUACY

The Air Force completed the R2 FDE and cyber survivability testing in January 2023. The test was observed by DOT&E and was executed in accordance with the DOT&E-approved test plan, with one exception. The R2 FDE included successful live employment of Air Intercept Missile (AIM)-120 Advanced Medium Range Air-to-Air Missiles and five large-force employment, mission-level trials covering both defensive and offensive counter-air mission areas. However, the required Open Air Battle Shaping (OABS) capability was not properly integrated into the F-22A and was therefore not ready for use during the R2 FDE mission-level trial evaluation. The OABS limitation, which was also present in R1 testing, stemmed from omissions in F-22A software and delays integrating the Common Range Integrated Instrumentation System (CRIIS) into the F-22A. CRIIS is the current flight test instrumentation capability needed for OABS in the F-22A and will enable high-fidelity, real-time kill removal and data collection. Data collected by the OABS system will also be essential during the verification, validation, and accreditation of the F-22A model in the Joint Simulation Environment.

One longstanding test limitation stems from FAA restrictions on Link 16 transmission, which continue to prevent testing and fielding of this important capability. A more thorough evaluation of the Link 16 capability in the F-22A will occur as soon as the FAA lifts the restriction and/or the DoD develops a method to accommodate FAA protocols and restrictions.

PERFORMANCE

» EFFECTIVENESS

Analysis of the operational effectiveness of the F-22A in tasked missions with R2 capabilities is ongoing and will be reported in the classified DOT&E R2 OFP test report, planned for 2QFY24.

» SUITABILITY

Analysis of the suitability of the F-22A with R2 enhancements is ongoing will be reported in the classified DOT&E R2 OFP test report, planned for 2QFY24.

One suitability issue that remains from R1 testing is the significant delay in receiving an avionics component from the vendor that is

critical to enabling F-22A Link 16 capabilities.

» SURVIVABILITY

Analysis of the cyber survivability of the F-22A's Integrated Maintenance Information System (IMIS) will be reported in the classified DOT&E R2 OFP test report, planned for 2QFY24.

RECOMMENDATIONS

The DoD should:

1. Solidify a plan to accomplish Link 16 testing that demonstrates operational effectiveness and cyber survivability while accommodating FAA protocols, restrictions, and test-specific operating procedures, as recommended in the FY22 DOT&E Annual Report.

The Air Force should:

1. Conduct all future mission-level evaluations of the F-22A with OABS to enable high-fidelity, holistic mission evaluations with new capabilities in operationally representative environments.
2. Continue to work with the vendor to remedy the Link 16 avionics component delivery delays.

HH-60W Jolly Green II

The Air Force completed the HH-60W IOT&E in October 2022 in accordance with the DOT&E-approved test plan and DOT&E observed the testing. In March 2023, DOT&E published a combined IOT&E and LFT&E report to inform the HH-60W full-rate production (FRP) decision in April 2023. The Air Force began FOT&E of deficiency corrections and deferred capabilities in June 2023.

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

The HH-60W is an Acquisition Category IC program. DOT&E approved the LFT&E Strategy in April 2015, the Milestone C Test and Evaluation Master Plan (TEMP) in January 2020, and an updated TEMP in March 2023 to support FRP. DOT&E approved the IOT&E plan, and the Air Force Operational Test and Evaluation Center (AFOTEC) started dedicated IOT&E in April 2022. DOT&E published a combined IOT&E and LFT&E report with a classified annex in March 2023 to inform the FRP decision in April 2023.

DOT&E approved the first FOT&E test plan in June 2023. This testing will evaluate upgraded hover symbology for restricted visibility approaches and the integration of a weapon deferred from IOT&E as well as corrections of deficiencies discovered before and during IOT&E. Subsequent FOT&E plans will evaluate other deferred capabilities, including the full data link capability discussed in the FY22 Annual Report, and planned capability upgrades.

» MAJOR CONTRACTOR

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

TEST ADEQUACY

AFOTEC conducted IOT&E, including cyber survivability testing, from April through October 2022, in accordance with DOT&E-approved test plans and it was observed by DOT&E. Operational testing focused on end-to-end mission scenarios including open, confined, and mountainous terrain; high and low altitude; water and shipboard operations; and a range of threats from small arms to surface-to-air missiles. The Air Force also completed all live fire testing, analyses, and assessments per the approved LFT&E Strategy. Testing was monitored or observed by DOT&E and was adequate to evaluate the operational effectiveness, suitability, and survivability of the HH-60W.

AFOTEC began HH-60W FOT&E, in accordance with a DOT&E-approved test plan, in June 2023 to evaluate the integration of a deferred weapon, corrections of test-identified deficiencies, and upgraded hover symbology. For FOT&E, the Air Force shifted responsibility for operational testing from the 23rd Wing, 347th Rescue Group at Moody AFB, Georgia, to the 53rd Wing, 53rd Test and Evaluation Group at Nellis AFB, Nevada.

PERFORMANCE

» EFFECTIVENESS

DOT&E's assessment of the HH-60W's operational effectiveness focused on whether the aircraft provided the capabilities and information necessary for crews to successfully conduct the personnel recovery mission in all expected physical and threat environments. Details can be found in DOT&E's March 2023 combined IOT&E and LFT&E report.

» SUITABILITY

DOT&E's assessment of the HH-60W's operational suitability used hardware and software failure rate and repair time data collected during IOT&E to determine operational availability and mission reliability. The assessment also includes the crews' ability to operate aircraft and weapon

systems, from both human-system interaction and training adequacy perspectives. Details can be found in DOT&E's March 2023 combined IOT&E and LFT&E report.

» SURVIVABILITY

DOT&E's assessment of system survivability used live fire testing and analyses as well as cyber survivability data collected during two cooperative vulnerability and penetration assessments, and three adversarial assessments. Details can be found in the classified annex to DOT&E's March 2023 combined IOT&E and LFT&E report.

RECOMMENDATIONS

The Air Force should:

1. Complete FOT&E of the deferred weapon and corrections of deficiencies identified in DOT&E's March 2023 combined IOT&E and LFT&E report.
2. Conduct FOT&E of the remaining deferred capabilities and planned capability upgrades.

KC-46A Pegasus

The Air Force has collected all achievable IOT&E aerial refueling (AR) and secondary mission data on the current configuration of KC-46A until the program updates the Wing Aerial Refueling Pods (WARPs), refueling boom, and Remote Vision System (RVS). Testing completed in FY23 included centerline drogue AR of the CV-22 and the remaining KC-10 refueling the KC-46A test events. The Air Force continues to work with Boeing to develop critical upgrades to the refueling boom and RVS, with IOT&E expected to be completed on those systems in FY24 and FY25, respectively. WARP testing was delayed by identified Federal Aviation Administration (FAA) certification non-compliance items, which are expected to be resolved no later than 1QFY24, forging a pathway for IOT&E testing continuation in FY24.

SYSTEM DESCRIPTION

The KC-46A tanker aircraft is a modified Boeing 767-200ER commercial airframe with military and technological upgrades. KC-46A upgrades include a fly-by-wire refueling boom, centerline and WARP hose-drogue baskets, a dual-remote Air Refueling Operator Station enabled by an exterior RVS, additional fuel tanks in the body, a boom refueling receiver receptacle above the cockpit, a Boeing 787 digital cockpit update, Large Aircraft Infrared Countermeasures, a modified ALR-69A radar warning receiver, and Tactical Situational Awareness System that integrates input from the Radio Frequency Self Defense System (RFSDS). The KC-46A cargo bay is designed to accommodate palletized cargo, aeromedical evacuation equipment, and roll-on command, control, and communications gateway payloads.

MISSION

Commanders will use units equipped with the KC-46A to:

- Perform AR in support of six primary missions of nuclear operations support, global strike support, air bridge support, aircraft deployment support, theater support, and special operations support.
- Accomplish the secondary missions of airlift, aeromedical evacuation, emergency AR, air sampling, and support of combat search and rescue.

PROGRAM

The KC-46A Pegasus is an Acquisition Category IC program intended to be the first increment of 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-FY25. Air Mobility Command (AMC) completed the interim capability releases process and concludes that the KC-46A is ready for worldwide use. In September 2022, AMC approved the KC-46A as a deployable asset, capable of performing operations as tasked by the U.S. Transportation Command.

» MAJOR CONTRACTOR

- Boeing Commercial Airplanes in conjunction with Boeing Defense, Space & Security – Seattle, Washington

TEST ADEQUACY

KC-46A testing in FY23 included centerline drogue refueling of the CV-22 and finishing the remaining KC-10 refueling of the KC-46A test events. The Air Force Operational Test and Evaluation Center (AFOTEC) concluded all the achievable IOT&E data collection for AR and secondary missions utilizing the current KC-46A configuration. AFOTEC has collected 82 percent of the planned IOT&E flight test data but cannot complete IOT&E until the program achieves certification of the WARP system and implements the final boom and RVS upgrades. AFOTEC published a classified annex to its seventh periodic report in June 2023, which summarized the findings of the RFSDS integrated testing in FY22. The Air Force also completed electromagnetic pulse testing of the KC-46A in FY23.

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 cyberattack conditions. DOT&E has been periodically observing and continually monitoring all IOT&E testing.

In November 2022, a KC-46A crew from the 157th Air Refueling Wing set an Air Mobility Command endurance record with a 36-hour refueling mission over the Pacific initiated from Pease Air National Guard Base, New Hampshire. In addition to ongoing receiver qualification and IOT&E, Air Mobility Command tasked the KC-46A to participate in

several exercises in FY23, such as MOBILITY GUARDIAN in July 2023. In FY23, the KC-46A Joint Reliability and Maintainability Evaluation Team completed adjudication of all maintenance records over the contract-required 50,000 fleet flight hours.

AFOTEC began a third and final phase of cooperative cyber survivability testing in September 2023 and plans to complete the cooperative vulnerability and penetration assessment by December 2023 with a second adversarial assessment phase in FY24. Flight testing of the new boom actuator is expected to begin in late FY24, and flight testing of the new RVS will follow in FY25. Previous IOT&E of the WARP system, scheduled for April 2023, was suspended pending resolution of FAA certification issues. An Agreement In Principle (AIP) was signed between the Air Force and Boeing in August 2023. The AIP enables a continuation of Lot 2 WARP deliveries, provides conditional DD250 transfer from the contractor to the Air Force, and documents a commitment to resolve burdensome maintenance tasks. The FAA certification criteria for thin skin (bird strike/lightning) protection still needs to be addressed with resolution expected by 1QFY24. If resolved, IOT&E could resume in FY24 for WARP testing. Assuming RVS 2.0 upgrades are completed in mid-FY25, IOT&E will resume and DOT&E expects to complete its assessment and issue an IOT&E report post data collection and analysis.

PERFORMANCE

» EFFECTIVENESS

The KC-46A continues to operate under the interim capability releases to support most mission requirements; however, restrictions persist on boom refueling due to RVS and boom deficiencies. Problems with the RVS also degrade the effectiveness of boom AR under certain lighting conditions. Furthermore, a problem with the boom telescope actuator control can cause excess loads during receiver contact, making it difficult for some receivers to maintain contact position, and/or lead to contacts outside of the receptacle. This has prevented boom AR of the A-10 until the boom actuator redesign is complete, but the excess boom loads are noticeable even with large aircraft such as the C-17. These shortfalls in RVS and the boom represent three of the remaining six open Category 1 deficiencies the program office is tracking. The remaining Category 1 deficiencies involve leaks in the fuel manifold system, cracks and leaks in the refueling receptacle drain line, and cracks in the auxiliary power unit drain mast. Two previous Category 1 deficiencies were downgraded to a Category 2 status. The program office will continue to address the downgraded Category 1 deficiencies despite their new status. The first downgraded deficiency addresses Flight Management System (FMS) instabilities. A software release was provided in April 2023 and the system was monitored to ensure known instabilities are fixed. The FMS deficiency status will be reviewed again in September 2023 and is expected to be closed if no further instabilities present. The second Category 1 deficiency that was downgraded to Category 2 documents unexpected failures during pressure testing of the boom telescope tube assembly. This deficiency is completing the final investigation steps prior to documenting a timeline for future resolution. As of August 2023, the program office was actively addressing six open Category 1 deficiencies.

The WARP system was not able to enter IOT&E or be released for operational employment, because it failed several compliance criteria for FAA supplemental-type certification. Developmental testing occurred on an experimental airworthiness approval for prototype hardware, but production hardware did not meet certification requirements such as cowling bird strike, lightning tolerance, and wiring corrosion protection. The program is addressing these shortfalls and is expecting the WARP system to be ready for operational test at the end of 1QFY24.

As reported in the FY22 Annual Report, cargo operations are still severely limited by a lack of technical data and procedures that are available to legacy aircraft to support safe cargo operations. Cargo deficiencies were segregated into 15 specific cargo loading projects managed by a Cargo Loading Tiger

Team. Consistent with DOT&E's recommendation in the FY22 Annual Report, the Air Force continues to address the cargo-related deficiencies to improve cargo-carrying operations. At the end of FY23, 6 of the 15 projects were completed with the remaining in projects in work. The program office is working with Boeing to develop an improved KC-46A cargo operations manual expected for delivery by 3QFY24.

» SUITABILITY

The program office is attempting to address suitability problems, but operational availability (≥80 percent threshold) and mission capable rate (≥90 percent threshold) remained steady at well below their threshold requirements throughout FY23. A notable factor adversely affecting availability metrics is the time-based maintenance driven by underlying commercial 767 requirements, along with commercial parts supply chain delays that contribute to a significant portion of the aircraft down-time. The program office is working with Boeing, the Defense Logistics Agency, and the Air Force Sustainment Center to develop Air Force-specific maintenance schedules and improve supply logistics.

Problems with the Automatic Performance Tool (APT) for calculating aircraft weight and balance contributed to delays and cancellations of operational KC-46A mission taskings. Furthermore, the technical publications for KC-46A that are composed of substantial baseline commercial 767 information do not allow Air Force personnel to employ common approaches to deal with weight and balance discrepancies with the APT.

» SURVIVABILITY

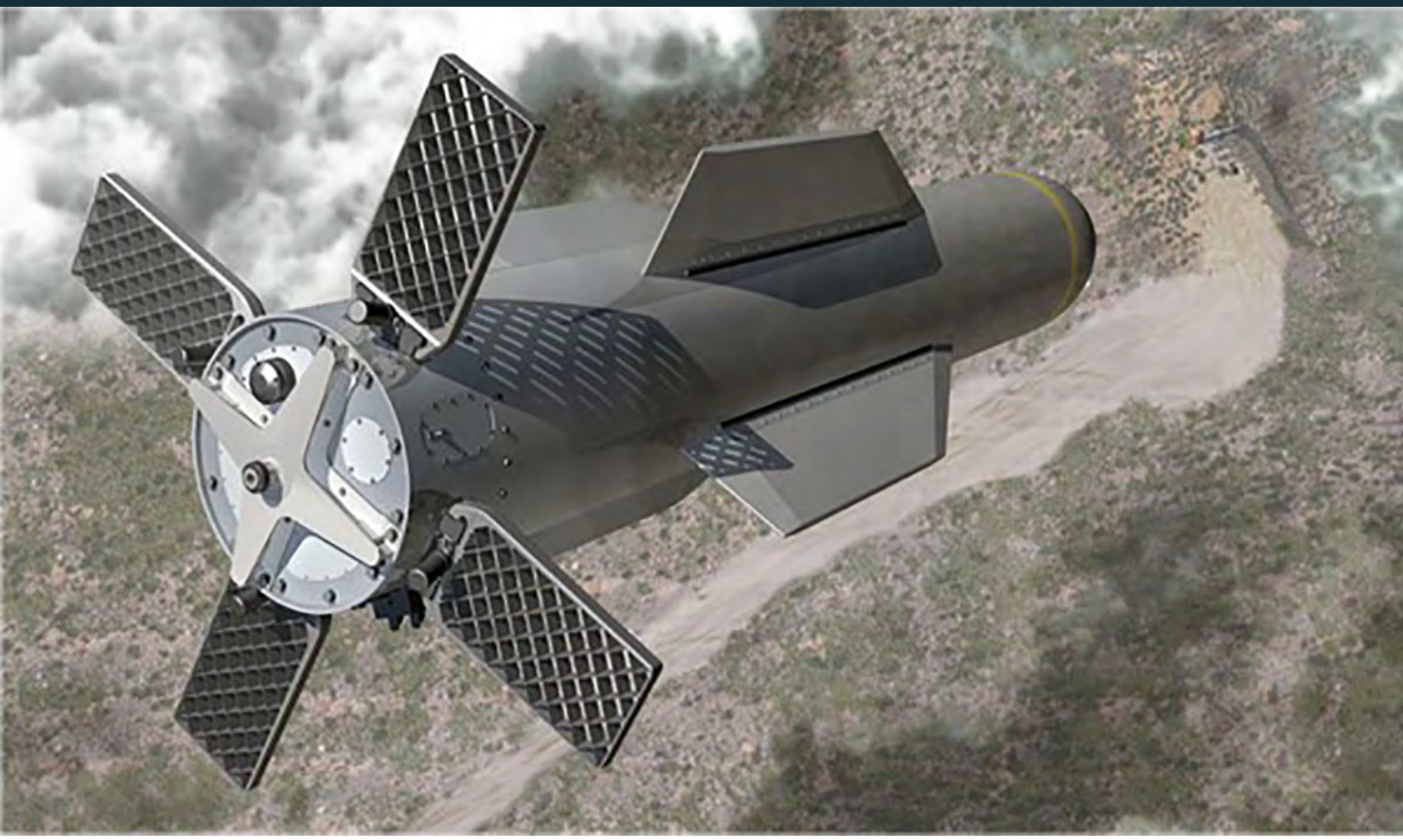
AFOTEC published a classified report in June 2023 detailing the integrated test of the RFSDS and does not plan any further testing of the current system during IOT&E. DOT&E is awaiting the final test data for analysis, but preliminary findings show that the program should continue to work on software updates to the RFSDS to improve the aircrew interface and the clarity of information presented to support threat avoidance capabilities. Active and passive system electromagnetic pulse testing in FY21 indicated that the KC-46A has basic survivability in a nuclear environment. The program conducted electromagnetic pulse direct electric current testing in FY23 to determine the extent of that survivability; DOT&E is awaiting the test data for analysis and will include the results of that analysis in the KC-46A IOT&E report.

RECOMMENDATIONS

The Air Force should:

1. Resolve the remaining six Category 1 deficiencies.
2. Address problems with the WARP design to obtain the FAA airworthiness certification needed for completion of IOT&E and operational fielding.
3. Develop KC-46A-unique sortie generation and maintenance schedules to improve mission reliability and aircraft availability over what current civilian technical data and certifications allow.
4. Complete development, with Boeing, of an improved KC-46A cargo operations manual.

Massive Ordnance Penetrator (MOP) Modification



The Air Force conducted sub-scale lethality testing and retested a fix to an integration issue with the B-2. The Air Force postponed fielding of the Large Penetrator Smart Fuze (LPSF)-enabled Massive Ordnance Penetrator (MOP) due to delays in target construction. The test effort will continue until required testing is complete.

SYSTEM DESCRIPTION

The GBU-57 MOP is a large, GPS-guided, penetrating weapon designed to attack hard and deeply buried targets (HDBTs) such as bunkers and tunnels. The GBU-57 warhead is intended to be more lethal than its predecessors, the GBU-28 and GBU-37. The LPSF integrates advanced smart fuze capability into the MOP warhead, providing increased probability of kill against HDBTs by mitigating the risk of target intelligence uncertainty. The B-2 Spirit is the only aircraft capable of employing the MOP.

MISSION

Combatant commanders will use MOP to achieve national security objectives with a low-observable, platform-deliverable, conventional HDBT-defeat capability.

PROGRAM

The MOP is an Acquisition Category IC program as of August 2017. The Air Force established the LPSF Quick Reaction Capability program in August 2018 to respond to an urgent operational need, validated in July 2018, to integrate and qualify a smart fuze capability into the MOP that had been previously fielded as the Enhanced Threat Response weapon modifications. This upgrade, known as MOP Modification, provides the capability to hold at risk additional high-value HDBTs with limited threat intelligence.

The MOP Mod phase of the program intends to finalize the smart fuze software, improve weaponeering tactics, and validate through demonstration, lower-risk smart fuze capability against a full-scale, high-fidelity underground target.

Due to program funding reprioritization, Defense Threat Reduction Agency (DTRA) contract challenges that affected the ability to construct targets to support testing, and modifications to the delivery platform, the MOP Mod program was unable to execute planned testing in FY21 and FY22. The Air Force rescheduled the test events and DTRA expedited the contracting and test plan review process.

The program is planning to submit a Test and Evaluation Master Plan (TEMP) in 1QFY24 for DOT&E approval to formalize the test program and resource requirements. The TEMP articulates the resources required to complete the LPSF MOP Mod test effort.

» MAJOR CONTRACTOR

- Boeing Defense, Space & Security – St. Louis, Missouri

TEST ADEQUACY

No significant LPSF MOP testing was conducted in FY23.

PERFORMANCE

» LETHALITY, SUITABILITY, AND SURVIVABILITY

DOT&E provided a classified assessment of the Enhanced Threat Response weapon modifications in the November 2017 early fielding report of the currently fielded MOP configuration.

RECOMMENDATIONS

The Air Force should:

1. Revalidate the urgent operational need requirement from July 2018 for the LPSF Quick Reaction Capability program.

DTRA should:

1. As recommended in the FY22 Annual Report, continue the contracting and test plan review processes to minimize delays and cost growth for target construction and test execution.

MH-139A Grey Wolf

The MH-139A program entered low-rate initial production in March 2023 after achieving Milestone C and is continuing with government-led developmental testing. However, the program still faces several ongoing risks to maintaining the planned IOT&E schedule and 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 nuclear security missions by providing emergency security response and convoy escort at Minot AFB, North Dakota; Malmstrom AFB, Montana; and Francis E. Warren AFB, Wyoming.
- Air Force District of Washington will use the MH-139A to provide contingency response, continuity of operations, and executive transport for senior government officials in the National Capital Region.

In addition, 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 of Civil Authorities.

PROGRAM

MH-139A is an Acquisition Category IB program. DOT&E approved the Alternative LFT&E Strategy in May 2019 and the Milestone C Test and Evaluation Master Plan in January 2023. In February 2023, DOT&E published an observation report to inform the Milestone C decision, which the Air Force executed in March 2023.

The MH-139A acquisition strategy relies on contractor flight testing to obtain a series of civil Supplemental Type Certificate (STC) approvals to expand MH-139A capabilities and support the military flight releases (MFRs) required for government-led developmental and operational flight testing. The number of STCs has grown over the course of the program from five to nine. The most recent additional STC is required by the Air Force's decision to add an environmental conditioning system (ECS) and an additional radio for AFGSC missions. Six of nine STCs have been approved leading to a third MFR in August 2023. An additional STC is required for issuance of the operational MFR needed to begin aircrew training for IOT&E and another STC (with associated MFR) is required to start IOT&E. IOT&E is scheduled to begin in 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 continued government-led developmental flight testing, which began in August 2022, primarily at Duke Field, Florida. Testing in early FY23 focused on initial demonstrations of military capabilities to inform the Milestone C decision, including the fast-rope insertion/extraction system, military communications, crew-served weapons, the countermeasures dispensing system, and austere landings at Malmstrom AFB, Montana. The Air Force also conducted developmental cyber testing in October 2022, but some components were unavailable or off-limits and will need to be evaluated in operational testing. The Air Force Operational Test and Evaluation Center published an operational assessment report in January 2023, in support of the Milestone C decision, and its eighth periodic report in May 2023. DOT&E's February 2023 observation report highlighted several risks to the program.

Developmental testing in the remainder of FY23 included the mission planning system, gun system modifications, performance and handling qualities, flare effectiveness, additional austere landings, and heavy-weight, high-density-altitude testing. The program expects to complete developmental testing in February 2024.

Contractor ground and flight testing continued at Duke Field and at contractor facilities in Philadelphia, Pennsylvania, in support of the remaining STCs. The six STCs issued to date support a partially expanded flight envelope and integration of most military equipment. Future STCs will complete the full expanded flight envelope, including heavy weight and high-density-altitude operations, along with remaining cabin modifications and equipment additions, including an ECS, an additional radio, and the military transponder.

Delays in the MH-139A retrofit schedule and the required operational MFRs pose a risk to the IOT&E scheduled in 4QFY24. The program does not expect to retrofit existing aircraft for STC testing and operational MFR issuance until 4QFY24. Furthermore, the program is unlikely to have the three aircraft required for IOT&E in the operational configuration until 1QFY25.

The Air Force completed live fire testing of the pilot and crew armor, engine nacelle fire extinguishing system, main gearbox, horizontal tail rotor drive, and the static tests of the main and tail rotor blades in FY23. Testing of flight controls and vertical tail rotor drive systems is ongoing. Planning is underway for ballistic vulnerability, occupant casualty, and low-energy laser analyses, as well as integrated survivability and chemical, biological, and radiological assessments.

Based on the results of the static main rotor blade testing to a specified threat, the Air Force has proposed to forgo dynamic testing of the main rotor blades as an exception to the approved Alternative LFT&E Strategy and instead will rely on comparing the static test results by similarity to other rotor blades. The program has not yet submitted the proposed analysis for DOT&E approval.

As reported last year, the Air Force has not yet conducted the approved testing of the MH-139A against electromagnetic pulse (EMP) as required by the Alternative LFT&E Strategy. In lieu of the approved testing, the Air Force proposed to conduct an analysis of flight-critical systems to determine if MH-139A meets the EMP survivability requirement in the Capability Production Document. The program has not yet submitted their EMP flight-critical analysis plan for DOT&E approval.

The Air Force has not yet released results of the limited infrared (IR) signature testing to support analytical evaluation of the lower hemisphere susceptibility of the MH-139A. The Air Force Dynamic IR Missile Evaluator Lab at Wright-Patterson AFB, Ohio, will use these data to verify and update the MH-139A IR signature models to determine countermeasure effectiveness against threat systems.

PERFORMANCE

» EFFECTIVENESS

While the Air Force has made progress addressing some previously reported deficiencies, both existing and newly identified deficiencies still present a risk to the MH-139A meeting operational effectiveness requirements.
To address previously reported concerns about the cabin layout, the Air Force conducted testing on alternative layouts and newly approved equipment tie-down points. However, the Air Force has not changed the Capability Production Document to align with the proposed cabin configuration.

The Air Force is adding an additional radio to the MH-139A to provide external communications with AFGSC ground forces, but problems with internal communications persist. Tests of alternative connections are ongoing.

The Air Force demonstrated MH-139A austere landing capabilities in snow and on unimproved terrain. The program has imposed restrictions on austere landings while investigating engine ingestion of dust and debris.

Developmental testing of the gun weapon systems showed malfunctions caused by the

ammunition feed system and the spent-brass catch bag. The vendor modified the design of both components and further testing is underway.

The additional radio and particularly the ECS will increase aircraft weight and power requirements. The effects on the full MH-139A flight envelope will not be known until developmental testing is completed.

» SUITABILITY

The program needs to address several challenges for the MH-139A to be operationally suitable. As previously reported, expansion of the MH-139A operating envelope relative to the commercial AW139 baseline may stress powertrain components and increase maintenance requirements.

The Air Force demonstrated the ability to mission plan with the vendor-provided software, but testing revealed some usability issues that pose a risk to meeting both suitability and effectiveness requirements. The vendor-provided software is not authorized for installation on government networks and will require stand-alone computers at each operating location.

Testing of alternative cabin layouts identified potential human factor concerns based on the size and weight capacity of the seat design and placement relative to aircraft structures.

» SURVIVABILITY

The program needs to address several challenges for the MH-139A to be survivable against anticipated threats. Ballistic testing of various components and subsystems has provided valuable information on the damage tolerance of the aircraft as well as armor protection against the specification threat and other operationally representative small arms threats. The contractor started testing of a new fuel cell in September 2023 to determine fuel leakage into the cabin and the potential for dry bay fires. Analysis is ongoing.

RECOMMENDATIONS

The Air Force should:

1. Continue developing plans to correct deficiencies that risk degrading operational effectiveness.
2. Conduct an adequate EMP flight-critical analysis to assess aircraft survivability in expected missions.
3. Ensure that sufficient aircraft in an operationally representative configuration and all associated support equipment consistent with approved concepts of operations are available for the start of IOT&E.
4. Complete the analysis of the performance of the armor and fuel system against ballistic threats.

Small Diameter Bomb Increment II (SDB II)

The Small Diameter Bomb Increment II (SDB II) program continued integration testing on the F-35B/C and F/A-18E/F. Cryptographic information delivery, mission planning, and Operational Flight Program (OFP) compatibility continued to delay test progress. This resulted in only one F-35 test mission and three F/A-18E/F missions in FY23. The program now anticipates SDB II initial operational capability (IOC) on F/A-18E/F in FY24 and on F-35B/C in FY25.

SYSTEM DESCRIPTION

SDB II, also known as the GBU-53/B Stormbreaker, is the second increment of a 250-pound air-to-ground glide bomb. It is a network-enabled weapon (NEW) equipped with an encrypted weapon data link (WDL) radio, which allows it to destroy moving targets in adverse weather at standoff range. When launched, SDB II guides to a designated target cue using an inertial navigation unit. In normal attack mode, the attacking aircraft or a third party updates the target location with inflight target updates (IFTUs) sent via the WDL. Finally, the weapon uses a multi-mode seeker to precisely locate, identify, and terminally guide to the target. SDB II also has laser illuminated attack and coordinate attack modes to engage laser-illuminated targets or GPS coordinates.

MISSION

Combatant Commanders will use SDB II to attack stationary and moving ground and littoral targets at standoff ranges in a variety of conditions including adverse weather.

PROGRAM

SDB II is a joint Air Force and Navy Acquisition Category IC program intended to deliver expanded capability deferred from SDB I. DOT&E approved the SDB II Milestone C Test and Evaluation Master Plan (TEMP) in April 2015. This TEMP outlines a two-phase multi-Service operational test and evaluation (MOT&E). Phase I achieved SDB II fielding on the F-15E in FY20 with IOC declared in September 2022. Phase II intends to achieve early fielding with limited capability on the F-35B/C in FY24, followed by IOC in FY25. In FY20, the Navy initiated a quick reaction assessment (QRA) to integrate SDB II into the F/A-18E/F. DOT&E approved a six-event QRA test plan, which the Navy expects to complete in FY24.

In January 2022, the Service Acquisition Executive for SDB II issued an acquisition decision memorandum approving an increase of 9,610 weapons to the total production quantity. This will provide a total inventory objective of 26,610 (21,610 for the Air Force and 5,000 for the Navy). The program anticipates a full-rate production decision in FY25, concurrent with F-35 IOC.

» MAJOR CONTRACTOR

- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Tucson, Arizona

TEST ADEQUACY

During FY23, the Navy conducted two live-fly operational tests for F/A-18E/F integration and the Marine Corps conducted one live-fly test for F-35B/C integration. DOT&E observed these events, which the Services executed in accordance with DOT&E-approved test plans. Concurrent software developments delayed test missions and limited NEW testing using the OFPs and Mission Planning Environment (MPE) software intended for operational fielding. The Operational Test Agencies will test these capabilities during the two remaining F-35B, four remaining F-35C, and three remaining F/A-18E/F OT missions.

Additionally, range safety restrictions continue to impose significant limitations on SDB II employment envelopes and F-35 self-lasing. These restrictions prevent testing SDB II's full operational capabilities.

MOT&E Phase I cyber survivability testing, conducted by the Air Force in FY19, was inadequate to support an independent survivability evaluation. The test asset was not production representative and testing lacked adequate documentation and engineering support to determine the emulated cyber threat's level of sophistication. Both the Navy and Air Force program offices are actively working to rectify these shortfalls during MOT&E Phase II.

PERFORMANCE

» EFFECTIVENESS

MOT&E Phase I verified SDB II's operational effectiveness on the F-15E. Despite ongoing efforts to modernize encryption keys and update aircraft, weapon, and mission planning software, the program has not yet demonstrated

operational effectiveness on the F-35B/C or the F/A-18E/F. Both platforms have been unable to use the weapon's full NEW functionality with the aircraft OFPs and MPE software intended for operational fielding. However, SDB II did perform as expected during one successful F-35B test in laser illuminated attack mode. The Navy also used previous versions of the F/A-18E/F OFP/MPE and test (not operational) encryption keys to conduct a successful operational test with NEW capability against a moving land target and a successful developmental test against a moving maritime target.

FY22 reporting highlighted a hardware issue affecting F/A-18E/F SDB II employment during bomb rack ejection. In FY23, the program implemented a materiel solution; however, further data analysis is required to determine whether this sufficiently reduces the likelihood of degrading weapon performance.

» LETHALITY

MOT&E Phase I verified SDB II's lethality against a variety of static and moving targets including legacy main battle tanks, infantry fighting vehicles, anti-aircraft guns, surface-to-air missile target-erector-launchers, and small patrol boats. The program has not yet demonstrated lethality with the F-35B/C or F/A-18E/F.

» SUITABILITY

MOT&E Phase I, completed in FY20, first highlighted concerns with cryptographic key loading and mission planning for the SDB II as employed by the F-15E. These same issues delayed F-35 and F/A-18E/F integration testing. Synchronizing cryptographic keys across the weapon, the MPE, and the key filler devices is a complex process that involves several management nodes outside the program office. Additionally, in FY22, the DoD mandated WDL conform to new standards established by the National Security Agency (NSA)-led Cryptographic Modernization Program. In several cases, these new requirements delayed delivery of the operational cryptographic keys necessary for NEW testing.

» SURVIVABILITY

The cyber-OT&E shortfalls from Phase I need to be addressed during MOT&E Phase II before providing an independent survivability evaluation. With input from DOT&E, the program office and Navy Operational Test Agency are currently drafting an updated cyber survivability test plan.

RECOMMENDATIONS

The DoD should:

1. Continue to streamline cryptographic material delivery, management, loading, and verification processes.
2. Continue to work with candidate open-air ranges to mitigate F-35 self-lasing restrictions and allow operationally representative SDB II employment by all platforms.

The Navy should:

1. Continue to develop and fund an adequate MOT&E Phase II cyber survivability T&E strategy to support an evaluation of SDB II survivability in a cyber-contested environment.

The SDB II Program Office should:

1. Update the Milestone C TEMP to reflect the updated Phase II cyber survivability T&E strategy.
2. Continue efforts to streamline the mission planning process across all objective platforms, particularly regarding cryptographic data entry.

T-7A Advanced Pilot Training (APT)

Since receiving the contract award from the Air Force in FY18, Boeing has conducted developmental testing (DT) on the T-7A using contractor-owned, contractor-operated prototype aircraft. On June 28, 2023, after several program delays, the Air Force completed its first T-7A test flight in a production-representative Engineering and Manufacturing Development (EMD) aircraft. Government-led DT will begin in FY24 and IOT&E in FY26.

SYSTEM DESCRIPTION

The Advanced Pilot Training (APT) Family of Systems (FoS) includes the T-7A Red Hawk aircraft and ground-based training systems (GBTS). It replaces the Air Force's fleet of T-38C aircraft and associated simulators.

The T-7A is a two-seat trainer powered by a single afterburning turbofan engine. The aircraft uses digital avionics and fly-by-wire flight controls that emulate the characteristics of fifth generation fighters. GBTS devices include the aircrew ground-egress trainer, part-task trainer, and three types of simulators with varying levels of fidelity. T-7A aircraft can be networked with each other and with the simulators via an unclassified data link.

MISSION

Air Education and Training Command (AETC) will use the APT FoS to train student pilots for assignments in fourth- and fifth-

generation fighter and bomber aircraft. Pilot training in the T-7A will include the basic and advanced fighter fundamentals taught in the T-38C and will add sustained high-g maneuvering, advanced sensor management, night-vision goggle operations, and in-flight refueling training.

PROGRAM

APT is an Acquisition Category IB program. The Air Force awarded the contract to Boeing on September 27, 2018. DOT&E approved the Milestone B Test and Evaluation Master Plan in January 2018. Due to the inability to meet the planned Milestone C threshold, the program office declared a schedule breech in June 2022. In April 2023, the Air Force approved an updated program schedule, which moves the Milestone C decision from December 2023 to February 2026 (threshold) and the full-rate production decision from September 2025 to January 2028 (threshold).

AETC plans to procure 351 T-7A aircraft, 46 simulators, and associated GBTS for deployment to its five Undergraduate Pilot Training bases: Joint Base San Antonio-Randolph, Texas; Columbus AFB, Mississippi; Laughlin AFB, Texas; Vance AFB, Oklahoma; and Sheppard AFB, Texas.

» MAJOR CONTRACTORS

- The Boeing Company – St. Louis, Missouri
- Saab AB – Linköping, Sweden and Lafayette, Indiana

TEST ADEQUACY

As of July 2023, Boeing flew 503 hours over 417 missions in two contractor-owned, contractor-operated prototype aircraft. The prototypes are substantially different from the EMD aircraft contracted for government-led DT and operational testing (OT). Therefore, DOT&E will not include test data from prototype aircraft in its final evaluation of system performance. Major differences between the aircraft include wing and empennage redesign, the escape system, on-board oxygen generating system (OBOGS), electrical system, and flight control software. Government-led DT is expected to begin in FY24 and complete in FY25; IOT&E is scheduled for 3QFY26 through 1QFY27.

Early program involvement by the Air Force Operational Test and Evaluation Center (AFOTEC) provided operational perspective and continuous feedback on Boeing's initial design efforts. AFOTEC Detachment 5 personnel stationed at the Boeing facility in St. Louis, Missouri, highlighted and helped resolve several significant program issues prior to government-led testing. In July 2023, AFOTEC published a 5th periodic report that added 7 new recommendations to the remaining 30 open recommendations from the previous reports. DOT&E concurs with AFOTEC's assessments and recommendations.

PERFORMANCE

» EFFECTIVENESS

Currently available data are inadequate to provide an independent assessment of operational effectiveness. However, prototype aircraft have demonstrated the necessary flying qualities, system, and subsystem performance to begin government-led DT. The program appears to have a clear pathway to resolving known effectiveness issues such as limited sortie duration and flight characteristics at high angle-of-attack.

» SUITABILITY

Currently available data are inadequate to provide an independent assessment of operational suitability. The program office continues to work through known suitability limitations, most notably the aircraft escape system, Automatic Ground Collision Avoidance System (AGCAS), and OBOGS.

As reported in FY22, the T-7A emergency escape system, including the canopy's bird strike resistance, does not meet minimum safety requirements for the Air Force's airworthiness certification. During the initial nine escape system tests, ejection events exceeded tolerances for impulse noise (acoustic pressure), probability of concussion, and probably of injury during parachute

deployment. While the system is still not compliant, a February 2023 test showed sufficient improvement for the Air Force to approve a waiver to begin government-led DT. The program added four additional escape system tests that will define the design changes required prior to delivering the T-7A to AETC.

AGCAS is another known suitability limitation. Fighter aircraft employ AGCAS to prevent loss of life during sustained high-g maneuvers, which can cause the pilot to lose consciousness. While the formal requirements for APT did not include AGCAS, the program office is developing a strategy to start AGCAS integration in FY26. Government-led DT will include aggressive maneuvering at low altitude to ensure current aircraft navigation and attitude heading reference systems support a future AGCAS upgrade.

Although not resolved, the program office has made progress on the T-7A OBOGS. In FY23, the program procured appropriate flight test instrumentation to collect operationally representative OBOGS data. The Air Force approved the instrument's airworthiness certification, and the program will begin collecting test data during government-led DT.

» SURVIVABILITY

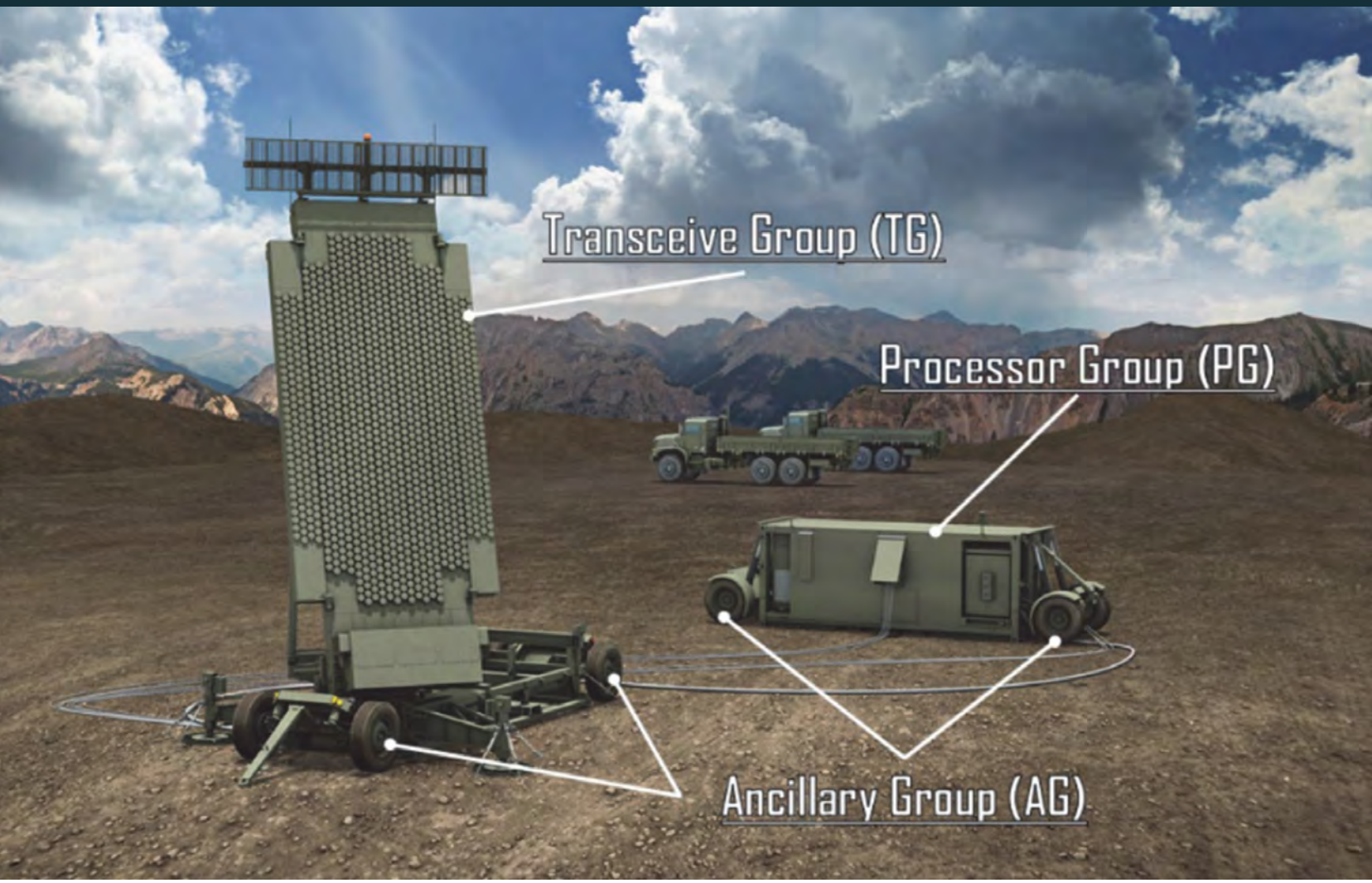
Currently available data are inadequate to provide a survivability assessment. The APT program has made considerable progress to address cyber survivability, which DOT&E identified as a top critical issue in FY22. The APT FoS uses a training data link to connect T-7A aircraft with each other, and to ground based training systems. During FY23, the APT cyber integrated test team conducted an adversarial cyber development assessment of aircraft hardware and a cyber vulnerability identification (CVI) on the APT FoS data link. The test team shared the CVI findings with Boeing, which the contractor used to develop several software updates. The program office continues to pursue material and non-material solutions to other known cyber vulnerabilities. During IOT&E, DOT&E will independently assess cyber survivability to support the T-7A Milestone C and full-rate production decisions.

RECOMMENDATIONS

The Air Force should:

1. Continue addressing AFOTEC periodic report recommendations and make necessary design changes prior to the start of IOT&E.
2. Continue testing the emergency escape system (including canopy bird strike resistance) and implement fixes as needed to meet safety requirements.
3. Support AETC's future efforts to integrate AGCAS capability to reduce safety risks.
4. Incorporate on-aircraft and data link cyber assessments during integrated testing and IOT&E.

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



In February 2022, the Air Force selected Lockheed Martin Corporation 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. The planned start of 3DELRR TPY-4 testing in 4QFY23 has moved to 2QFY24 due to prime contractor production delays. The Air Force plans to start government-led developmental testing in 2QFY24 and dedicated IOT&E in 3QFY25 to support an initial fielding decision in FY25. The Air Force plans to begin mobility testing on Initial Production Radar #1 in 4QFY24 and government developmental testing on IP2 in 1QFY25.

SYSTEM DESCRIPTION

The 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 aircraft and theater ballistic missiles. The 3DELRR employs a single-face, rotating, active electronically scanned array (AESA) with a highly distributed and scalable digital beam-forming architecture.

MISSION

The U.S. Air Force employs the CRC WS to conduct battle management, command and control, air surveillance, combat identification, airspace management, and tactical data link management to enable fluid, continuous, offensive and defense operations. The 3DELRR will support key CRC functions, including:

- Long-range, wide-area surveillance
- Detecting and tracking air-breathing threats and theater ballistic missiles
- Threat evaluation for timely defensive and offensive action
- 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 plans to transition to a major capability acquisition program no earlier than 2QFY24.

» MAJOR CONTRACTOR

- Lockheed Martin Corporation – Syracuse, New York

TEST ADEQUACY

There were no formal government test events in FY23. In 1QFY23, the government observed the contractor's TYQ-23A interface test event. The government plans to observe the validation/verification of requirements and the production acceptance test on Lockheed Martin's performance representative unit in 1QFY24. The start of 3DELRR government-led testing in 4QFY23 moved to 2QFY24 due to prime contractor production delays. The Air Force plans to conduct an operational assessment on a performance representative TPY-4 radar at Eglin AFB in 2QFY24. The 3DELRR T&E Strategy and the 2QFY24 operational assessment test plan are currently in coordination for DOT&E-approval.

The Air Force plans to utilize integrated testing at every opportunity and resource the test for appropriate threat representative targets as part of the planned developmental testing that starts in 2QFY24. The Air Force plans to start dedicated IOT&E in 3QFY25.

PERFORMANCE

» EFFECTIVENESS, SUITABILITY, AND SURVIVABILITY

DOT&E will provide an assessment of the system's potential to be operationally effective, suitable, and survivable in the operational assessment report anticipated in 3QFY24.

RECOMMENDATION

The Air Force should:

1. Plan and resource for appropriate threat representative targets, as recommended in FY22 Annual Report.

Space Force Programs

This page intentionally left blank.

Global Positioning System (GPS) Enterprise

As reported over the course of several years, ongoing development delays of the Next Generation Operational Control System (OCX) are continuing to delay full operational control of the U.S. Space Force's GPS modernized civil, Military Code (M-code), and navigation warfare functions and the fielding of operationally acceptable M-code capable receivers. These delays increase risk that U.S. and allied warfighters will be unable to conduct successful operations in future contested environments due to the lack of access to modernized GPS position, navigation, and timing (PNT) information.

SYSTEM DESCRIPTION

The GPS Enterprise is a Space Force operated satellite-based global radio navigation system of systems that provides accurate and secure PNT information to users worldwide. It consists of three operational segments: space, control, and military user equipment. The space segment includes 31 operational satellites in the GPS constellation that transmit both civilian and encrypted military signals to users. The control segment (primary and alternate sites) operates the GPS constellation; supports launches, anomaly resolution, and disposal operations; and tasks navigation warfare effects in support of combatant commands. The user segment includes the Military GPS User Equipment (MGUE) intended to modernize military GPS receivers, including the ability to receive and use M-code. Beyond military GPS users, there are billions of daily civilian users freely using the civilian signal, including many federal agencies within the U.S. Department of Transportation (DOT) and other various state and tribal agencies.

MISSION

GPS provides PNT information globally to military and civilian users, allowing them to conduct a wide variety of missions. GPS military receivers allow military commanders to navigate and maneuver within strategic, operational, and tactical theaters.

MGUE Increment 1 receivers will allow military users to access the more secure M-code signal, which is currently available for developmental and user equipment testing over the continental United States. MGUE Increment 2 receivers will include the ability to use Regional Military Protection, which will concentrate higher M-code signal power broadcast by GPS III Follow-On Production (GPS IIIF) satellites in a targeted region to ensure the warfighter has continued access to PNT data in contested environments.

PROGRAM

The GPS Enterprise consists of multiple programs pursuing separate acquisition paths to advance the space, control, and user segments.

- GPS III Satellite – An Acquisition Category (ACAT) IC program which achieved Milestone C (MS C) in January 2011. The last of the GPS III satellites, Space Vehicle 10, was made available for launch in December 2022. To date, the Space Force has successfully launched six GPS III satellites since 2018 and plans to launch the seventh satellite in FY24, the eighth in FY25, and the last two GPS III launches in FY26.
- GPS IIIF Satellite – An ACAT IB program. These satellites will provide enhanced Regional Military Protection signals and support for search and rescue services. The Air Force made the GPS IIIF MS C decision in July 2020 following completion of the program's Critical Design Review. The Space Force plans to launch the first GPS IIIF satellite in FY27.
- Operational Control System (OCS) Architecture Evolution Plan (AEP) – The Air Force fielded OCS AEP in 2007. It features two ACAT III upgrades: M-code Early Use (MCEU) and Contingency Operations

(COps). These upgrades allow the system to command and control GPS III satellites and provide core M-code capability from the existing GPS constellation while maintaining previous civilian and military services from older, non-M-code GPS IIR satellites.

- OCX – An ACAT ID program awarded in February 2010 with an initial expected completion date of early 2016. OCX achieved MS B in June 2017 and was relieved of MS C requirements. OCX will provide full control of modernized civil and M-code signals and navigation of warfare functions. OCX will replace OCS AEP following a successful constellation transfer that the Space Force currently plans in March 2025, a delay of 16 months from last year's Annual Report. This 16-month delay is in addition to last year's reporting of a 9-month delay from the FY21 Annual Report. The Space Force plans to operationally accept OCX in July 2025.
- OCX 3F – A tailored ACAT II program that builds on the software delivered by OCX. Contingent on successful OCX deployment, the subsequent OCX Block 3F upgrade will allow OCX to support launch as well as command and control GPS IIIF satellites. The Space Force anticipates delivery from the vendor in FY25 and plans to operationally accept OCX 3F in FY27. Since OCX 3F builds on the software delivered by OCX, corresponding schedule slips to OCX affect operational acceptance and reduce any remaining margin in the OCX 3F delivery schedule.
- MGUE Increment 1 – An ACAT IC program that achieved MS B in January 2017 and was relieved of MS C requirements. The program was designed to deliver personnel- and vehicle-based M-code receivers to the warfighter, including improved GPS signal availability in degraded threat environments. Due to program delays resulting in Application-Specific Integrated Circuit (ASIC) obsolescence and limited production, the Army and Marine Corps will not field their respective MGUE lead platforms (Joint Light Tactical Vehicle and Stryker) with the ground-based MGUE Increment 1 receiver cards. Instead, the Army and Marine Corps plan to use commercially available, MGUE-derived M-code receivers for their ground-based platforms. The commercially derived M-code receivers will undergo user evaluations in fielded platforms outside of the MGUE Increment 1 program of record. The MGUE Increment 1 program delivered an interim functional aviation/maritime receiver card in September 2022. Despite the delivery of subsequent builds, delays continue with both software and hardware builds by MGUE Increment 1 vendors, which impact the operational test schedules for the two remaining MGUE Increment 1 lead platforms (the B-2 aircraft and the *Arleigh Burke*-class destroyer). The B-2 aircraft with this capability is currently scheduled for operational testing in late FY24/early FY25, and the *Arleigh Burke*-class destroyer is scheduled for operational testing in July – August 2025.

- MGUE Increment 2 – The program is structured as two Middle Tier of Acquisition rapid prototyping efforts. The first is the Miniaturized Serial Interface receiver with next-generation ASICs that will deliver improved jam resistance, address MGUE Increment 1 ASIC hardware obsolescence, support the enhanced Regional Military Protection offered by GPS IIIF satellites, and support low-power applications (e.g., guided munitions). The second is the handheld receiver, which will incorporate the Miniaturized Serial Interface receiver with the prototype unit planned for FY27 availability. The Miniaturized Serial Interface development continues to experience challenges, and the handheld unit has technical challenges meeting battery life requirements.

DOT&E approved the GPS Enterprise Test and Evaluation Master Plan (E-TEMP) Revision C in August 2021. The Space Force continues to revise the GPS E-TEMP to update threat requirements, address cyber testing, and define the test strategies for OCX, MGUE Increments 1 and 2, Nuclear Detonation Detection System control system upgrades, GPS IIIF satellites, and OCX Block 3F. DOT&E approved TEMP annexes in February 2023 for the GPS IIIF and OCX 3F programs.

» MAJOR CONTRACTORS

Space Segment

- Lockheed Martin Space – Denver, Colorado (GPS III / IIIF satellites)

Control Segment

- Lockheed Martin Space – Denver, Colorado (OCS AEP)
- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Aurora, Colorado (OCX)
- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – Aurora, Colorado (OCX 3F)

User Segment (MGUE Increment 1 and 2)

MGUE Increment 1 and 2:

- L3Harris Technologies, Inc. – Anaheim, California
- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – El Segundo, California
- BAE Systems – Cedar Rapids, Iowa

MGUE Increment 2 Handheld Device:

- Technology Advancement Group – Ashburn, Virginia
- Raytheon, a subsidiary of RTX (formerly Raytheon Technologies) – El Segundo, California
- BAE Systems – Cedar Rapids, Iowa

TEST ADEQUACY

No operational testing was conducted in FY23 across the GPS Enterprise. The OCX cyber assessment that was scheduled for August 2023 has now been delayed until 4QFY24. The GPS Enterprise IOT&E that had been scheduled to commence in 4QFY23 has now been delayed until FY26.

DOT&E worked with the MGUE Increment 1 Program Office to address concerns identified in the FY22 Annual Report. The program office scheduled and conducted additional suitability testing to verify its updated software corrected encryption key concerns identified during the Joint Light Tactical Vehicle Field User Evaluation in August 2021. After reviewing the data from the evaluation, DOT&E concurs that the program office corrected the problem.

The current MGUE Increment 2 handheld operational test schedule does not align with the GPS IIIF launch strategy. The GPS IIIF family of satellites delivers a Regional Military Protection capability that the MGUE Increment 2 handheld provides to military units. Without GPS IIIF satellites on orbit, operational testers will not be able to verify that the MGUE Increment 2 handheld can take advantage of Regional Military Protection signals in a contested environment.

Currently, M-code is only available within the continental United States. While this is sufficient for initial testing, U.S. and allied forces are only able to test M-code outside of the United States by exception. The United States Space Command is developing a plan to transition military users to M-code as receivers are fielded.

The DOT and the Federal Aviation Administration have responsibilities for testing civilian GPS-based PNT systems outlined in the Federal Radionavigation Plan. OCX Transition office is incorporating DOT's request to test OCX with a four GPS satellite "mini constellation" as a part of the formal constellation transition dress rehearsal. This is a key event, planned for FY25 ahead of full operational testing, to build confidence that OCX will support safe and effective commercial air transportation within the continental United States.

PERFORMANCE

» EFFECTIVENESS

Based on previous operational testing, the current OCS AEP control segment is operationally effective for legacy military signals, legacy civil signals, and M-code signals. GPS operators can command and control all GPS satellites except for the future GPS IIIF satellites. OCS AEP received the Contingency Operations upgrade to command and control the newer GPS III satellites. OCX requires the OCX 3F software upgrade to conduct launch and check out of the GPS IIIF satellites. The Space Force plans to operationally accept OCX in FY25 and OCX 3F in FY27, but the first GPS IIIF satellite is also expected to launch in FY27. Any additional delays of OCX 3F will likely impact the launch of the first GPS IIIF satellite.

Contractor system testing of OCX has been on-going since October 2022, with major delays caused by unstable mission control software, mission simulator, and training systems. Software delays and overall program schedule slips have been mainly due to inadequate contractor testing, incomplete functional integration between various software components, and a lack of Agile coding experience by the contractor during development. The OCX Program Office is working to address these concerns with the contractor in future software deliveries. Space Systems Command leadership has engaged the vendor's senior leadership about the seriousness of these delays.

The MGUE Increment 1 aviation/maritime receiver card experienced software challenges that resulted in delays that the Space Force worked to address. The program is maintaining the current schedule to complete the final program milestone, B-2 Program Executive Officer Certification, in October 2024.

» SUITABILITY

From previous operational test reporting, both GPS III satellites and the OCS AEP command and control system are operationally suitable.

Ongoing OCX contractor and development testing continues to reveal software instability and sustainment concerns with operator training and maintenance technical orders that the program office is working to address. Previous DOT&E Annual Reports noted concerns with the OCX simulator, which the program office has addressed in software updates.

The OCX 3F's first critical capability release adds launch and checkout

capabilities to support the launch of GPS IIIF satellites. Delays to OCX, and consequentially OCX 3F, may put the GPS constellation at risk since OCS AEP will not be able to launch or command and control new GPS IIIF satellites to replenish older satellites as they exceed their service life.

Due to delays with the program, the MGUE Increment 2 Program Office does not have a customer for the MGUE Increment 2 handheld unit. Since operational testing would involve assessing a military unit's ability to carry out their mission using the handheld device, the current lack of a buyer complicates the development of an operational test plan.

» SURVIVABILITY

As part of the recommendations from the 2016 Nunn-McCurdy program breach for OCX, the Air Force implemented additional cyber survivability improvements to OCS AEP due to the expected delay in OCX delivery. Due to these cyber improvements and ongoing further delays to OCX, the current instantiation of OCS AEP may now be more cyber secure than the initial delivery of the OCX system that will eventually replace it. DOT&E plans on performing a cyber survivability comparison and report between OCS AEP and OCX before the U.S. Space Command approves the transfer of the GPS constellation from OCS AEP to OCX in March 2025.

In last year's Annual Report, DOT&E recommended that the Space Force conduct a no-notice transfer of operations from the primary OCX control station at Schriever Space Force Base, Colorado, to the backup at Vandenberg Space Force Base, California. Subsequently, the 2d Space Operations Squadron Commander initiated a no-notice transfer in April 2023 on OCS AEP and is following up on lessons learned from the event. Also mentioned in last year's Annual Report, the GPS IIIF Program Office continues to examine space threats to evaluate the survivability of the latest generation of satellites in a contested space environment.

RECOMMENDATIONS

The Space Force should:

1. Synchronize the GPS IIIF and MGUE Increment 2 handheld programs to provide a realistic environment for fully testing all capabilities.
2. Work with the Services to identify a military unit to operationally use the MGUE Increment 2 handheld who can also support operational testing.
3. Discuss with Air Force senior leaders the mission impacts of fielding MGUE Increment 1 receiver technology that could affect B-2 mission effectiveness and ensure thorough testing of version 7.0 of the MGUE Increment 1 software.
4. Support an operational cyber assessment to compare OCS AEP and OCX cyber survivability scheduled in FY25.
5. Conduct a no-notice transfer of operations from the primary OCX control station at Schriever Space Force Base to the backup at Vandenberg Space Force Base.
6. Adequately address kinetic, cyber, electromagnetic spectrum, nuclear, and directed energy threats in future test plans.

Space Command and Control System (Space C2)

The Space Command and Control (Space C2) program continues to progress toward delivery of capabilities that will allow for the retirement of aging Space Defense Operations Center (SPADOC) infrastructure. In June 2023, DOT&E published a cyber survivability report on Warp Core, Space C2's Data-as-a-Service capability, finding it to be resilient to nascent-level cyber threat actors and to have appropriate defensive response capabilities to address emulated cyber threats on some classification domains. Operational testing of the Advanced Tracking and Launch Analysis System (ATLAS), Space C2's primary Space Domain Awareness Command and Control (SDA C2) capability, which had been planned for FY23, was slowed by delayed capability delivery, system stability problems, lack of trained operators, and non-operationally representative test environments.

SYSTEM DESCRIPTION

The Space C2 system uses a common commercially supported platform to access data and services for user applications that enable command and control operations. Space C2 uses a hybrid cloud, as well as hardware at operations centers, for resiliency and accessibility, and to enable multi-domain operations that are integrated with classified mission partner capabilities.

System capabilities fall into three updated mission-focused product portfolios:

- Space Defense focuses on providing the U.S. Space Command's Joint Task Force – Space Defense (JTF-SD) with operational command and control capability and supporting battle management services for the integration of new and legacy systems to address critical mission needs.
- SDA C2 focuses on developing the next generation of SDA capabilities for the Combined Force Space Component Commander, Space Delta 2, and users at the 18th Space Defense Squadron (18 SDS) and JTF-SD. This portfolio includes ATLAS.
- Cross-Mission Data focuses on providing an enterprise data integration capability that spans the U.S. Space Force (USSF) and DoD user base. This portfolio includes Warp Core.

The system has its own continuous integration/continuous deployment (CI/CD) pipeline, known as Kobayashi Maru, for capability and application development. Space C2's development efforts are primarily focused on delivering the capabilities that will allow for the retirement of the outdated SPADOC.

MISSION

USSF Guardians will use Space C2 to provide a wide range of space defense, SDA C2, 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, 18 SDS, and other command and control centers.

PROGRAM

The Space C2 program was initiated as a Development, Security, and Operations (DevSecOps) pathfinder in 2019, and is continuing to seek designation as a software acquisition pathway (Execution Phase) program. That decision, which had been anticipated in December 2022, is now not expected until 1QFY24 due to delays in closing acquisition decision memorandum-mandated actions related to program documentation. The program, which has been on the DOT&E oversight list since FY19, formally submitted its test and evaluation strategy (TES) in 1QFY23. DOT&E approved the TES in 2QFY23.

In FY22, the Space C2 program restructured its capability development efforts to focus on the near-term challenge of retiring outdated SPADOC infrastructure. The restructure was intended to accelerate delivery of ATLAS capabilities to allow for the decommissioning of SPADOC, while deemphasizing the delivery of non-critical applications. In FY23, the foundational capabilities required to allow for the retirement of SPADOC infrastructure were the focus of product developers. While progress has been made due to the program restructure, product development has been slower than anticipated, and the projected date to decommission SPADOC continues to extend further to late FY24, a delay of more than two years from the original timeline.

The Space C2 program uses an integrated testing construct and has made significant efforts to define how it will accomplish that testing within USSF's new Integrated Test Force model. The program currently implements quarterly integrated testing events to assess SDA C2 capabilities. Despite those efforts, the program struggled to define incremental capability operational acceptance T&E goals and test methodology. To address those problems, USSF chartered the Space C2 Integrated Test Force in September 2023

to implement their vision for the Space Test Enterprise.

» MAJOR CONTRACTORS

Space C2 is comprised of a multitude of contracts and contractors developing capabilities, including:

- Parsons Corporation, Space Operations Division – Centreville, Virginia
- Omitron, Inc. – Colorado Springs, Colorado
- Tecolote Research, Inc. – Goleta, California
- Systems Planning and Analysis, Inc. – Alexandria, Virginia
- The Boeing Company – El Segundo, California
- General Dynamics Missions Systems – Fairfax, Virginia
- Lockheed Martin Corporation – King of Prussia, Pennsylvania
- Peraton, Inc. – Herndon, Virginia
- Palantir Technologies, Inc. – Denver, Colorado
- L3Harris Technologies, Inc. – Colorado Springs, Colorado
- Leidos Inc. – Reston, Virginia
- ManTech – Herndon, Virginia

TEST ADEQUACY

As discussed in the FY22 Annual Report, there were two Space C2 tests planned for early FY23. The first was the cyber adversarial assessment (AA) of Warp Core. The second was the operational utility assessment of ATLAS. USSF conducted the AA of Warp Core in accordance with a DOT&E-approved test plan in October 2022 at Vandenberg Space Force Base, California, with remote participation from McConnell AFB, Kansas, and Schriever Space Force Base, Colorado. The testing was observed by DOT&E, and despite Air Force cyber Red Team limitations, was adequate for DOT&E to assess Warp Core's cyber survivability. Both the Secret and Top Secret capabilities of Warp Core were tested, but activities focused on the Secret capability of Warp Core due to lack of Red Team preparation to assess the Top Secret capability. The AA demonstrated cross-domain solution functionality but did not assess the cyber survivability of the Warp Core cross-domain solution. Additionally, the CI/CD pipeline responsible for developing the applications that reside on Warp Core was also not evaluated for cyber survivability.

While integrated test events for ATLAS occurred in FY23, they did not produce operationally relevant data and cannot be used to meet operational test needs, primarily due to delayed capability delivery, system stability problems, a lack of trained operators, and non-operationally representative test environments. ATLAS operational testing is intended to be phased product release testing, aligned with program increment development timelines (approximately quarterly), executing as integrated tests known as SDA capability integrated tests (SCITs). SCITs are intended to produce usable data for both developmental and operational testing communities; however, the four SCITs conducted in FY23 produced little relevant operational test data. Test activities were primarily useful to the contractor testers, government-led developmental testers, and numerical validation analysts responsible for ensuring ATLAS accuracy meets the minimum legacy program standards.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

No data to inform an assessment of operational effectiveness or suitability was collected for the Space C2 program in FY23.

» SURVIVABILITY

Warp Core is resilient to nascent-level cyber threat actors and has appropriate defensive response capabilities to address the emulated cyber threats on some security domains. The Red Team could not penetrate the Warp Core infrastructure and could not generate any cyber effects against Warp Core or its end users by using nascent-level techniques in any of the postures. Since the Red Team was not able to compromise the system or produce any effects, they requested that the program office and the system developer (Palantir Technologies, Inc.) fabricate a cyber compromise of system data in order to capture end-user responses and mission effects during the test. Those fabricated data scenarios resulted

in successful detection of modified data by end-users, leading them to employ appropriate actions to notify supervisors of the discovery and proceed with proper prevention/mitigation procedures.

Other survivability findings dealt with known configuration issues for classified security domains and were not directly attributable to Warp Core.

Full details are included in the DOT&E Space C2 Warp Core Cyber Survivability Report and classified annex published in June 2023.

RECOMMENDATIONS

The USSF should:

1. Ensure the organizations responsible for future cyber survivability assessments of Space C2 capabilities are appropriately prepared and resourced to provide threat-representative cyber activities, including those related to commercial cloud assessments.
2. Perform additional government-led cyber survivability testing of Space C2 capabilities, including the CI/CD pipeline and cross-domain solutions, as part of major capability releases, once all relevant external users, data feeds, and operational applications are finalized across each applicable security domain.
3. Continue to refine the Integrated Test Force construct to define common T&E goals and methodology across all USSF programs in order to satisfy the equities of all T&E stakeholders.
4. Continue focused efforts on development and adequate operational testing of SDA capabilities required to complete the SPADOC decommissioning.
5. Continue to fund the assignment of cyber defenders for Space C2-related capabilities.

U.S. SPECIAL OPERATIONS COMMAND PROGRAMS

This page intentionally left blank.

Dry Combat Submersible (DCS)

In October 2023, DOT&E issued a classified IOT&E report following the completion of IOT&E of the Dry Combat Submersible (DCS) in April 2023. DCS is operationally effective within limited operational environments and with limited mission capability. DCS is not operationally suitable. DOT&E's assessment of DCS cyber survivability is contained in the classified IOT&E report.

SYSTEM DESCRIPTION

The DCS is a 39.4-foot long, dry submersible with lock-in/lock-out capability for up to eight special operations forces (SOF) occupants. The DCS is battery-powered and operated by two pilots. The DCS maintains a one-atmosphere dry environment within the personnel compartments.

MISSION

U.S. Special Operations Command (USSOCOM) developed DCS to provide Special Operations Forces (SOF) with an undersea mobility material solution for use in relevant special operations environments. The program will provide three DCS's for SOF.

PROGRAM

DCS is an Acquisition Category III program managed by USSOCOM. DCS achieved Milestone C in 2018 and DOT&E approved a Test and Evaluation Master Plan update the same year. The Navy ended IOT&E in April 2023 and intends an FOT&E of the DCS in FY24. USSOCOM declared initial operational capability in June 2023.

» MAJOR CONTRACTOR

- Lockheed Martin Rotary Mission Systems – Riviera Beach, Florida

TEST ADEQUACY

The Navy completed IOT&E of DCS in April 2023. Testing was in accordance with DOT&E approved test plans and DOT&E observed all test events. Testing was adequate to determine operational effectiveness and suitability, as well as cyber survivability of DCS against nearsider and insider threats. Testing did not assess cyber survivability against outsider threats because the test plan specified evaluation through a program protection analysis. DOT&E submitted a classified IOT&E report in October 2023.

PERFORMANCE

» EFFECTIVENESS

DCS is operationally effective within limited operational environments and with limited mission capability. Details are in the classified IOT&E report.

» SUITABILITY

DCS is not operationally suitable. Details are in the classified IOT&E report.

» SURVIVABILITY

DCS survivability assessment in a cyber-contested environment is classified. Details are in the classified IOT&E report.

RECOMMENDATIONS

USSOCOM should:

1. Address recommendations included in the classified IOT&E report.
2. Submit an FOT&E test plan for DOT&E approval.

MISSILE DEFENSE SYSTEM

BMD - Ballistic Missile Defense
BLK - Block
MPQ - Mobile, Position Locating, Special Purpose
SM - Standard Missile

SPY - Surface Ship Radar Surveillance
TPY - Transportable Radar Surveillance
UEWR - Upgraded Early Warning Radar

Missile Defense System (MDS)

The Ground-based Midcourse Defense (GMD) weapon system has demonstrated the capability to defend the U.S. homeland from a small number of ballistic missile threats with ranges greater than 3,000 kilometers and employing simple countermeasures when supported by the full architecture of Missile Defense System (MDS) sensors. The Regional/Theater MDS has demonstrated the capability to defend the U.S. Indo-Pacific Command (USINDOPACOM), U.S. European Command (USEUCOM), and U.S. Central Command (USCENTCOM) areas of responsibility 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, most of which were outlined in the FY22 Annual Report, for the MDS are: 1) the need for realistic and emerging threat representations in flight and ground testing; 2) the need for an adequate, accredited federation of modeling and simulation (M&S) with well understood and documented limitations to assess MDS effectiveness; 3) susceptibility of the MDS to cyberattack; 4) interoperability and maturation of engagement coordination; and 5) the need for test range infrastructure and instrumentation upgrades.

In FY23, the Missile Defense Agency (MDA) continued testing three significant new MDS capabilities:

- Aegis Ballistic Missile Defense (BMD) capability to detect, track, engage, and intercept a medium range ballistic missile (MRBM) target in the terminal phase of flight using a single salvo of two Standard Missile-6 (SM-6) Dual II Software Upgrade interceptors.
- Aegis Ashore Missile Defense System-Poland integration into the MDS.
- Initial Long Range Discrimination Radar (LRDR) performance through flight and ground testing in support of U.S. homeland defense and space domain awareness.

MDA started testing a significant new MDS capability of space domain awareness using the Army Navy/Transportable Radar Surveillance (Forward Based Mode) (AN/TPY-2 (FBM)) capability to detect, track, and report on resident space objects.

MDA delivered upgrades to the GMD Weapon System; Command and Control, Battle Management, and Communications; and the Sea-Based X-Band Radar (SBX) in FY23 that increase battlespace for the warfighter and improve network communication paths.

DOT&E will provide additional information and recommendations in the classified FY23 DOT&E Assessment Report of the MDS to be published in February 2024.

SYSTEM DESCRIPTION

The MDS is a geographically distributed system of systems that relies on element interoperability and warfighter integration for combat capability and efficient use of guided missile/interceptor inventory. As shown in Table 1, the MDS consists of six weapon systems, a sensor architecture (i.e., terrestrial, maritime, and global sensors), and a command and control element.

Table 1. Elements of MDA's Missile Defense System

Type	U.S. Homeland Defense	Global Regional/Theater Defense	Hypersonic Defense
Weapon Systems	**GMD[a]:** Defends the U.S. homeland against IRBM/ICBM attacks using GBIs to defeat threat missiles during the midcourse segment of flight. The MDA is developing a Next Generation Interceptor to 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 exo-atmospheric ballistic missile threats alongside SM-6 guided missiles that Aegis SBT (Inc 2 and Inc 3) 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 allies from SRBM and MRBM threats and aircraft attack and defeats enemy air assets. It is a mobile air and missile defense system employing a mix of PAC-3 hit-to-kill interceptors and PAC-2 blast fragmentation warhead interceptors.	**Aegis SBT (Inc 3)[a]:** Provides critical asset protection at sea and for joint forces ashore against ballistic, maneuverable, and hypersonic glide threats in the terminal phase. **GPI[a]:** Provides an additional layer of hypersonic defense augmenting Aegis SBT (Inc 3) to increase depth of fire against hypersonic threats. The program is currently competitively developing two prototype interceptors.
Terrestrial and Maritime Sensors	**Cobra Dane Radar[d]:** L-band fixed site phased array radar. **UEWRs[d]:** Ultrahigh frequency fixed site phased array radars. **SBX[a]:** X-band mobile phased array radar located aboard a self-propelled, ocean-going platform. **LRDR[a]:** S-band two-face fixed site phased array radar.	**AN/SPY-1 Radar[c]:** S-band four-face radar providing Aegis long-range surveillance and track functions in addition to guided missile engagement support. **AN/SPY-6(V)1 Radar[c]:** S-band four-face radar being installed on new construction Aegis DDG 51 Flight III destroyers. It will extend Aegis threat detection ranges and provide simultaneous ballistic missile and air defense support. **AN/TPY-2 (FBM) Radar[a]:** X-band single-face transportable phased array radar that also supports U.S. homeland defense. **LTAMDS[b]:** C-band three-face multi-function, multi-mission radar interfacing with IBCS and supporting interoperability with PAC-3.	Leverages U.S. homeland defense, global regional/theater defense, and global sensors.
Global Sensors	**SBIRS[d]:** Satellite constellation of infrared sensors. **BOA[a]:** Element that combines OPIR observations to provide missile event and track reports to C2BMC. **SKA[a]:** Network of space sensors providing interceptor hit assessments. **HBTSS[a]:** Network of space sensors to detect and track both ballistic and hypersonic threats and provide fire-control quality data to MDS sensors and weapon systems. MDA is planning to launch prototypes in 1QFY24.		
Command and Control	**C2BMC[a]:** Integrating element within the MDS providing deliberate and dynamic planning, situational awareness, sensor track management, engagement support and monitoring, data exchange between elements, and network management. C2BMC also directs sensor tasking for the LRDR, AN/TPY-2 (FBM) radars and provides cueing support to BOA.		

Notes:
[a] Under MDA development/sustainment. [b] Under Army development/sustainment. [c] Under Navy development/sustainment. [d] Under Space Force development/sustainment.

Acronyms: AN/SPY - Army Navy/Surface Ship Radar Surveillance; AN/TPY – Army Navy/Transportable Radar Surveillance; BMD – Ballistic Missile Defense; BMDS – Ballistic Missile Defense System; BOA – BMDS Overhead Persistent Infrared Architecture; C2BMC – Command and Control, Battle Management, and Communications; FBM – Forward-Based Mode; GMD – Ground-based Midcourse Defense; GBI – Ground-Based Interceptors; GPI – Glide Phase Interceptor; HBTSS – Hypersonic and Ballistic Tracking Space Sensor; IAMD – Integrated Air and Missile Defense; IBCS – IAMD Battle Command System; ICBM – Intercontinental Ballistic Missile; Inc – Increment; IRBM – Intermediate-Range Ballistic Missile; LRDR – Long Range Discrimination Radar; LTAMDS – Lower Tier Air and Missile Defense Sensor; MDA – Missile Defense Agency; MDS – Missile Defense System (formerly BMDS); MRBM – Medium-Range Ballistic Missile; OPIR – Overhead Persistent Infrared; PAC – Patriot Advanced Capability; SBIRS – Space-Based Infrared System; SBT – Sea-Based Terminal; SBX – Sea-Based X-band Radar; SKA – Space-Based Kill Assessment; SM – Standard Missile; SRBM – Short-Range Ballistic Missile; THAAD – Terminal High Altitude Area Defense; UEWR – Upgraded Early Warning Radar

MISSION

The Commanders of U.S. Northern Command (USNORTHCOM), USINDOPACOM, USEUCOM, and USCENTCOM employ the assets of the MDS to defend the United States, deployed forces, and allies against missile threats at all ranges and in all phases of flight.

PROGRAM

The MDS is a single Acquisition Category (ACAT) ID program that encompasses five of its six weapon systems (all but Patriot), most of its sensor architecture, and its command and control element. In 2002, the 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 mission of MDA is to develop and deploy a layered MDS to defend the United States, its deployed force, allies, and friends from missile attacks in all phases of flight.

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 September 2023 (version 25.0).

The Army manages the Patriot and Lower Tier Air and Missile Defense Sensor (LTAMDS) programs. Patriot is an ACAT IC program. DOT&E approved the Patriot Post Deployment Build (PDB) 8.1 Test and Evaluation Master Plan (TEMP) in FY20. LTAMDS is a Middle Tier of Acquisition program for rapid prototyping; the Army expects to designate LTAMDS as an ACAT-1C at its Materiel Development Decision now planned for January 2025, delayed by approximately a year because of integration challenges and supply chain delays. DOT&E approved the LTAMDS initial TEMP in 2019. The program office continues to develop a Test and Evaluation Strategy, with DOT&E approval now expected in 1QFY24.

The Navy manages the AN/SPY-1 and AN/SPY-6(V)1 radar programs. The AN/SPY(6)1 is an ACAT IC program. DOT&E approved its TEMP in September 2022.

The Space Force operates and sustains four sensor systems integrated into the MDS: Cobra Dane Upgrade, five Upgraded Early Warning Radars (UEWRs), the Space-Based Infrared System (SBIRS) constellation, and the LRDR. The Air Force completed development and initial operational testing for the first three sensor systems prior to them becoming Space Force assets. The Space Force has not yet operationally accepted the LRDR. In FY23, DOT&E placed the UEWRs under oversight.

» 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 "Black" AUR through Critical Design Review: Huntsville, Alabama (Note: Black and Gold denote the two NGI contractor teams)
  - 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: Huntsville, Alabama
  - GBI Boost Vehicles: Chandler, Arizona
  - NGI "Gold" AUR through Critical Design Review and GPI: Huntsville, Alabama

  - BOA: Boulder, Colorado; Colorado Springs, Colorado; and Azusa, California
  - HBTSS through Prototype Demonstration Phase: Redondo Beach, California and Azusa, California
- RTX (formerly Raytheon Technologies)
  - GMD EKV, SM-3/6 Interceptors, LTAMDS, and GPI: Tucson, Arizona
  - Patriot Ground System and PAC-2 interceptor variants, AN/SPY-6(V)1 radar, AN/TPY-2 radar, SBX radar, and UEWRs: Tewksbury, Massachusetts
  - Cobra Dane Radar: Dulles, Virginia
- L3Harris Technologies
  - HBTSS through Prototype Demonstration Phase: Fort Wayne, Indiana
- Johns Hopkins University, Applied Physics Laboratory
  - SKA: Laurel, Maryland

TEST ADEQUACY

The MDA IMTP focuses on collecting the flight, ground (e.g., hardware-in-the-loop), 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 some events experienced technical and programmatic delays. Table 2 outlines the 31 flight, ground, high-fidelity M&S, and cyber survivability test events that the MDA performed or participated in during FY23. For each test event in Table 2, the footnotes indicate whether DOT&E approved the test plan and whether DOT&E observed the event.

Table 2. FY23 Testing

Date	Test	Mission Area	Description
June 2022 to October 2023	Patriot PDB-8.1 LUT[a,d]	Regional/Theater Defense	The Army conducted this OT to assess the effectiveness, suitability, and survivability of the Patriot PDB-8.1 system through flight test, accredited HWIL scenarios, and cyber survivability testing (CVPA and AA).
September 2022 to January 2023	SM-3 Block IIA M&S OT Runs for Record, Phase 2A[a,d]	Regional/Theater Defense	The MDA executed and delivered a set of high-fidelity M&S runs to assess Aegis BMD remote and organic engagement performance against select threats in scenarios relevant to the USINDOPACOM area of responsibility.
October 2022	Live Radiate-08a Part 1[c,e]	Space Domain Awareness	The MDA conducted this live-radiate test to collect data of the AN/TPY-2 (FBM) radar space domain awareness capabilities in an operational environment.
October 2022	Ground Test Distributed-08a (USNORTHCOM/ USINDOPACOM) Part 1[c,e]	Homeland Defense and Regional/Theater Defense	The MDA and the MDS OTA conducted this DT/OT using distributed operational assets and HWIL laboratory test assets supporting MDS capability assessment in USNORTHCOM/USINDOPACOM geographic regions, examining new functions of LRDR, C2BMC, GMD, SBX, BOA, Aegis BMD, THAAD, and AN/TPY-2 (FBM).
October 2022	High Operational Tempo for Hypersonics Campaign-2[c,e]	Hypersonic Defense	The MDA participated in this joint Service flight test event, collecting data on new technologies in hypersonic environments.

Table 2. FY23 Testing, continued

Date	Test	Mission Area	Description
November 2022	Japan Flight Test Aegis Weapon System-07[c,d]	Regional/Theater Defense	The MDA and the Japan Maritime Self-Defense Force cooperatively demonstrated SM-3 engagement capabilities in four live fire events including two intercept events with Japanese destroyers. In the first intercept event, an SM-3 Block IIA engaged an MRBM target. The second intercept event was an integrated air and missile defense scenario whereby SM-3 Block IB Threat Upgrade and SM-2 Block IIIB missiles engaged an SRBM target and a cruise missile, respectively.
November 2022	Hypersonic Air Breathing Weapon Concept Flight Test-3[c,e]	Hypersonic Defense	The MDA participated in this DARPA event to collect hypersonic missile phenomenology and tracking data to inform future capability development.
November 2022	System Integration and Checkout-09-1 (USEUCOM/ USCENTCOM)[c,e]	Regional/Theater Defense	The MDA executed a limited architecture distributed event utilizing operational assets and focused on the verification of operational communication and message flows of theater/regional capabilities.
December 2022	Ground Test Integrated-08a (USNORTHCOM/ USINDOPACOM) Part 2[c,e]	Homeland Defense	The MDA and the MDS OTA conducted this follow-on DT/OT using HWIL laboratory test assets to support assessment of U.S. homeland defense MDS capabilities in the USNORTHCOM/USINDOPACOM geographic regions, focusing on GMD and C2BMC.
December 2022	Ground Test Distributed-07b (Aegis Ashore)[c,e]	Regional/Theater Defense	The MDA and the MDS OTA team conducted this DT/OT using distributed operational assets and HWIL laboratory test assets to support assessment of MDS capabilities in the USEUCOM geographic regions with a focus on Aegis Ashore integration and interoperability.
December 2022	Air-Launched Rapid Response Weapon AUR Test Flight-1[c,e]	Hypersonic Defense	The MDA participated in this Air Force event to collect hypersonic missile phenomenology and tracking data to inform future capability development.
January to December 2023	UEWR 22-1 Upgrade[a,e]	Homeland Defense	STARCOM conducted OT on each of the five UEWRs to evaluate the operational effectiveness, suitability, and survivability of those systems after the 22-1 upgrade.
January 2023	Ground Test Integrated-23 Sprint 1 (USNORTHCOM/ USINDOPACOM)[c,e]	Homeland Defense	The MDA executed an HWIL event collecting data supporting the assessment and fielding decisions of the upgraded IDT 8B.8, LMS 8C.1, GFC 8A.6.4 and GCN 8B.8 capability.
February 2023	SICO-09-2 (USEUCOM/ USCENTCOM)[c,e]	Regional/Theater Defense	The MDA executed a limited architecture distributed event utilizing operational assets and focused on the verification of operational communication and message flows of theater/regional capabilities.
February to March 2023	GMD/C2BMC/BOA Cyber Event[b,d]	Homeland Defense	The MDS OTA team, the MDA, and the U.S. Army's DEVCOM and TSMO performed cyber events at Fort Greely, Alaska; Schriever Space Force Base, Colorado; and Fort Drum, New York to assess outsider, insider, and nearsider threat postures. DOT&E did not approve the test plan because of critical limitations to test adequacy.

Table 2. FY23 Testing, continued

Date	Test	Mission Area	Description
March 2023	SICO-23 (N/I)[c,e]	Regional/Theater Defense	The MDA executed a limited architecture distributed event utilizing operational assets to support assessments and fielding of the upgraded IDT 8B.8, LMS 8C.1, GFC 8A.6.4 and GCN 8B.8 capability.
March 2023	Flight Test Aegis Weapon System-31 Event 1a[c,d]	Regional/Theater Defense	The MDA demonstrated an Aegis BMD capability to detect, track, engage, and intercept an MRBM target in the terminal phase of flight using the SM-6 Dual II with Software Upgrade in a single salvo of two interceptors fired at the target. Software Upgrade introduces select SBT Increment 3 capabilities into the Dual II missile.
March 2023	Patriot PDB 8.1 OT-3[a,e]	Regional/Theater Defense	The Army demonstrated the capability of the Patriot PDB-8.1 system to detect, track, engage, and intercept an MRBM with MSE interceptors.
March 2023	Ground Test Integrated-09 Sprint 2 (USEUCOM/ USCENTCOM)[c,e]	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, Aegis BMD, THAAD, and Patriot.
March 2023	XBR 4.2 CVPA/ AA-08b (N/I)[a,d]	Homeland Defense	The MDS OTA, the MDA, and the U.S. Army DEVCOM and TSMO performed a CVPA and AA on the SBX XBR to assess insider and nearsider threat postures.
April 2023	Glory Trip-246[c,e]	Homeland Defense	The MDA participated in this Air Force Global Strike Command event to collect data, exercise MDS communication links, and perform future capability assessments.
May 2023	Formidable Shield-23[c,e]	Regional/Theater Defense	NATO forces executed this live fire exercise to build joint interoperability and demonstrate command and control in integrated air and missile defense scenarios. Two Aegis BMD destroyers detected and tracked SRBM targets during the exercise.
May 2023	Ground Test Integrated-103[c,e]	Regional/Theater Defense	The MDA conducted this limited architecture DT to characterize Aegis BMD cued acquisition with BOA and C2BMC using Common Interactive Broadcast and Link 16.
June 2023	Live Radiate-08a Part 2[c,e]	Space Domain Awareness	The MDA conducted this live-radiate test to collect data on the space domain awareness capabilities of the LRDR radar in an operational environment.
July 2023	SICO-08a-2 (USNORTHCOM/ USINDOPACOM)[c,e]	Homeland Defense	The MDA executed a limited architecture distributed event utilizing operational assets and focused on the verification of operational communication and message flows of theater/regional capabilities.
August 2023	Aegis Ashore MDS-Poland CVPA/AA[a,d]	Regional/Theater Defense	The MDA supported a cyber-survivability evaluation of the Aegis Baseline 9.B2.1 at the facility Poland. The assessment included outsider, insider, and nearsider threat postures.
August 2023	Patriot PDB 8.1 DT-1d[c,e]	Regional/Theater Defense	The Army demonstrated the capability of the Patriot PDB-8.1 system to detect, track, engage, and intercept a subscale aircraft target employing electronic attack with an MSE interceptor.

Table 2. FY23 Testing, continued

Date	Test	Mission Area	Description
August 2023	Flight Test Other-26[a,d]	Homeland Defense	The MDA conducted an OT of the LRDR to assess its ability to detect, track, and discriminate an operationally representative target. A target anomaly resulted in a no test.
September 2023	Flight Test Other-49[c,e]	Homeland Defense	The MDA conducted a tracking exercise for UEWR Clear, SBX, and LRDR in a non-OT.
September 2023	LTAMDS DT Missile Flight Test – Patriot-as-a-Target[c,e]	Regional/Theater Defense	The Army demonstrated the capability of a unit equipped with LTAMDS to detect, track, and engage a close range ballistic missile target with two PAC-3 CRI missiles. Sensor/Interceptor communication issues and range safety constraints prevented intercept of the target.
September 2023	Glory Trip-247[c,e]	Homeland Defense	The MDA participated in this Air Force Global Strike Command event to collect data, exercise MDS communication links, and perform future capability assessments.

Notes:
[a] Testing performed per DOT&E-approved test plan. [b] Test plan not approved by DOT&E. [c] Test plan not required by DOT&E. [d] Test observed by DOT&E. [e] Test not observed by DOT&E.

Acronyms: AA – Adversarial Assessment; AN/TPY - Army Navy/Transportable Radar Surveillance; AUR – All-Up Round; BMD – Ballistic Missile Defense; 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 Test; FBM – Forward-Based Mode; FY – Fiscal Year; GCN – GMD Communications Network; GFC – GMD Fire Control; GMD – Ground-based Midcourse Defense; HWIL – Hardware-in-the-Loop; IDT - In-Flight Interceptor Communication System (IFICS) Data Terminal; LMS – Launch Management System; LRDR – Long Range Discrimination Radar; LTAMDS – Lower Tier Air and Missile Defense Sensor; LUT – Limited User Test; M&S – Modeling and Simulation; MDA – Missile Defense Agency; MDS – Missile Defense System; MRBM – Medium-Range Ballistic Missile; MSE – Missile Segment Enhancement; NATO – North Atlantic Treaty Organization; OT – Operational Test; OTA – Operational Test Agency; PAC – Patriot Advanced Capability; PDB – Post Deployment Build; SBT – Sea-Based Terminal; SBX – Sea-Based X-band Radar; SICO – System Integration and Checkout; SM – Standard Missile; SRBM – Short-Range Ballistic Missile; STARCOM – Space Training and Readiness Command; 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; XBR – X-Band Radar

As previously reported, the need for additional threat representations, independently accredited M&S, and system survivability data in a cyber-contested environment presents significant challenges for DOT&E in completing a comprehensive assessment of the MDS. Specifically:

- Realistic and up-to-date representations of threat missile scenes are critical to the assessment of MDS performance. As DOT&E has noted since FY21, the rate of adversary threat development is currently faster than the pace of flight test target and ground test high-fidelity M&S threat model development. The MDA has made advancements to their threat modeling process, but models can still take several years to develop.
- Independent accreditation of M&S used in ground tests and high-fidelity analyses to ensure M&S can adequately represent current threat missile capabilities, electronic attack, countermeasures, post-intercept debris, and realistic raid sizes. DOT&E has emphasized this need in previous annual reports. The rate at which the MDA's models have been independently accredited has increased, but significant gaps remain. While over 90 percent of element sensor models are accredited, critical components

like newer threat models and post-intercept debris remain unaccredited. MDA and the MDS OTA are laying the foundation to accredit the End-to-end Digital Integrated System-level Simulation, which is a new MDS-level high-fidelity digital modeling architecture that presents a different set of challenges, once sufficient element assets are incorporated into it.

The MDS is a large system of systems with an extensive cyberattack surface. As noted in previous annual reports, the MDS OTA should focus on improving cyber test planning collaboration with DOT&E to ensure test adequacy, in particular by submitting test plans to DOT&E for approval at least 60 days prior to the test event and by ensuring these test plans include sufficient test lengths to assess system cyber survivability. Overall, more operationally realistic testing is needed both at the element- and the MDS-level to characterize MDS cyber survivability and identify potential areas for improvement. Periodic cyber Red Team events, emulating advanced adversaries, are needed to ensure MDS cyber defenses are and remain adequate to protect MDS missions. MDA is developing an action plan for persistent cyber operations (PCO) assessments of their internal and external networks. PCOs are the best way to emulate advanced cyber threats and find and fix mission-critical vulnerabilities.

Flight and ground test programs and high-fidelity M&S analyses at both the system- and element-level have been limited in the variety of realistic threat countermeasures, electronic attack, post-intercept debris scenes, raid sizes, and multi-element engagement scenarios. As reported in DOT&E's FY22 Annual Report, the MDA often designs flight tests to demonstrate a specific new capability, not for operational realism. Operationally realistic intercept flight tests are necessary to provide: 1) needed referent data to support verification, validation, and accreditation of models used in high-fidelity M&S and ground testing; 2) realistic data on multi-element interactions; and 3) data in multi-domain operations.

The Army as the lead Service, with MDA and the Navy, is currently developing a concept for a persistent, 360-degree, layered and 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 integration and test planning challenge. DOT&E assesses that the current test strategy needs significant 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

» U.S. HOMELAND MISSILE DEFENSE

With the support of the full architecture of MDS sensors, the GMD weapon system has demonstrated the capability to defend the U.S. homeland from a small number of ballistic missile threats employing simple countermeasures and with ranges greater than 3,000 kilometers. In FY23, the MDA tested the ability of the newly constructed LRDR to track and discriminate a ballistic missile target. The Space Force plans to operationally accept LRDR no later than 2QFY25.

In FY23, the MDA continued development of an emerging-target lethality model for future lethality assessments based on ground-based interceptor hypervelocity impact testing conducted in FY22.

» REGIONAL/THEATER MISSILE DEFENSE

The regional/theater MDS has demonstrated a capability to defend the USINDOPACOM, USEUCOM, and USCENTCOM areas of responsibility from a small number of 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 the capability to 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, threat features, 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. Flight testing in FY23 verified some of the corrective actions 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. The SM-3 Block IIA missile is reliable as it meets its threshold reliability metric, but not with statistical confidence because of the relatively small number of live firings and ground test data collection events to date. The MDA has implemented 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 demonstrated the capability to intercept and destroy ballistic missiles of varying types (short- to intermediate-range) inside or outside the earth's atmosphere during the terminal phase of flight, although the flight testing and M&S still need to address more complex engagement conditions and realistic raid scenarios. In FY23, the MDA indefinitely postponed a planned THAAD flight test due to the operational status of the AN/TPY-2 radar. The MDA is now planning for execution in FY24. The MDA and the Army continue to address THAAD training and component reliability shortfalls. In addition, the MDA continues to develop and deploy updates to the THAAD software for both the radar and THAAD Fire Control and Communications.

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 continues to address shortfalls in reliability, training, and survivability. The Patriot PDB-8.1 Limited User Test (LUT) will assess how Patriot effectiveness, suitability, and survivability have changed since the last Patriot operational test that concluded in April 2019. DOT&E will publish the results of the PDB-8.1 LUT in a separate classified report in 1QFY24.

As reported in the FY22 DOT&E Annual Report, the Patriot M&S representations for ground tests used the new Battalion Simulation under development by the Army, but the Army has not yet provided sufficient verification and validation evidence to accredit the 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 FY23, AN/SPY-1 demonstrated the capability to detect and track SRBMs and MRBMs during live intercept flight tests. The AN/SPY-6(V)1 radar prototype at the Pacific Missile Range Facility Barking Sands, Hawaii continues to track all classes of ballistic missiles, as available, during MDS flight tests. In FY23, AN/TPY-2 (FBM) demonstrated the capability to detect, track, and report on resident space objects based on space domain awareness tasking received by C2BMC during a live radiation event.

» HYPERSONIC MISSILE DEFENSE

The MDA collected hypersonic test data throughout FY23 to inform future sensors, sensor detection and tracking algorithms, and M&S validation. The MDA also conducted ground hypersonic impact, thermal, and aerodynamic testing to support the development of the M&S architecture specifically for hypersonic missile defense.

» COMMAND AND CONTROL AND SPACE SENSORS

Almost every FY23 test conducted by the MDA included space sensors acquiring, tracking, and reporting on observed objects. C2BMC globally and regionally integrates and synchronizes autonomous sensors, weapon systems, and operations. C2BMC is also a part of all system ground and flight tests, which verify and exercise current and future MDS capabilities. In FY23, C2BMC and BOA continued to support real-world situational awareness in USEUCOM. In two events in FY23, C2BMC communicated with Space Command and Control for space domain awareness, tasking LRDR and

AN/TPY-2 (FBM) and receiving reports back from the radars on resident space objects.

RECOMMENDATIONS

The MDA should:

1. Continue to increase the rate of regional/theater and U.S. homeland defense 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 high-fidelity analyses and ensure M&S can adequately represent current threat missile capabilities, electronic attack, countermeasures, post-intercept 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 provide referent data to support verification, validation, and accreditation of the models representing post intercept debris.
4. Ensure comprehensive cyber test and evaluation plans are created and developmental and operational cyber testing is completed prior to capability delivery to the warfighter.
5. Continue to work with DOT&E and combatant commands to conduct PCOs – Red Teams emulating advance adversaries – across MDS systems and networks.
6. Coordinate with the Army and Navy to 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, as well as fully fund the verification and validation efforts for the model.
2. Coordinate with MDA to ensure the test strategy for the defense of Guam incorporates multi-element interoperability and coordination into intercept flight testing.

DOT&E-MANAGED ACTIVITIES

This page intentionally left blank.

Center for Countermeasures (CCM)

In FY23, the Center for Countermeasures (CCM) performed 39 test events in support of the following: 1) evaluation of aircraft-based countermeasures (CMs) and vehicle protection systems, 2) evaluation of counter-unmanned aircraft systems (C-UASs), 3) development and evaluation of directed energy weapons (DEW) for potential use as CMs and counter-CMs, 4) pre-deployment training with CMs, 5) data collection for threat characterization to advance the threat representation to CMs, and 6) development and fielding of unique instrumentation for CM testing. CCM also partnered with allies on project arrangements to advance the infrared (IR) and radio frequency (RF) threat CMs development and testing.

PROGRAM OVERVIEW

CCM was established and chartered in 1972 by OSD to address the emergence of more technologically advanced weapons systems, including rapid development of terminally guided weapons and CMs. In 1999, management and responsibility of the CCM program was transferred to DOT&E from the Deputy Director, Defense Research Engineering Test and Evaluation. Today, CCM operates and deploys mobile testing instrumentation capable of simulating an array of threats to measure and evaluate the operational effectiveness of CMs employed by DoD and foreign weapon systems. The portability of CCM test tools and personnel provide the test agility and efficiency required by DoD to develop and field critical CMs at operationally relevant speeds, minimizing the logistical burden on each program office and preserving schedules and resources.

MISSION

CCM expedites the development and fielding of CMs and counter-CMs employed by U.S. systems by supporting T&E activities with portable instrumentation. CCM supports the T&E community by preparing for future needs in DoD emerging technology areas, such as DEWs, cyber, hypersonic, and space CMs. Additionally, CCM leverages allies' support to advance T&E of IR and RF threat CMs. CCM also provides the threat environment for pre-deployment training to ensure warfighters are trained in a combat representative environment.

FY23 KEY ACTIVITIES

» T&E OF AIRCRAFT AND VEHICLE PROTECTION CMs

In FY23, CCM generated more than 20,000 threat missile plume signatures and executed 14 tests (12 aircraft and 2 vehicle protection system tests). These efforts expedited development and fielding of several Quick Reaction Capability programs as well as hardware and software upgrades of

fielded systems against IR-guided, RF-guided, and/or laser threats. Testing included the following:

Common Infrared Countermeasure (CIRCM)

CCM facilitated testing that resulted in the fielding of upgraded CIRCM solutions. CCM supported a CIRCM Jupiter risk reduction test with the Common Missile Warning System (CMWS) required to increase the survivability of rotary-wing aircraft. CCM also tested software upgrades to the CIRCM system integrated with the Advanced Threat Warner (ATW) in support of Army and Navy efforts to improve survivability of rotary-wing aircraft. Additionally, CCM supported an initial integration verification flight test of the CIRCM as installed on the HH-60V aircraft.

Common Missile Warning System (CMWS)

CCM supported the HH-60W IOT&E equipped with the CMWS that evaluated the aircraft's operational effectiveness.

Limited Interim Missile Warning System (LIMWS)

CCM supported two events with LIMWS Quick Reaction Capability flight testing: 1) a test to provide the data necessary to support a fielding decision on rotary-wing aircraft, and 2) a tower test to support a preliminary operational assessment of missile warning systems (MWSs) in development.

Large Aircraft Infrared Countermeasure (LAIRCM)

CCM supported initial integration verification flight test of the Department of Navy LAIRCM ATW, as installed on the CH-53K. Additionally, CCM supported the LAIRCM ATW system upgrade performance testing to evaluate changes to the survivability of C-40A aircraft. CCM also participated in a pre-deployment test event to evaluate the systems' operational effectiveness.

Distributed Aperture Infrared Countermeasure (DAIRCM)

CCM supported a pre-deployment test to evaluate the DAIRCM's operational effectiveness.

Future Missile Warning System (MWS) Development Testing

CCM facilitated the assessment of the current state of next generation electro-optical and IR sensors and threat detection capabilities. CCM also supported the testing of the Pilotage Distributed Aperture System 2.0 MWS to assess additional operational capabilities.

Vehicle Protection System

CCM supported the testing of the Layered Soft-Kill System (LSKS) and Controlling Access using Proximity-focused Semantic Analysis (CAPSA) system. Testing of the LSKS, as installed on the Model 2 Bradley Fighting Vehicle, evaluated its ability to defeat anti-tank guided missile threats. The CAPSA test assessed the CAPSA system's interoperability with multiple off- and on-board sensors, their ability to locate and identify threats, and the transference of threat information from the CAPSA system to the integrated Vehicle Protection System.

» T&E OF COUNTER-UNMANNED AIRCRAFT SYSTEMS (C-UAS)

Because of the rapid technological advancements and growth of UAS threats, CCM supported operational performance assessments of a select set of C-UASs as installed, integrated, and employed in an operationally representative environment. In FY23, CCM provided certified UAS operators and analysts for four test events to evaluate and improve C-UAS systems for the protection of U.S. forces, facilities, and assets. The FY23 test events included one Family of Counter Unmanned System (FoCUS) test, two U.S. Special Operations Command (USSOCOM) tests, and one Sentinel A4 test. The FoCUS and USSOCOM tests evaluated the capabilities of C-UAS to detect, classify, identify, track, and defeat Group 1 and 2 UAS threats (systems less than 55 pounds, operate under 3500 feet above ground level, and fly less than 250 knots). The Sentinel A4 test evaluated next-generation, passive UAS detection with man-out-of-the-loop operations.

» T&E OF DIRECTED ENERGY WEAPONS (DEWs)

In FY23, CCM supported the rapid capabilities development and fielding of prototype DEWs and made significant progress in equipping the DoD with the tools and methods needed to adequately test and evaluate the operational effectiveness of DEWs and directed energy (DE)-based CMs. CCM supported 15 DE-based tests in four test series:

DE Maneuver Short Range Air Defense Performance Capabilities

This testing evaluated the ability of the DE Maneuver Short Range Air Defense prototype to detect, track, and engage rocket, artillery, and mortar (RAM) targets. Testing also facilitated new equipment training, enabling soldiers to gain hands-on experience with prototype systems in multiple operationally representative vignettes.

Air Force DE Prototype Materiel Solution Analysis

This testing evaluated DE beam diagnostics and performed system analyses, including beam characterization and system performance, across various prototype systems developed to defeat adversary UASs.

High Energy Laser (HEL) with Integrated Optical Dazzler and Surveillance Integration and Tracking

This testing collected and evaluated beam diagnostics and atmospheric characterizations to determine the system's ability to execute its counterintelligence, surveillance, and reconnaissance mission.

Probability of Weapon Effectiveness Experimentation

The objective of this test series is to determine HEL weapon effectiveness against a series of dynamic targets and compare results to model predictions.

» PRE-DEPLOYMENT TRAINING

In FY23, CCM provided its unique assets — such as a missile plume simulator, an instrumented Man-Portable Air Defense System (MANPADS) surrogate system, and an RF threat simulator — to support four pre-deployment exercises. During the following exercises, CCM provided data to the trainers to assist with their tactics, techniques, and procedures development intended to enhance their survivability potential in a combat environment:

EMERALD WARRIOR 23

This exercise was a joint interoperability large force exercise 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 infrared countermeasure (IRCM) technology.

160th Special Operations Aviation Regiment (Airborne) Field Test Exercises

The objective of these two exercises was to train aircrews on threat identification, notification to headquarters, CMs, and evasive maneuvering.

NEPTUNE FALCON 22

This exercise was a joint interoperability series of exercises designed to maintain readiness and evaluate combat search and rescue employment capabilities in a realistic training environment at night.

» DATA COLLECTION FOR THREAT CHARACTERIZATION

In FY23, CCM provided data collection support during two test events. CCM utilized signature measurement instrumentation for the collection of imaging and radiometric data of threat missiles. These data improved signature models for MANPADS and RAM to enhance digital representation of MANPADS and hardware-in-the-loop models used for evaluating MWS and CM performance. CCM's support and instrumentation were also used to detect, identify, and characterize unknown objects in or near military installations, operating areas, training areas, and special-use airspace to improve threat awareness and mitigate risks to U.S. forces, facilities, and assets.

» DEVELOPING AND FIELDING OF UNIQUE INSTRUMENTATION FOR CM SYSTEMS

In FY23, CCM continued to develop and upgrade the following test instrumentation and capabilities to keep pace with adversary advances and T&E needs to expedite testing, development, and fielding of CMs needed to dominate and survive in increasingly complex, multi-domain environments:

HEL Remote Target Scoring (HRTS) System

HRTS is an integrated optical and sensor suite that will provide radiometric and multi-spectral imaging of targets, starting at the system's acquisition and HEL engagement until target flight path termination. HRTS enables the tracking and scoring of a variety of targets during HEL engagements — including light boats, RAM, UASs, and subsonic and supersonic cruise missiles. CCM, in collaboration with White Sands Missile Range – Army Test and Evaluation Command, accepted delivery of the land-based HRTS in 2QFY23. Delivery of the maritime-based HRTS system did not occur in FY23 due to supply chain delays and cost overruns. The continued development of the maritime HRTS system is anticipated to continue in FY24.

Joint Mobile IRCM Test System (JMITS) and Multi-Spectral Sea and Land Target Simulators (MSALTS)

JMITS and MSALTS consist of five dual-band IR and ultraviolet simulators capable of replicating threat missile plumes. CCM continues to work on upgrades to the simulators to include enhanced bandwidth and processing capabilities — which provide high-fidelity threats to evaluate advanced MWSs and Directed Infrared Countermeasures — and improvements to automated mission-based data collection and reduction. Only one simulator was successfully upgraded in FY23 due to software delays and the unavailability of simulator hardware caused by CCM's busy test schedule. All remaining simulator upgrades are estimated to be completed by 4QFY24.

Joint Standard Instrumentation Suite (JSIS)

This suite of instrumentation is used to collect missile plume and hostile fire threat signatures and time-space-position information data during live-fire events. The JSIS-collected data will further develop the Missile Space and Intelligence Center's threat models to support MWS and CM development and evaluation. In FY23, the JSIS Missile Attitude Subsystem for tracking imagery and time-space-position information continued to be developed and is on track to be delivered by 2QFY24. In FY23, JSIS equipment requirements were solidified, and all remaining instrumentation is scheduled to be delivered by 4QFY24, completing all three phases of the JSIS project providing full operational capability to the T&E community. JSIS personnel continue to update and improve automated mission-based data collection and reduction features and are investigating the feasibility of using enterprise engineering platforms for artificial intelligence and machine learning to enhance data analysis of target tracking capabilities.

High Elevation Target Simulator (HETS)

HETS is a new test capability developed to provide a low-cost, portable IR target simulation to collect missile signature data at elevation angles up to 65 degrees to enhance current Threat Modeling and Analysis Program fly-out models. Existing models were developed from limited static and very low-angle-of-attack live missile firings. This new high-elevation capability will improve current and future IRCM T&E effectiveness.

Towed Airborne Plume Simulator (TAPS)

TAPS is a towable airborne, fixed-wing body missile plume simulator intended to replicate the IR temporal characteristics and approximate the spectral and spatial behavior of threat missiles approaching an aircraft. By simulating a threat's movement in different backgrounds, TAPS can more effectively evaluate aircraft MWSs. Upgrades include a TAPS airframe that can be towed by a rotary-wing platform (TAPS-Helo) and augmentation of the baseline capability with emitter-based IR and ultraviolet source (Towed Optical Plume Simulator). CCM completed Flight Validation Testing on TAPS-Helo in 3QFY23 and expects the system to be operational in FY24. The Towed Optical Plume Simulator emitter performance will be evaluated in 1QFY24 to determine suitability for supporting testing of advanced MWSs.

DoD Space T&E Instrumentation Initiatives

In collaboration with the Test and Evaluation Threat Resource Activity (TETRA), CCM continues to identify gaps in space CM T&E capabilities and actions or investments required to fill those gaps. CCM has been collecting data, conducting the gap analysis, and working with TETRA to report the results by 3QFY24.

DE-based Projects to Fulfill T&E Instrumentation Capability Gaps

DE-based efforts assist in the development and implementation of tools to support HEL and High-Power Microwave (HPM) testing. Specifically, CCM supports projects that include airborne free-flying and tethered UAS with HEL target boards, dynamic UAS detect and track radar systems, HEL beam characterization equipment, and HPM diagnostic instrumentation. In FY23, CCM conducted the developmental and acceptance testing for the following joint DE T&E tools and instrumentation:

- Target boards for directly measuring HEL performance (stationary or mounted on an inflight, operationally representative cruise missile and UAS).
- Beam characterization sensor suite to compare data outputs of the various T&E HEL power and irradiance measurements systems across the U.S. Airforce, CCM, and HEL community.
- HEL beam capture and safe heat dissipation system to provide a backstop for HEL testing.
- Portable and compact multi-mission hemispheric radar system to detect and track air threats (traditional and unmanned) while conducting DEW engagements.
- UAS-mounted HPM instrumentation for measurement and characterization of HPM beam on target.
- 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.

» SUPPORTING PROJECT ARRANGEMENTS WITH ALLIES TO ADVANCE CM T&E

In FY23, CCM and TETRA continued to support the execution of the Australia, Canada, Great Britain, and U.S. Airborne Electronic Warfare (EW) Cooperative T&E Project Arrangement which is advancing and standardizing coalition Air EW T&E capabilities. The following working groups (WGs) support all four nations in advancing and standardizing T&E:

Modeling and Simulation (M&S) and Threat Environment Representation WG

This WG continued validation of the Australia High-Fidelity Chimera Chaff model. The WG completed and incorporated Air EW M&S tools into optimization algorithms and distributed the Double MANPADS M&S tool. The WG also developed new level of confidence qualifications for Air EW CM effectiveness.

Air EW T&E Methodology WG

This WG completed both the standardized T&E terminology and the T&E methodology documentation. It is expected to be distributed in 2QFY24.

Integrated Aircraft Survivability Equipment (IASE) WG

This WG developed Air EW T&E infrastructure, methodologies, processes, and procedures to enable future IASE T&E and establish acceptance of survivability levels for blue air platforms. It also matured blue platform survivability and IASE performance test objectives and plans to manage all Air EW T&E activities.

RF Threats & CM WG

This WG is preparing for a trial, scheduled for 3QFY24, that will incorporate updated Air EW M&S tools into an overarching battlespace environment simulation hub using an Air EW scenario to evaluate CM effectiveness. It is also developing follow-on goals and objectives for a trial scheduled for FY26, which will develop a wider Air EW scenario battlespace.

Cyber Assessment Program (CAP)

As DoD cyber defenses continue to improve, the offensive capabilities of potential adversaries are escalating; many DoD cyber defenses and warfighter missions remain vulnerable to offensive cyber capabilities of potential adversaries. DoD is implementing Zero Trust best practices, which are imperative to defend against advanced cyberattacks, but full implementation will take several years, and may require a level of training, expertise, and automation that is not currently planned. Until effective defenses and fight-through capabilities are developed, implemented, and routinely practiced, critical DoD missions will likely be degraded in conflicts with an advanced adversary.

DoD's cyber posture remains at risk from attacks by unconventional threats, such as those posed by radio frequency (RF)-enabled cyberattacks

where cyber payloads in radio emissions disrupt systems, or direct attacks on weapon systems' data busses and control systems that are essential to aircraft, ships, and vehicles. During FY23, relatively simple RF-enabled cyberattacks caused critical mission disruptions. Future DoD cyber strategies, resource allocation, development, and testing must consider such cyber threats.

Many combatant commands (CCMDs) are increasing the threat realism of their exercises, with U.S. Indo-Pacific Command leading the transition from training exercises to mission rehearsals. These operationally realistic events enabled DOT&E's Cyber Assessment Program (CAP) to emulate more advanced adversaries in selected events, affording warfighters and defenders opportunities to fight through more realistic contested environments. With the increasing demand from CCMDs for greater threat realism, additional cyber Red Team resources are needed to emulate increasingly advanced threats in these expanding mission rehearsals. Because every CAP assessment provides recommendations on how to improve defenses, commands almost always demonstrate improved network and mission assurance in subsequent assessments, decreasing the risk of mission disruption due to advanced cyberattacks.

DoD continues to accelerate the migration of critical missions and classified data to commercial clouds, but limited access to proprietary cloud infrastructure has prevented the DoD from independently assessing the cyber survivability of commercial clouds and the DoD missions that they support. Commercial clouds containing classified DoD mission data are a prime target for advanced cyber adversaries, and such assessments are critical to ensure DoD data is protected. The DoD should perform operationally realistic assessments of the proprietary cloud infrastructure needed to support DoD's portion of the cloud, using cyber Red Teams emulating advanced adversaries. The DoD's Joint Warfighting Commercial Cloud contracts require this, as does recent legislation. Both DoD and the commercial cloud vendors would benefit from such assessments, and DoD Components should work with commercial cloud vendors and DOT&E to ensure they are routinely performed.

Cross domain solutions (CDS) are key to the movement of critical DoD mission data. CAP performed reviews of CDS implementation in FY23 and identified the need for further evaluation of the cyber survivability of DoD CDS capabilities. DOT&E has placed CDS on oversight to ensure rigorous testing and full awareness of the operational state of CDS capabilities.

Significant advances in artificial intelligence (AI) and machine learning (ML) occurred in the commercial sector during FY23. In FY23, CAP – in partnership with the Chief Digital and AI Office (CDAO), federally funded research and development centers (FFRDCs), National Labs, academia, and DoD cyber Red Teams – accelerated its efforts to develop and demonstrate assessment methods and tools unique to AI/ML technologies and will continue these efforts in FY24 in anticipation of deployments of AI-enabled capabilities to the CCMDs.

PROGRAM OVERVIEW

CAP is a congressionally directed program, established in FY03, focused on assessing the cyber survivability of CCMD and Service missions in contested environments. Congress directed DOT&E to plan and conduct these operational evaluations during major exercises.

DOT&E resources cyber Red Teams to emulate realistic adversaries during major CCMD and Service exercises, and to provide assessment venues to help warfighters improve their ability to fight through cyberattacks and accomplish critical missions. DOT&E also provides resources to assessment teams from the Operational Test Agencies and FFRDCs to plan and execute mission-focused assessments and analyze and report on the results at the system, network, and operational levels.

Although exercises are the primary venues for CAP assessments, DOT&E also employs Cyber Readiness Campaigns (CRCs) that include non-exercise events to examine specific elements of warfighter missions

and defenses. These CRC events may include pre-exercise Red Team activities, cyber-stimulation events to help cyber defenders fine-tune their sensors and response actions, tabletop exercises with leadership to explore various contingency plans, and range-based events to examine mission elements and threats that may not be appropriate for operational networks. CRCs provide advanced training opportunities for the CCMDs and Services to rehearse their missions in environments that include realistic adversary emulation. The CRC events that culminate with an exercise capstone event enable CAP to assess cyber warfighting in a realistic mission context.

MISSION

The CAP mission is to characterize and support improvement of the DoD's ability to defend critical warfighting capability and missions against cyberattacks and to project cyber power in support of national defense and security objectives. CAP assessments focus on fielded warfighting capabilities and encompass the ability of operational warfighters to plan and conduct full-spectrum cyberspace operations in support of overall CCMD missions.

FY23 KEY ACTIVITIES

In FY23, CAP fused together focused intelligence expertise, pre-exercise Red Teams (see Persistent Cyber Operations below), and exercise Red Teams into a unified cyber opposing force (OPFOR) that affected a wide range of missions and supporting components at U.S. Indo-Pacific Command (USINDOPACOM), U.S. European Command (USEUCOM), U.S. Special Operations Command (USSOCOM), and other venues. These activities set the conditions for rigorous assessments with representative adversary emulation and improved the realism of mission rehearsal for the participating commands.

During these assessment activities, CAP teams identified cyber vulnerabilities and demonstrated potential impacts that could degrade CCMD missions, all of which were fully communicated to system owners and network defenders so that vulnerabilities could be remediated, and missions made more resilient. The assessment teams also identified improvements in cyber defenses, including well-defended enclaves that have been assessed and enhanced through multiple cycles and have incorporated some Zero Trust principles. Room for improvement remains, particularly at Service-level components, which can be targeted through long-duration persistent Red Teams and other more advanced means.

To help keep pace with evolving cyber adversaries, in FY23 CAP developed new cyberattacks targeting cloud technologies and AI/ML capabilities. CAP developed cyberattacks using the RF spectrum, and techniques integrating cyberspace effects with both kinetic and non-kinetic effects. CAP also developed new capabilities for cyber Red Team data automation and improved collection methodologies for cyber-defense data.

» CCMD AND SERVICE ASSESSMENTS

During FY23, CAP performed cyber assessments at nine CCMDs (U.S. Africa Command [USAFRICOM], U.S. Central Command [USCENTCOM], USEUCOM, U.S. Northern Command [USNORTHCOM], USINDOPACOM, USSOCOM, U.S. Southern Command [USSOUTHCOM], U.S. Strategic Command [USSTRATCOM], and U.S. Transportation Command [USTRANSCOM]), and four Services (Air Force, Army, Navy, and Space Force). As projected in the FY22 Annual Report, DOT&E ramped up assessment activities with the U.S. Space Force and the U.S. Space Command. In FY23, CAP collected data on sensors, manning, and training to inform cyber defense initiatives, and in FY24, CAP will conduct its first assessment of the new Tier 1 APOLLO GRIFFEN exercise.

CAP prepared a classified report for each CCMD and Service assessment that documents the planning, execution, analyses, and recommendations. Cybersecurity perimeter defenses at most assessed CCMDs and Services were effective but defensive capabilities against threats that have penetrated the perimeter were often lacking. This is a concern because a persistent adversary is highly likely to

penetrate any defensive perimeter, given enough time. At several CCMDs, perimeter cyber defenses were improved from prior years, as were abilities to detect and respond to threats rapidly. These improvements resulted in a greater number of events where Red Team activity was stopped before these exercise adversaries could achieve opposing-force objectives. Once inside perimeter defenses, Red Team activities were generally successful, at the expense of warfighter missions and objectives.

In FY23, CAP expanded exercise assessments to include more component commands, Service cyber components, and U.S. allies and partners in recognition that exercises frequently involve components supporting the CCMD. DOT&E observed a range of cyber defense capabilities across the participating components. Some groups of local defenders were better resourced and trained than others, and those defenders tended to be more capable. The CCMDs should ensure that their subordinate components are adequately resourced to counter cyber threats and inform the components of how their cyber vulnerabilities affect CCMD missions.

CAP continued to incorporate cyber opposing-force leads in exercise assessments to help translate cyber effects into mission effects for the exercise control group. Exercise controllers included those mission effects in multiple exercise scenarios, providing dynamic training opportunities for the command staff and exercise participants. This training could be improved by including a wider range of disruptive effects representative of those that potential adversaries could deliver. Exercises with more realistic adversary portrayal would provide warfighters and defenders with improved opportunities to practice their missions in the expected contested environments and help them enhance their fight-through capabilities. In FY23, leadership at several CCMDs emphasized the shift from "training exercises" to more operationally realistic "mission rehearsals," most prominently by USINDOPACOM.

Operationally realistic mission rehearsals simultaneously stress all aspects of CCMD missions and provide the best opportunities for DOT&E to assess CCMD's ability to fight through contested environments and be successful in their missions. The DoD should continue the enhanced realism observed by DOT&E in FY23 during FY24 and beyond.

A significant limitation to enhanced operational realism during CAP assessments is that DoD Red Teams remain under-staffed and under-resourced. Compounding this issue are continuing challenges with retention of Red Team experts who are being stressed by ever-increasing demand, and lack of development pipelines for advanced cyber tools and tradecraft. DoD Red Teams lost many of their journeyman and master-level operators over the last several years, and it will take many years and significantly more resources to remedy these losses. Unless remedied, cyber Red Team shortfalls will lead to inadequate preparation during mission rehearsals, inadequate program acquisition activities, and ultimately critical warfighter capabilities that are not survivable.

DOT&E observed in FY23 that cyber-related information sharing could be improved across the DoD at all levels. Successful cyber defense requires completing prevent, detect, respond, and recover actions, and organizations should ensure they can reliably conduct incident reporting and cyber-threat intelligence sharing. The interconnected nature of networks and systems, trust relationships across commands, and the ability for data to be rapidly disseminated means that an individual CCMD's data security depends on all participating DoD parties. Combatant commanders and DoD leadership should fully understand the mission risks associated with data sharing initiatives across the Department, including the Combined Joint All-Domain Command and Control (CJADC2) initiative.

» SPECIAL ASSESSMENTS

CAP performed the following special assessments in FY23 in collaboration with U.S. Cyber Command (USCYBERCOM), USSTRATCOM, the DoD Chief Information Officer (CIO), CDAO, Joint Forces Headquarters DoD Information Network (JFHQ-DODIN), the Defense Information Systems Agency (DISA), and the Department of Energy's Sandia National Laboratories:

- Zero Trust architectures in Software-as-a-Service environments
- Transponder-Combat Identification
- Commercial cloud assessments
- Cross-Domain Solution (CDS) assessments
- Nuclear Command, Control, and Communications (NC3)
- Offensive Cyberspace Operations (OCO)
- Preparations for assessments of artificial intelligence (AI) and machine learning (ML) technologies
- Industrial Control Systems
- Radio frequency (RF)-enabled cyber operations
- 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 CRCs, as well as cybersecurity OT&E of acquisition programs. A number of these special assessments are discussed below.

Zero Trust Environment Assessments

The DoD CIO describes Zero Trust as "protecting critical data and resources, not just the traditional network or perimeter security" (DoD Zero Trust Reference Architecture). In keeping with recommendations made by DOT&E over the past several years to move from boundary-focused to data-focused protections, the DoD CIO has many ongoing efforts to move to a Zero Trust architecture, and CAP has observed positive outcomes because of the adoption of various combinations of the tenets and pillars of Zero Trust, as defined by the DoD CIO.

CAP has not yet observed a complete implementation of Zero Trust that includes continuous multi-factor authentication, micro segmentation, encryption, endpoint security, automation, analytics, and robust auditing. The CIO Zero Trust Portfolio Management Office resourced four commercial providers to develop and deploy Zero Trust environments, and in FY23 CAP completed two assessments of a cloud service provider's Zero Trust environment. Other cloud service provider environments will be examined in FY24.

Cross-Domain Solution (CDS) Assessments

CDS are integrated hardware/software systems that enable access and exchange of sensitive data across networks at different levels of security classification. CDS capabilities are essential for the movement of data across myriad DoD systems that are critical to warfighting capabilities. CAP reviewed CDS implementation in FY23 and identified the need for further evaluation of the cyber survivability of DoD CDS capabilities. As a result, DOT&E has placed CDS on oversight to ensure rigorous testing and full awareness of the operational state of CDS capabilities.

Nuclear Command, Control, and Communications (NC3)

CAP and USSTRATCOM continued a partnership for assessing and improving the cyber survivability of NC3. The complex nature of the hybrid legacy and modernized system-of-systems that comprises NC3 poses challenges to assessments of this mission space, however, progress is being made across the NC3 enterprise as a result of the continued partnership. Barriers to cyber assessments of the NC3 enterprise include a lack of operational capacity to support operations and testing simultaneously, as well as ongoing modernization efforts.

CAP is sponsoring the development of a high-fidelity virtualization environment for a subset of NC3 legacy systems. This environment will assist with assessments and Red Team activities that would otherwise be challenging on the operational networks. Once validated, the environment will also help assess and experiment with improved cybersecurity defenses and allocation of sensors deployed across the transitioning NC3 systems-of-systems.

Offensive Cyberspace Operations (OCO)

DOT&E continued assessments of OCO, defined as missions intended to project power in and through cyberspace. DOT&E conducted OCO capability assessments on capabilities developed and fielded

by the Air Force and by USCYBERCOM. DOT&E also conducted assessments on the integration and synchronization of OCO in major exercises at USINDOPACOM, U.S. Forces Korea (USFK), USEUCOM, and key events with Joint Special Operations Command. In addition to continued assessments supporting USINDOPACOM, USFK, USEUCOM, and Joint Special Operations Command in FY24, DOT&E plans to assess capabilities and events supporting USSOUTHCOM, U.S. Space Command (USSPACECOM), and USSTRATCOM's Joint Electromagnetic Spectrum Operations Center.

In FY24, DOT&E will also expand its ties with the Defense Advanced Research Projects Agency (DARPA) and with OUSD(R&E) to support early operational assessments of unique, "fast-tracked" capabilities. In some cases, this will require broader team accesses to specialized programs, and DOT&E will continue to work with the OUSD(A&S) Special Access Program Central Office (SAPCO) to ensure early operational assessments are conducted to improve development and timely delivery of important capabilities to the warfighter.

The DoD continues to develop most OCO capabilities without formal operational testing. Although CAP provides operationally realistic assessments for a small subset of OCO capabilities, there are many more OCO capabilities being developed in multiple DoD Components with no such assessments. OCO capabilities continue to grow in importance to DoD missions, and insufficient testing in operational environments with representative threats may result in OCO capabilities failing to work as needed, or in a lower confidence regarding the scope and duration of OCO capability effects.

Artificial Intelligence (AI) and Machine Learning (ML) Assessments

In FY23, CAP expanded efforts to prepare for assessments of AI-enabled technologies, working with the CDAO, FFRDCs, National Labs, academia, and DoD Red Teams on the development and demonstration of assessment methods and tools unique to AI/ML technologies. CAP will continue these efforts in FY24 in anticipation of deployments of AI-enabled capabilities to the CCMDs and ensure good alignment with related DOT&E initiatives addressed under Pillar 4 of the DOT&E Strategy Implementation Plan, especially "Evaluate the operational and ethical performance of AI-based systems."

CAP performed the first phase of a series of tabletop exercises for a technology recommended by the CDAO, which will help develop best practices for future assessments of AI/ML capabilities. In parallel, CAP is identifying the Red Team tools and tradecraft needed to perform counter-AI/ML assessments, and specific requirements for range environments. CAP coordinated with the Joint Information Operations Range to create a persistent range environment where AI/ML assessments can be hosted and is working with CDAO to receive models under development for pilot assessments and training of DoD Red Teams in aggressing AI/ML systems.

Radio Frequency (RF)-Enabled Cyber Operations

DOT&E recognizes the importance of Joint Electromagnetic Spectrum Operations and its close relationship to offensive and defensive cyber capabilities. The National Defense Strategy notes that electromagnetic spectrum (EMS) and other non-kinetic threat developments are challenging U.S. response capabilities, and rapid and low-cost technology is eroding U.S. technology leads. In close partnership with the Air Force Cyber Resiliency Office for Weapon Systems (CROWS), CAP is expanding its assessments to include RF-enabled cyberattacks to facilitate an enhanced OPFOR that is not solely focused on traditional cyber and Internet Protocol (IP) networks but includes spectrum and apertures to the spectrum. CAP has taken action on the assertion made in last year's Annual Report by integrating effects based on potential RF-enabled cyberattacks (cyber payloads contained in radio emissions). These effects include system degradation due to direct attacks on weapon systems' data buses and other control systems essential to many DoD aircraft, ships, and vehicles.

In FY23, DOT&E consolidated two years of data showing potential mission effects for Transponder – Combat Identification systems and developed tools and methods to safely replicate and insert

these effects into aircraft flying during operational exercises. DOT&E is working with operators and solution providers to assess remedial actions and updates to tactics, techniques, and procedures to mitigate risks posed by these threats. Additionally, these results will be included in planning for future CCMD and Service exercise assessments.

Cyber Wargames to Expand Mission Assurance Assessments

CAP has designed a set of cyber wargames with an emphasis on the operational level of warfare. These wargames will help extend assessments beyond the limitations of exercises on operational networks and help demonstrate potential mission impact of advanced cyberattacks to warfighters and leaders. To highlight the importance of cyber defenders and expose non-experts to key aspects of cyber warfare, CAP Wargame (CMOCK-W). CMOCK-W will help leaders become more familiar with degraded environments not generally permitted during training exercises and assist in refinement of contingency and response-action planning. CMOCK-W will be implemented in FY24 as part of the CRC for several CCMDs. Rigorous and recurring CMOCK-W engagement will improve warfighter preparations to fight through contested cyber environments and improve mission assurance.

» SUPPORTING ACTIVITIES

Persistent Cyber Operations (PCO)

PCO provide cyber Red Teams with longer dwell time on DoD networks to probe selected areas and portray more advanced adversaries. As opposed to one- to two-week exercises or tests, long-duration activities offer Red Teams time for stealthier cyber reconnaissance to identify cybersecurity weaknesses and access points that might otherwise go undetected. These activities help identify subtler and more pervasive vulnerabilities and provide more realistic training for cyber defenders. The longer dwell time enables PCO Red Teams to escalate privileges and move laterally within target networks to cause effects at the time of their choosing, as an advanced persistent threat would. Accesses gained by PCO are handed off to exercise Red Teams acting as cyber OPFOR during specified exercises.

During FY23, DOT&E expanded PCO to include three DoD-certified Red Teams and improved the process for PCO planning and execution. The new process focuses on campaign-style assessments of selected missions and includes more rigorous planning and reporting. The PCO team was able to support seven CCMDs during FY23, and when the process is fully implemented, all CCMDs will be eligible to receive PCO support for their primary missions on an annual basis.

Also in FY23, the PCO team supported the combined exercises of PACIFIC SENTRY 2023 at USINDOPACOM and TURBO CHALLENGE 2023 at USTRANSCOM. This PCO mission lasted approximately six months and involved three separate Red Teams operating in multiple theaters and on numerous headquarters and component enclaves. Red Teams were assigned to operate in designated enclaves to meet objectives provided by those CCMDs. Specific targets were based on real-world cyber intelligence.

DOT&E and the Missile Defense Agency (MDA) are working to provide a briefing to the congressional committees on plans for a PCO to cover MDA systems and networks, in accordance with congressional direction.

Advanced Cyber Operations (ACO) Team

CAP continued to cultivate relationships across multiple organizations that can provide master-level cyber operators and serve as members of the CAP's ACO team. CAP utilizes the ACO team to conduct assessments of emerging technologies, provide cutting-edge expertise as part of continuous augmentation to DoD Red Teams, and facilitate the portrayal of more advanced cyber threats. Organizations participating in the ACO team include DoD-certified Red Teams, FFRDCs, National Labs, University-Affiliated Research Center Laboratories, academia, and industry. During FY23, the DOT&E ACO team supported:

- Assessments of several Zero Trust architectures offered by vendors as Software-as-a-Service environments

- Cyber survivability testing of the F-35
- Assessments of data-lake repositories currently in use throughout the DoD to store, process, and secure large amounts of data (both structured and unstructured), to include the Advancing Analytics (Advana) platform
- Assessments of cyber-physical systems such as industrial control systems and aircraft transponders
- Assessments of specialized networks used by special operations forces
- Assessments of Offensive Cyber Operations (OCO) capabilities
- Development of cyber survivability testing procedures for CDS currently in use throughout the DoD
- Development of enhanced Red Team capabilities, tools, and tradecraft
- Expansion of Red Team accesses via PCO
- Preparation for assessments of AI/ML technologies
- Assessments of NC3 networks

Demand for ACO support grew in FY23 and is expected to continue to grow in FY24. Hiring and retention challenges are a primary concern for the Red Team community, which thus far has been unable to keep pace with the opportunities and salaries offered in the private sector for cyber professionals.

Advanced Cyber-Threat Emulation Capabilities

DOT&E sponsors the Capabilities Development Working Group (CDWG), providing the cyber Red Team community with a collaborative forum to acquire more advanced tools and tradecraft for teams supporting CAP assessments and OT&E. DOT&E also continues to pursue additional resources for tool development and acquisition that include IP, RF, and other special cyber capabilities that will be needed for assessments of new and emerging technologies such as AI-enabled capabilities.

During FY23, the DOT&E CDWG supported:

- Development of a capability that can be used to change Red-Team tool signatures, enabling them to better represent advanced adversaries and evade detection by virus scans
- Standardizing and automating Red Team action maps, data collection, and data visualization
- Development of a command and control framework for Red Teams

In order to address the increasing demand for Red Team participation, DOT&E began a new project in FY23 to identify and acquire tools for Red Teams that automate their current tasks and activities. These enhancements will include tools and tradecraft that expand beyond current Red Team capabilities and may include AI-enablers for Red Teams to plan and execute assessments. In FY24, DOT&E will also explore tools and methods that enable Red Teams and assessment teams to assess and explain the cybersecurity vulnerabilities of AI/ML capabilities in DoD applications and systems.

Engagement with the Intelligence Community

CAP's collaboration with the Intelligence Community remains an essential element of CCMD mission-focused assessments and OT&E events. High security classifications assigned to intelligence information on advanced adversary capabilities and intent limit the ability of assessment teams to fully emulate the full-spectrum adversary against which warfighters should routinely practice the execution of their missions. The lack of opportunity to experience the most representative and known threats may leave warfighters unprepared to defend and sustain their critical missions. DOT&E is working with the Defense Intelligence Agency, the National Security Agency, DoD Red Teams, the National Ground Intelligence Center, the National Air and Space Intel Center, and the Missile and Space Intelligence Center to improve the information sharing and the resulting realism of the threats portrayed in assessments and OT&E.

Table 1. CAP FY23 Activity

Type of Event
Physical Security Assessment (6 Events) USEUCOM, USINDOPACOM, USFK, USNORTHCOM, USTRANSCOM (2)
Assessment of Mission Effects during Exercises (15 Events) USN (2), USAFRICOM, USEUCOM, USFK, USCENTCOM, USINDOPACOM, USNORTHCOM (2), USSOCOM (3), USSOUTHCOM, USSTRATCOM, USTRANSCOM
Assessments of Network Security, Stimulation Exercises, and Tabletop Exercises (8 Events) USAF, USEUCOM (2), USINDOPACOM, USSOCOM, USSOUTHCOM, USSF, USTRANSCOM
Range Event USINDOPACOM
Assessment of Cyber Fires Processes for Offensive Cyber Operations (3 Events) USINDOPACOM, USEUCOM, USFK
Assessment of Special Capabilities and Projects (17 Events) Capability (5), Non-Kinetic Fires (6), SME Support (3), TCID (3)
Acronyms: SME – Subject Matter Expert; TCID – Transponders, Combat Identification; USAF – U.S. Air Force; USAFRICOM – U.S. Africa Command; USCENTCOM – U.S. Central Command; USEUCOM – U.S. European Command; USFK – U.S. Forces Korea; USINDOPACOM – U.S. Indo-Pacific Command; USN – U.S. Navy; USNORTHCOM – U.S. Northern Command; USSF – U.S. Space Force; USSOCOM – U.S. Special Operations Command; USSOUTHCOM – U.S. Southern Command; USSTRATCOM – U.S. Strategic Command; USTRANSCOM – U.S. Transportation Command

International Test and Evaluation Program (ITEP)

The Director signed 12 new project documents in FY23. These documents facilitated 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 (RUTF). There are currently 24 ongoing tests described in project documents with our partners. There are four bilateral international test and evaluation documents in negotiation or technical discussions.

PROGRAM OVERVIEW

The United States holds 12 bilateral agreements with international partners. During FY23, 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. ITEP was established pursuant to a legislative proposal submitted by DOT&E and enacted into law in 2001. The Secretary of Defense delegated administration of the program to DOT&E in 2003. Prior to ITEP, test services were generally provided to international partners through Foreign Military Sales.

MISSION

The ITEP permits establishment of bilateral and multilateral agreements between the U.S. and international partners. Such agreements are enablers for expediting the development and fielding of advanced warfighting technologies and supporting T&E infrastructure and capabilities.

FY23 KEY ACTIVITIES

Table 1 below lists the current greements in effect prior to FY23.

Table 1. IT&E Ongoing Project Agreements in Effect

No.	IT&E Projects [a]	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 (C-CBRN), CBRNE Defense TTPs RUTF Project Arrangement	United Kingdom	Dugway Proving Ground, Utah	January 13, 2031
6	Electronic Warfare Operational Test 2016 RUTF PA	Canada	Naval Research Lab Hawaiian Operating Areas, Marine Corps Air Station, Kaneohe Bay, Hawaii	May 19, 2024
7	CF-18 Software Upgrade T&E RUTF PA	Canada	Naval Air Warfare Center Weapons Division, China Lake, California	June 14, 2024
8	T&E of the German Bundeswehr CBRNE Defense TTPs RUTF PA	Germany	Dugway Proving Ground, Utah	June 15, 2026
9	Aircraft Electronic Warfare CTE PA	Australia, Canada, United Kingdom	Various partner test locations	August 5, 2026

Table 1. IT&E Ongoing Project Agreements in Effect, continued

No.	IT&E Projects [a]	Partner(s)	Test Activity Locations	Expiration
10	T&E of Protective Ensembles Using the Porton Man Test Fixture CTE PA	United Kingdom	Porton Down, United Kingdom	May 11, 2025
11	SIMULATION DISPLAY (SIMDIS™) Sustainment for Sensors, Weapons, Analysis and Tactical Display Developments RUTF PA	Canada	Naval Research Laboratory, Washington, D.C.	October 29, 2025
12	Project RAIDER Data Evaluation RUTF PA	Canada	Naval Research Laboratory, Washington, D.C.	March 10, 2025
13	Tactical Armored Personnel Vehicle Testing RUTF PA	Canada	Aberdeen Test Center, Aberdeen Proving Ground, Maryland	December 31, 2023*
14	Land Platforms Autonomy and Robotics WG Terms of Reference (TOR)	Italy	Not Applicable	January 21, 2030
15	Joint-Improvised-Threat Defeat Organization Electronic Counter Measures RUTF PA	Australia	China Lake, California	December 5, 2023*
16	Partnership for Autonomous Robotic Test Instrumentation WG TOR	Germany	Not Applicable	April 11, 2028
17	Combat Archer II Omnibus RUTF PAs	Canada	Tyndall Air Force Base, Florida	December 21, 2025
21	Combat Hammer Omnibus RUTF PA	Canada	Various U.S. Air Force Bases	November 23, 2026
19	TOR for Live Fire WG	United Kingdom	Not Applicable	December 20, 2025
20	Amendment Seven to the Integrated Air and Missile Defense (IAMD) Testing Reciprocal Use of Test Facilities (RUTF) Project Arrangement (PA)	United Kingdom	Hebrides Test Range, Scotland, United Kingdom	May 12, 2027
21	Test and Evaluation of the Australian Special Operations Engineer Regiment (SOER) Chemical, Biological, Radiological, and Nuclear (CBRN) Defense and Explosive Ordnance Disposal (EOD) Tactics, Techniques, and Procedures (TTPs) RUTF PA	Australia	Dugway Proving Ground, Utah	September 20, 2031
22	HMCS Windsor Testing RUTF PA	Canada	Andros Island, Commonwealth of the Bahamas	April 28, 2025

Notes:

* Test completed.

[a] The IT&E Projects column represents the legal names of each Project Arrangement.

Acronyms:
C-CBRN – Counter Chemical, Biological, Radiological, and Nuclear; CBRNE – Chemical, Biological, Radiological, Nuclear, and Explosive; CTE – Cooperative Test & Evaluation; TTPs – Tactics, Techniques, and Procedures.

1. Advanced Distributed Modular Acquisition System (ADMAS) Instrumentation Equipment and Material Transfer Arrangement

This agreement between the U.S. and Germany enables the Army's T&E Command to transfer the ADMAS instrumentation and software tools to the Bundeswehr Head of Robotics 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.

2. Sky Sabre System RUTF Project Arrangement

This testing was completed in 2021 but the Project Arrangement is still active under the U.S. Army Test and Evaluation Command. The objectives were the testing, evaluation, and analysis of an accepted and integrated Ground Based Air Defence system prior to initial operational capability, including threat detection, threat prioritization, weapon allocation, and threat engagement, as well as post-launch analysis of system data.

3. Flight Test Working Group (WG) Terms of Reference (TOR)

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 WG 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 evaluated the effectiveness and accuracy of novel diagnostics from a series of explosive charges in a test environment. Testing completed in 2023.

5. T&E of the United Kingdom 28 Engineer Regiment (C-CBRN), 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 Test and Evaluation Command's Dugway Proving Ground in Utah hosts 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 effects on mission effectiveness.

6. 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 COVID-19. It is expected to be conducted in Hawaii, where the U.S. will simulate anti-ship missile attacks to validate the Canadian Softkill System.

7. 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 Air Warfare Center Weapons Division, China Lake, California. This test 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. Initial tests were conducted July – August 2021. Additional tests are under consideration.

8. T&E of the German Bundeswehr CBRNE Defense TTPs RUTF Project Arrangement

This agreement enables the German Bundeswehr to develop and test its defense TTPs against CBRNE threats. The U.S. Army Test and Evaluation Command's Dugway Proving Ground in Utah hosts the tests, providing threat representative scenarios to support the evaluation of the operational effectiveness of new detectors, to include mass spectrometers, multi-gas measuring devices, radiation detection devices, PPE, and decontamination equipment in an operationally

representative environment. Tests also include the firing of weapons by soldiers in protective clothing to evaluate impacts on mission effectiveness. Additionally, tests assess post attack reconnaissance after an IED attack. Initial testing was conducted October – November 2019. Figure 1 shows a group of German soldiers in PPE assaulting a target. .

9. 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 of Countermeasures section of this annual report.

Figure 1. Germans Assaulting the Target as part of a test against CBRNE threats

10. 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 continuing to develop test methods and conduct performance testing of chemical protective ensembles (suits) against actual chemical warfare agents. Porton Man is an articulated, life-size, moving mannequin with a combination of cumulative and real-time sensors that can quantify the permeation and penetration of various threat agents through Chemical Biological PPE. The Porton Man CTE Project Arrangement supports U.S. DoD requirements to protect personnel from CBRN threats.

11. 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.

12. Project RAIDER Data Evaluation RUTF Project Arrangement

This agreement supports testing and validating Canadian ships' ability to generate Maritime Domain Awareness data for the Project Radar and Automatic Identification System Information Dominance Enhanced Reporting – Marine (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.

13. Tactical Armored Personnel Vehicle Testing RUTF Project Arrangement

This agreement permitted the U.S. Army Test and Evaluation Command to provide T&E support to a Canadian Department of National Defence acquisition program. The testing and validation of a tactical armored personnel vehicle consisted 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 a Step Steering test, suspension vibration, and tire characterization.

14. Land Platforms Autonomy and Robotics Working Group TOR

This WG, 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.

15. Joint Improvised-Threat Defeat Organization Electronic Counter Measures RUTF Project Arrangement

This agreement covered testing of the Australian Department of Defence's electronic countermeasures (ECM) systems. The U.S. DoD, through the Naval Air Warfare Center Weapons Division (NAWCWD) China Lake Facility in California, 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/electromagnetic compatibility issues as well as system reaction and processing limitations in the electromagnetic environment.

16. Partnership for Autonomous Robotic Test Instrumentation Working Group TOR

This WG, led by the U.S. Army Test and Evaluation Command, was established to harmonize T&E instrumentation and autonomous/robotic requirements, study feasibility of future cooperative TEP activities, and exchange data reports on specific T&E issues of mutual interest with Germany.

17. 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 which includes personnel, munitions, and machines.

18. 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.

19. TOR for Live Fire Working Group

This WG, led by DOT&E, was established to identify potential collaborative efforts in the LFT&E area, to include ground combat vehicles and PPE with the United Kingdom.

20. Amendment Seven to the Integrated Air and Missile Defense (IAMD) Testing 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, exercise Formidable Shield 2023 (FS23). In May 2023, the Maritime Theater Missile Defense Forum (MTMD-F) participated in the Naval Striking and Support Forces NATO exercise FS23. The purpose of FS23 was to improve Allied interoperability in a live-fire joint IAMD environment, using NATO command and control reporting structures. Twelve NATO Allied and partner nations, 24 ships, more than 35 aircraft, 8 ground units consisting of radars, National Advanced Surface-to-Air Missile System, and High Mobility Artillery Rocket System, and nearly 4,000 personnel from across the Alliance participated in the event. Building on the achievements of previous forum events, FS23 increased coalition interoperability and joint capabilities through complex scenarios designed to meet tomorrow's Air Defense and Ballistic Missile Defense challenges.

21. Test and Evaluation of the Australian Special Operations Engineer Regiment (SOER) Chemical,

Biological, Radiological, and Nuclear (CBRN) Defense and Explosive Ordnance Disposal (EOD) Tactics, Techniques, and Procedures (TTPs) RUTF Project Arrangement

This agreement allows 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. See further detail below in Table 2, Item 11.

22. HMCS 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 HMCS Windsor.

In addition to current and ongoing agreements, the following agreements listed in Table 2 were signed with partners in FY23.

Table 2. IT&E Documents Signed into Effect in FY23

No.	IT&E Projects [a]	Entry into Effect Date	Partner	Test Activity Locations
1	Crash Truck Foam Test (CTFT) Project Equipment Transfer (PET)	October 6, 2022	Canada	Tyndall Air Force Base, Florida
2	Annex C to the RUTF PA Concerning the German CBRNE TTPs	November 15, 2022	Germany	Dugway Proving Ground, Utah
3	The Canadian Forces Electronic Warfare Support Test and Evaluation (CFEWS) RUTF PA	February 28, 2023	Canada	Shirley's Bay, Ottawa, Canada
4	Amendment One to the RUTF PA Concerning Project RAIDER Data Evaluation	March 6, 2023	Canada	Navy Research Laboratory, Washington, D.C.
5	Counter-Laser Directed Energy Weapons (CLDEW) RUTF	April 11, 2023	United Kingdom	Army Research Laboratory, Adelphi, Maryland
6	Amendment One to the AU SOER CBRN TTP RUTF PA and Annex C	May 16, 2023	Australia	Dugway Proving Ground, Utah
7	Annex B to the Laboratory and Field T&E of the Australian DSTG CB Defensive Material RUTF PA	May 26, 2023	Australia	Dugway Proving Ground, Utah
8	Technology Experimentation and Characterization Field Trials (TECFT) RUTF PA	May 30, 2023	Canada	Dugway Proving Ground, Utah
9	Annex D to the RUTF PA Concerning the German CBRNE TTPs	August 18, 2023	Germany	Dugway Proving Ground, Utah
10	Tactics Validation and Operational Readiness Assessment RUTF PA	August 24, 2023	Canada, Australia, United Kingdom	Naval Warfare Center, China Lake, California
11	Annex D to the AU SOER CBRN TTP	September 13, 2023	Australia	Dugway Proving Ground, Utah
12	Cybersecurity Assessment Working Group Terms of Reference	December 14, 2022	Australia, Canada, New Zealand, United Kingdom	Not Applicable

Notes:

[a] The IT&E Projects column represents the legal names of each Project Arrangement.

Acronyms:
AU – Australia; SOER – Special Operations Engineer Regiment; DSTG – Defence Science and Technology Group.

1. Crash Truck Foam Test (CTFT) Project Equipment Transfer (PET)

The purpose of the CTFT PET is to test cleanout procedures to transition aircraft rescue firefighting vehicles from aqueous film-forming foam to fluorine-free firefighting foam.

2. Annex C to the RUTF PA Concerning the German CBRNE TTPs

Refer to Table 1, entry 8 and its accompanying narrative for information on this agreement.

3. The Canadian Forces Electronic Warfare Support Test and Evaluation (CFEWS) RUTF PA

The electronic warfare software and the Scenario Simulation Controller are part of a U.S. DoD-owned electronic warfare and reprogramming software suite managed by the U.S. Navy's Next Electronic Warfare Generation Program Office. Canadian Forces Electronic Warfare Centre at Shirley's Bay has a unique configuration that can benefit from the testing of its electronic warfare capabilities by the scenarios contained in the EW toolset. The testing of CFEWS capabilities utilizes the U.S. DoD's electronic warfare toolset and components of its electronic warfare programming toolset (Scenario Simulation Controller) and Monitoring and Analysis.

4. Amendment One to the Project RAIDER Data Evaluation RUTF Project Arrangement

Refer to Table 1, entry 12 and its accompanying narrative for information on this agreement.

5. Counter-Laser Directed Energy Weapons (CLDEW) RUTF Project Arrangement

The purpose of this RUTF is to test the laser damage and vulnerability of the UK cameras, imaging systems, and optical materials to femtosecond, picosecond, and continuous-wave lasers.

Figure 2. German Soldier Performing Chemical Testing in Tunnel under the T&E of the German Bundeswehr CBRNE Defense TTP RUTF PA

6. Amendment One to the AU SOER CBRN TTP RUTF Project Arrangement and Annex C

Refer to Table 1, entry 21 and its accompanying narrative for information on this agreement. The purpose of Amendment One to the CBRN/EOD TTPs RUTF PA is to expand the scope of the Australian Defence Forces participants beyond the Special Operations Engineer Regiment. Annex C allowed the testing of chemical and biological production and dissemination signature recognition and evaluated existing data collection and analysis techniques.

7. Annex B to the Laboratory and Field T&E of the Australian DSTG CB Defensive Material RUTF Project Arrangement

The purpose of this Annex is to utilize chemical and biological simulant releases provided during the Technology Experimentation and Characterization Field Trials (TECFT) to characterize the performance of multiple technologies. Field trials will be conducted in accordance with the U.S. Army Test and Evaluation Command's standard operations procedures.

8. Technology Experimentation and Characterization Field Trials (TECFT) RUTF Project Arrangement

The purpose of the TECFT RUTF PA is to provide an assessment of Chemical-Biological-Radiological Situational Awareness based on co-deployment of point/standoff CB sensors in an environment representative of realistic CB threats.

9. Annex D to the RUTF PA Concerning the German CBRNE TTP

Refer to Table 1, entry 8 and its accompanying narrative for information on this agreement. Figure 2 shows a German soldier performing chemical testing in a tunnel.

10. Tactics Validation and Operational Readiness Assessment RUTF Project Arrangement

This Project Arrangement will let the testers evaluate the effectiveness of the defensive tactics of Royal Canadian Air Force aircraft and to assess the capability of Canadian Tactical Aviation personnel to conduct realistic mission sets in an EW threat environment.

11. Annex D to the AU SOER CBRN TTPs

This Annex supports the latest series of tests to enhance and improve the tactics, techniques, and procedures and identify any operational gaps of the Australian Defence Forces. Figure 3 shows an Australian unit at a CBRN test site.

Figure 3. Australian Unit at CBRN Test Site at Dugway Proving Ground, Utah

12. Cybersecurity Assessment Working Group Terms of Reference

The TOR established the WG and provides authority for technical discussions and exchange of information during WG discussions. The Cybersecurity WG will be focused on identifying and developing collaborative efforts to increase the cybersecurity of coalition missions and joint weapons systems.

Table 3 below lists potential future test agreements.

Table 3. Future Test Agreements

No.	IT&E Projects	Objective
1	U.S.-Japan Test and Evaluation Program (TEP) Memorandum of Understanding (MOU)	Sign a TEP MOU
2	Amendment Two to the U.S.-Netherlands TEP MOU	Sign an updated TEP MOU
3	U.S.-India TEP Memorandum of Agreement (MOA)	Develop a TEP MOA
4	U.S.-Republic of Korea TEP MOU	Develop a TEP MOU

1. U.S.-Japan TEP MOU

The U.S. will sign a TEP MOU with Japan. Significant test opportunities have been identified.

2. Amendment Two to the U.S.-Netherlands TEP MOU

The U.S. will sign the Amendment Two to the Netherlands TEP MOU to extend the current TEP MOU by 10 years.

3. U.S.-India TEP MOA

The U.S. opened technical discussions with India pursuant to developing a TEP MOA. Test opportunities have been identified.

4. U.S.-Republic of Korea TEP MOU

Upon completion of an umbrella agreement with the Republic of Korea, the U.S. will negotiate a TEP agreement.

Joint Aircraft Survivability Program (JASP)

In FY23, the Joint Aircraft Survivability Program (JASP) continued to advance tools, processes, infrastructure, and workforce to transform the OT&E and LFT&E of aircraft survivability. For example, JASP delivered new digital tool capabilities enabling: 1) enhanced evaluations of the effects of red threat engagements against blue rotary wing aircraft in the low altitude battlespace and 2) improved capability to predict engagement induced aircraft fires, with increased confidence.

In FY23, JASP also continued the development of new techniques and technologies demonstrating the potential to enhance the survivability of U.S. aircraft in contested, multi-domain operations. For example, JASP delivered: 1) new electronic attack (EA) techniques to counter advanced radar threats, 2) new application of a fielded 2-Color infrared (IR) missile warning system to detect a new class of missile threats, 3) enhanced man-portable air-defense systems hardware-in-the-loop simulation capabilities by utilizing actual missile seeker tracking and guidance hardware, 4) a high output, low divergence laser prototype capable of providing improved IR countermeasures aircraft defense, and 5) a new light-weight self-sealing aircraft fuel bladder design.

PROGRAM OVERVIEW

The Joint Technical Coordinating Group on Aircraft Survivability (JTCG/AS) was chartered in 1971, in response to high aircraft loss rates experienced during the Vietnam War. The JTCG/AS initially focused on aircraft susceptibility reduction (design characteristics that make an aircraft harder to detect) and aircraft vulnerability reduction (design characteristics that give an aircraft the ability to withstand a hit). The JTCG/AS focus later grew to include modeling and simulation and establishing aircraft survivability as a design discipline through the development of a formal curriculum at the Naval Postgraduate School.

In 1985, the oversight responsibility of the JTCG/AS was assigned to the newly established Joint Aeronautical Commanders Group (JACG). Funding for the JTCG/AS was consolidated under what is now the DOT&E.

In January 2003, the JACG signed a new charter establishing JASP to replace the JTCG/AS while expanding the JTCG/AS charter to include the Joint Combat Assessment Team (JCAT).

In 2005, the service aviation systems commands (U.S. Army Aviation and Missile Command, U.S. Air Force Life Cycle Management Center, and Naval Air Systems Command) chartered JASP as it is known today.

MISSION

JASP develops cross-Service aircraft survivability solutions and evaluation methods needed to dominate the air domain and mitigate U.S. aircraft losses in combat. Specifically, JASP:

- Advances the capability and credibility of joint aircraft combat effectiveness tools used in combat mission planning, training, and weapon schools to support the development of air combat tactics, techniques, and procedures.
- Develops and manages enterprise-level digital tools required to support comprehensive evaluation of aircraft effectiveness and survivability, with confidence.
- Collects and analyzes U.S. aircraft combat damage and losses via the Joint Combat Assessment Team, to develop the requirements for joint aircraft survivability solutions that provide force protection and remedy operational shortfalls.
- Leverages advances in science and technology to develop innovative aircraft survivability enhancement features.

FY23 KEY ACTIVITIES

» ADVANCING THE CAPABILITY AND CREDIBILITY OF JOINT AIRCRAFT COMBAT EFFECTIVENESS TOOLS

JASP, in coordination with the Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME), continued the co-development of the Air Combat Effects Library (ACEL) – the joint suite of Intelligence Community threat models and Service-based simulations for use in multi-domain combat simulations. ACEL underpins the Survivability and Lethality of Aircraft in a Tactical Environment (SLATE) v1.x and Joint Anti-Air Model (JAAM) v6.x applications shown in Figure 1. ACEL enables a collection of hostile and U.S. systems simulations across air, sea, and surface domains with multiple weapon classes enabling evaluation of the combat survivability and lethality kill chains. SLATE supports one-on-one, few-on-few engagements, or batch runs with large collections of engagement permutations. SLATE supports acquisition system evaluations and long-lead ACEL development of credible simulations. Once ACEL capabilities are demonstrated within SLATE, they are migrated for use in JAAM supporting operational warfighters' tactics, techniques, and procedures development, debriefing and training across the DoD.

Air Combat Effects Library (ACEL)

In FY23, JASP advanced ACEL for the low-altitude and high-altitude battlespace, by maturing the helicopter aero performance simulation (BlueMax), and

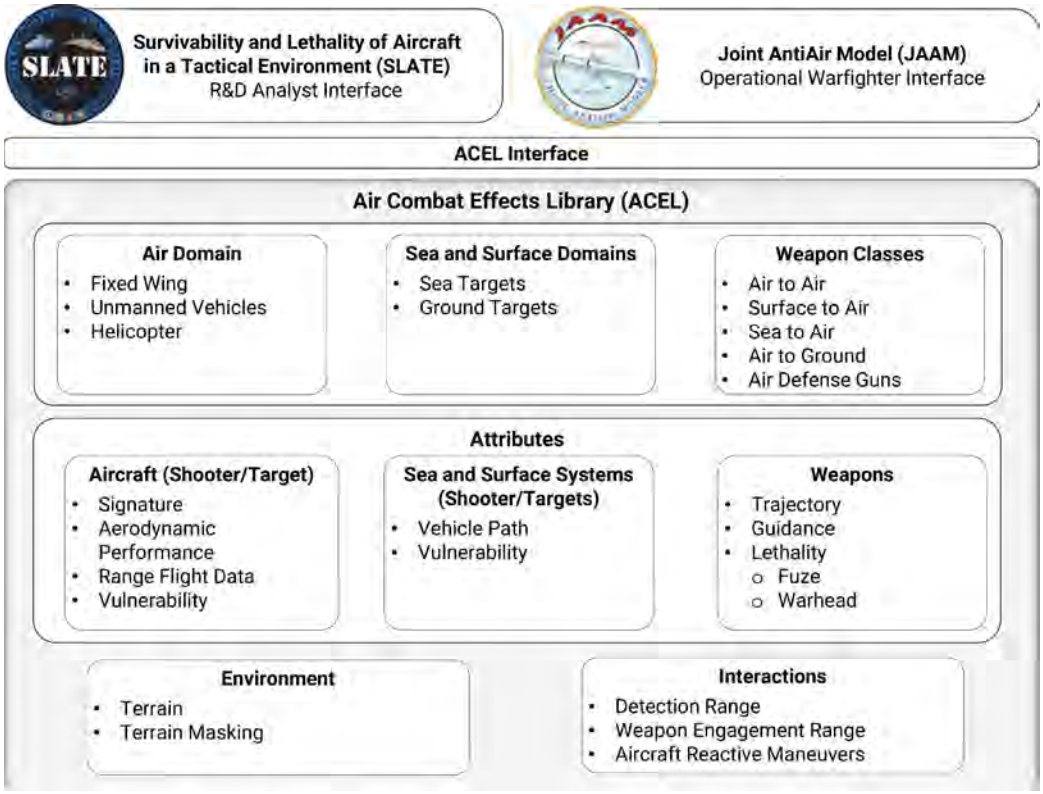


Figure 1. Air Combat Effects Library Architecture

weapon simulations for surface, sea, and air-artillery weapons. JASP continued a multi-year investment in helicopter aero performance methodology (BlueMax) for single main rotor, tandem rotor, and tilt-rotor vehicles. BlueMax's fourth helicopter aero data set was provided for use in ACEL. Figure 2 illustrates the helicopter aerodynamic simulation capabilities in ACEL that include takeoff, flight, hover, and landing.

In FY23, JASP and JTCG/ME also: 1) streamlined the process and reduced the migration of Intelligence Center surface to air missile (SAM) simulations into ACEL from four months to two weeks and 2) advanced ACEL's weapon lethality and helicopter target vulnerability simulation and data for missiles and air-artillery projectile attack.

Survivability and Lethality of Aircraft in a Tactical Environment (SLATE)

In FY23, JASP evolved the SLATE application's graphical displays along with development of ACEL's new capabilities. SLATE was used to demonstrate simulation capability in areas of high-fidelity terrain, terrain masking, radio frequency (RF) signal propagation, enhanced chaff displays, bursts of air-artillery projectiles flyouts, naval SAM flyouts, and helicopter dynamic blade flash signature. Figure 3 illustrates a simulation of a helicopter reactive maneuver with chaff against incoming hostile missile.

In FY23, JASP conducted the first phase of the Joint Aircraft Threat Modeling Simulation Validation effort to validate Integrated Air Defense System digital tools

Figure 2. Helicopter Aerodynamics Simulation

Figure 3. SLATE Low-Altitude Helicopter/SAM Engagement

and their engagement with the U.S. Army UH/HH-60M aircraft equipped with radar countermeasures. JASP successfully validated the SLATE graphical interface, Enhanced Surface-to-Air Missile Simulation (ESAMS), and BlueMax7 using flight these test data.

Joint Anti-Air Model (JAAM)

JAAM's broad usage provides common operational insight regardless of squadron or test range's debriefing tool. In FY23, the JTCG/ME's JAAM application was used daily by warfighters at operational squadrons, test and training ranges, mission rehearsals, and debriefing to evolve tactics. The user base included 360 sites and 4,000 personnel:

- Operational Squadrons and Intelligence Community
- Test/Training ranges, mission playback and debriefing applications
- Joint Mission Planning System

In FY23, JTCG/ME in coordination with JASP, developed a beta version of the next generation JAAM application. The JAAM user interface was designed to provide warfighter intuitive workflow and advanced graphical displays. The new design uses a modern graphical engine to enable agile development and integration with ACEL's shooters and targets across air, sea, and land domains. ACEL's new helicopter capabilities will further expand the JAAM user base in the out-years.

» DEVELOPING AND MANAGING ENTERPRISE-LEVEL DIGITAL TOOLS

In FY23, through tri-Service configuration control boards, JASP continued the management of major digital tools used to estimate air combat effectiveness and survivability against an array of operationally representative kinetic threats. The toolsets include the air-to-air combat simulation Brawler, the surface-to-air engagement model ESAMS, multiple domain air combat simulation SLATE, and the vulnerability analysis code Computation of Vulnerable Area Tool (COVART), along with its supporting penetration and fire prediction codes Projectile Penetration, Fast Air Target Encounter Penetration, and the Next Generation Fire Model (NGFM). 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/ BCAT	Brawler	ESAMS	SLATE	COVART	NGFM
Bomber Aircraft	-	1	1		1	1
Fighter Aircraft	ID, IC, II	5	5		4	1
Rotary-Wing Aircraft	IB, IC		3	3	2	2
Transport/Tanker Aircraft	IC		1		2	1
Special Use Aircraft	ID, III		1		2	2
Weapons	IC	1				
Totals		***7***	***11***	***3***	***11***	***7***

Acronyms: ACAT – Acquisition Category; BCAT – Business System Category; COVART – Computation of Vulnerable Area Tool; ESAMS – Enhanced Surface-to-Air Missile Simulation; NGFM – Next Generation Fire Model; SLATE – Survivability and Lethality of Aircraft in Tactical Environments

In FY23, JASP also:

- Continued the Machine Assisted Exploitability Simulation for Testing Resilient Operations effort to add cyber survivability evaluation capability to the COLE tool. Advancements included the

- representation of threat actor capabilities, aircraft operational technologies, system and mission state models and vulnerability assessments. This effort, in collaboration with the Air Force, Army, and Navy aviation cyber survivability communities, provides digital tool capability and data standardization to develop and evaluate aircraft survivability in contested cyberspace.
- Advanced efforts to inform survivable design decisions by coordinating requirements for a survivability digital ecosystem to provide joint community access to authoritative aircraft survivability data and enhance the efficiency and speed of acquisition, T&E, and design decisions.
- Released the initial version of the Next Generation Fire Model tool for use by the community to inform acquisition decision-making regarding aircraft vulnerability to fires – one of the largest aircraft vulnerability contributors.

Collect and Analyze U.S. Aircraft Combat Damage and Losses using the Joint Combat Assessment Team

In FY23, JASP continued to enable aircraft combat damage incident reporting through the JCAT. The JCAT is heavily engaged with Indo-Pacific Command and European Command supporting operational commanders with combat data collections while also leveraging operational exercises. They developed new concept of operations utilizing Title 50 (i.e., intelligence) tools to enable the near real time forensics of aircraft combat damage.

JASP also transitioned the Combat Damage Incident Reporting System from the National Ground Intelligence Center to the U.S. Army Corps of Engineers Engineer Research and Development Center to enable combat incident reporting and data sharing across the DoD, Services, and combatant commands. Combat Damage Incident Reporting System is available via SIPRNet.

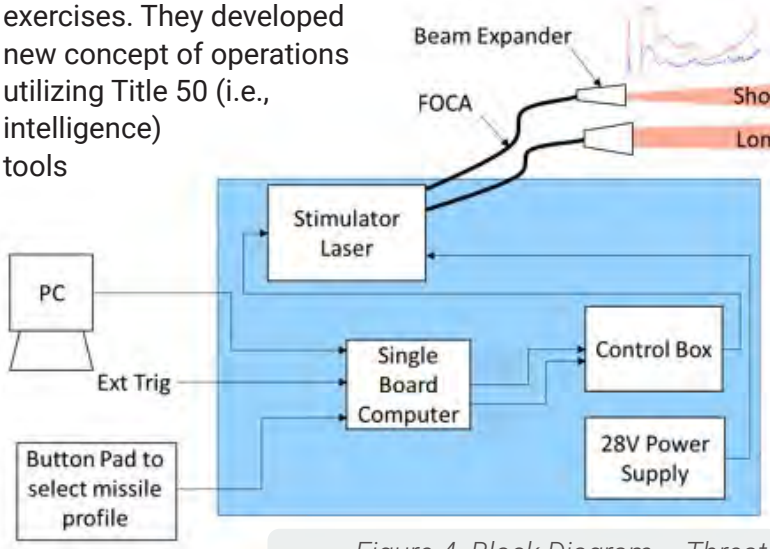


Figure 4. Block Diagram – Threat Launch Simulator 2CIR MWS

» DELIVERING INNOVATIVE SURVIVABILITY ENHANCEMENT FEATURES

Threat Detection and Countermeasures Technologies

In FY23, in collaboration with the OSD and Service organizations, JASP matured threat detection and countermeasure technologies needed to defeat advanced electro-optical (EO)/IR- and RF-guided threat systems. For example, the RF Threat Launch Detection and Track project was designed to develop algorithms to allow currently deployed DoD IR warning systems to detect and track RF missile threats and is transitioning into an Air Force Special Operations Command acquisition program. In partnership with the Naval Research Laboratory, JASP continued the development and demonstration of aircraft self-protection RF EA technologies and EO/IR technologies. JASP leveraged the validated threat simulator at the Naval Air Systems Command Electronic Combat Simulation and Evaluation Laboratory, to demonstrate the effectiveness of advanced techniques against a class of stressing RF threats. Specifically, the modern anti-countermeasures effort has demonstrated new EA techniques, including coordinated EA and determining effectiveness to countering such systems. Where validated threat simulators were not available, JASP, in coordination with the intelligence community, developed an electronic warfare environment for a specific type of threat to further develop and test EA

techniques to counter such specific type of threats. This provided the Services with a unique capability for development of countermeasure techniques.

In addition, JASP supported the development of a successful prototype system that can produce transmitted missile signatures detectible by aircraft in the field – the threat launch simulator 2-Color IR Missile Warning System (2CIR MWS). The Naval Research Laboratory demonstrated the capability to produce the simulated missile signatures suitable for 2CIR MWS performance testing. Figure 4 depicts a block diagram of the Threat Launch Simulator 2CIR MWS.

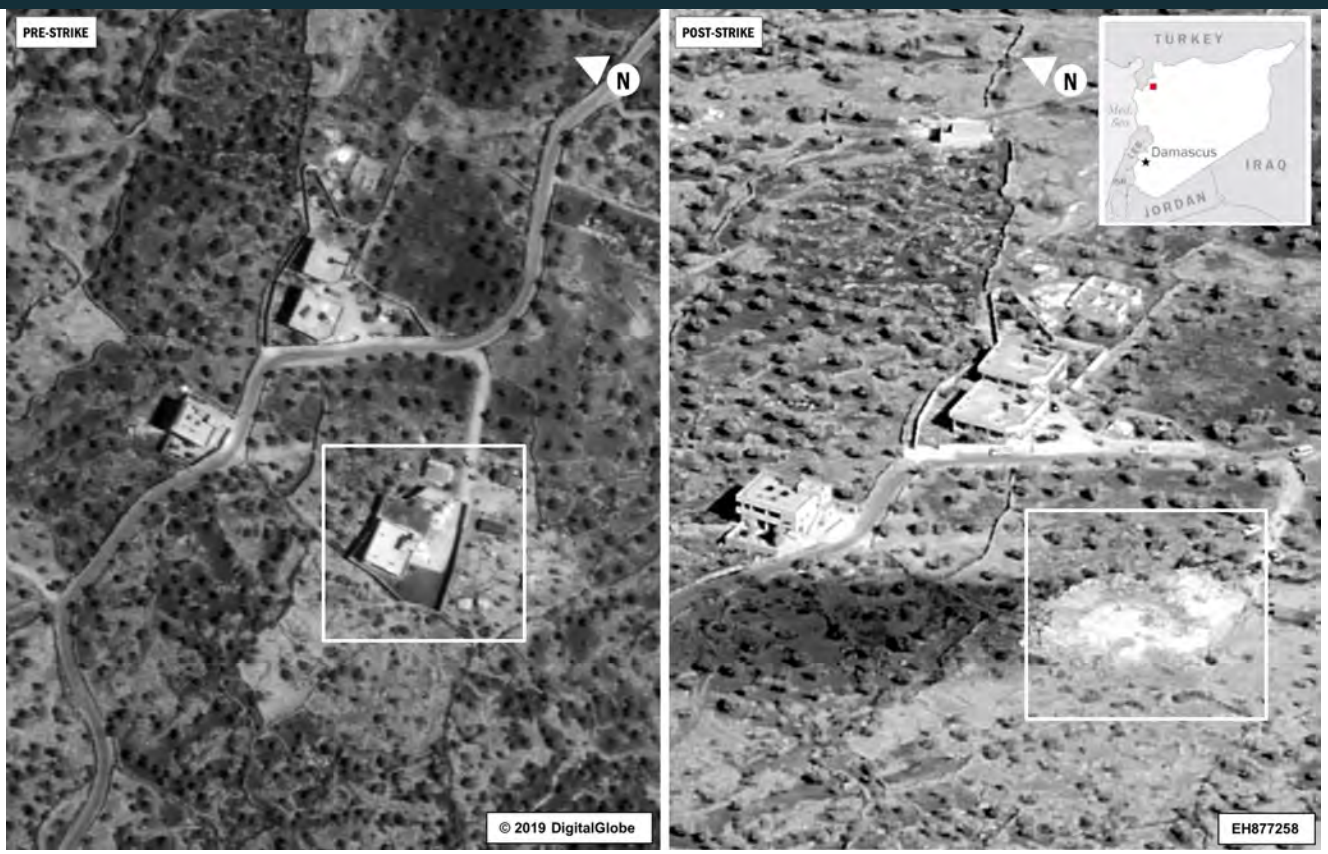
JASP continued the development of a Reconfigurable Signal Injection Missile Simulation Hardware-in-the-Loop (HITL) Simulation of Advanced Threats. This HITL simulator for multiple reticle-based IR missiles utilizes actual missile seeker tracking and guidance hardware and will support testing against advanced threats that were previously unavailable.

In FY23, JASP funded development of a 20-watt Mid-Wave Infrared laser which could provide improved infrared countermeasures aircraft defense. JASP supported the fabrication of all laser subcomponents to include a completed laser driver that accepts external waveforms.

Force Protection Technologies

In FY23, JASP successfully tested a design optimization methodology for self-sealing fuel cell bladders that demonstrated an up to 35 percent decrease in weight while meeting the predetermined crashworthiness requirements. Other JASP testing further quantified the decrease in ballistic ignition of aircraft coolant fluid treated with a mist control additive which could reduce aircraft vulnerability with minimal weight impact.

Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) Program



In FY23, the Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) program utilized modern software development methods to demonstrate the ability to increase the capability, user interface, experience, and integration of weaponeering tools more effectively and efficiently. JTCG/ME uses target vulnerability data, standards, methodologies, and processes to advance the weaponeering capabilities and accuracy of lethality effects and collateral damage estimates (CDE) against kinetic, maritime, cyber, electromagnetic spectrum (EMS), and directed energy targets. In FY23, the JTCG/ME program used automated data collection to collect over 90,000 strike products to analyze strikes, inform reach-back support, and support weaponeering tool verification and validation, training, and expenditure analysis. In FY23, JTCG/ME generated 13 reach-back packages for weaponeering, CDE, and munition effectiveness assessment in support of current operations. In coordination with the Joint Live Fire (JLF) program, JTCG/ME also continued to collect data to underpin the methodology required to advance full-spectrum survivability and lethality methods and tools applicable to operations planners and OT&E and LFT&E of DoD systems and services.

PROGRAM OVERVIEW

The JTCG/ME program was chartered in 1968 to serve as the DoD's focal point for munitions effectiveness information. It started by delivering Joint Munitions Effectiveness Manuals (JMEMs) – the sole source for all non-nuclear weapons effectiveness data and methodology for the DoD. The JMEMs have been the "how to" manuals for determining the type and number of ordnance on target. Today, JMEMs have transitioned to kinetic and non-kinetic tools used in operational weaponeering, and CDE in direct support of multi-domain operations, mission planning, and training. These tools are used by joint and Service planners in force-on-force effect estimations, mission area analysis, requirements studies, and weapon procurement planning. These tools are also used by the Service acquisition community in performance assessments, analyses of alternatives, and survivability enhancement studies, and include:

- The Digital Imagery Exploitation Engine (DIEE), a tool that enables users to plan and execute kinetic strikes by seamlessly performing the following Advanced Target Development steps: (1) geographically locate and characterize the target; (2) weaponeer the target using JMEM Weaponeering System (JWS); (3) perform target coordinate mensuration; (4) determine CDE using the Digital Precision Strike Suite Collateral Damage Estimation (DCiDE) tool; and (5) produce and output graphics to the appropriate databases.
- Weaponeering tools capable of estimating lethal effects for directed energy weapons (DEW), cyber, maritime targets, and 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 (TTP). The J-ACE tool's main module is the Joint Anti-Air Model (JAAM), which is discussed in the Joint Aircraft Survivability Program (JASP) section of this Annual Report.

The JTCG/ME program also manages the JLF program. The JLF program is focused on the development of adequate full-spectrum survivability and lethality tools, methods, and infrastructure required for both; advancement and accreditation of weaponeering tools; and support of OT&E and LFT&E of DoD systems and services.

MISSION

The JTCG/ME program develops, advances, and sustains weaponeering tools. These tools, frequently referred to as JMEM products, are used by the combatant commands (CCMDs) to estimate and optimize the type and number of U.S. offensive kinetic and non-kinetic capabilities required to achieve the desired lethal effect. These products support assessment against a range of kinetic and non-kinetic strategic or tactical targets, while mitigating risk for collateral damage including civilian casualties. JTCG/ME leverages the JLF program to develop and enhance full-spectrum survivability and lethality digital tools; improve survivability and lethality T&E methods and processes; and enable live data collection to support rigorous verification, validation, and accreditation (VV&A) of survivability and lethality digital tools.

FY23 KEY ACTIVITIES

» DELIVERING CREDIBLE WEAPONEERING TOOLS TO CCMD STRIKE AUTHORITIES

JMEMs are used daily by warfighters worldwide in direct support of operations, mission planning, and training. The user base includes approximately 26,000 personnel, spanning the following entities:

- DoD Service members
- Joint Staff/CCMDs
- Multiple coalition partners
- Acquisition community, T&E enterprise, Intelligence Community, and National Laboratories

In FY23, JTCG/ME fielded updates to DIEE to improve product accuracy and efficiency in support of operational warfighters. Specifically:

- In collaboration with Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) and the Joint Staff Directorate for Intelligence (J-2), JTCG/ME has been improving the efficiency and effectiveness of the Joint Targeting Intelligence process by developing, standardizing, and integrating the Advanced Target Development workflow and tools. As part of this process, operational users will be able to link desired effects to tactical tasks outlined in operational plans, which will increase the probability of meeting the commander's objective via enhanced integration and connectivity across the targeting enterprise to enable targeting at scale.
- JTCG/ME has been applying modern software development methods including development, security, and operations (DevSecOps) to enable continuous and incremental improvement in capability, user interface, and experience of JWS tools. JTCG/ME also added new weapon and weapon trajectory data to its scene-based weaponeering products, allowing the strike authorities to account for enhanced technologies and capabilities in their calculations of target defeat. To maintain consistency with the latest National Geospatial-Intelligence Agency mensuration methods, JTCG/ME updated calculation tools for both Mensuration Services Program and Common Geopositioning Services.
- JTCG/ME completed updates to collateral effects radii tables, reducing their error margins. It advanced the friendly force collateral effects library mitigation tool to increase the efficiency of collateral effects analysis and enhance risk estimate distance calculations used by DCiDE. Using the JLF program, JTCG/ME continued the collaboration with the University of Virginia on the development of Traumatic Brain Injury (TBI) risk functions. Based on Joint Trauma Analysis and Prevention of Injury in Combat Program (JTAPIC) combat data, available military blast models/methodologies testing from the Enhanced Weaponeering Integrated Product Team, JLF developed a conservative approach to update TBI blast risk estimates for inclusion in Risk Estimate Distances (REDs).
- JTCG/ME generated 13 reach-back packages for weaponeering, CDE, and munition effectiveness assessment in support of current operations.
- JTCG/ME facilitated 28 training classes/events for over 300 students at 22 locations. Training of integrated product capabilities (DIEE/JWS) continues to enable the operational community to successfully employ munitions while minimizing collateral damage.

» ADVANCING THE CAPABILITY, EFFICIENCY, AND ACCURACY OF TARGET DEVELOPMENT TOOLS

JTCG/ME continued to advance the capabilities efficiency and accuracy of target development tools to respond to CCMD needs in an increasingly complex and dynamic multi-domain operational environment. JTCG/ME upgraded existing weaponeering capabilities to increase the effectiveness of kinetic strikes and developed new capabilities to enable deliberate and dynamic engagements using cyber, EMS, and DEW capabilities.

Advanced Target Development

The DIEE is a vital software program for the targeting enterprise at the global level. The DIEE provides digital solutions to the essential Joint Targeting Cycle functions for both the U.S. and coalition partners.

The DIEE software turns current workflow inefficiencies into automated and integrated solutions within one ecosystem. DIEE's essential targeting functions apply across the targeting spectrum and address Basic, Intermediate, and Advanced Target Development. Key functions include Target Coordinate Mensuration, weaponeering methodologies using JWS, CDE effects using the DCiDE tool, targeting graphics production, and combat assessment.

FY23 accomplishments include the release of DIEE v2.3.2 to address critical issues with hardware dependencies. In addition, developing DIEE v3.0 with native 3D viewing capabilities without hardware dependencies (as shown in Figure 1), integration of JWS and Capability

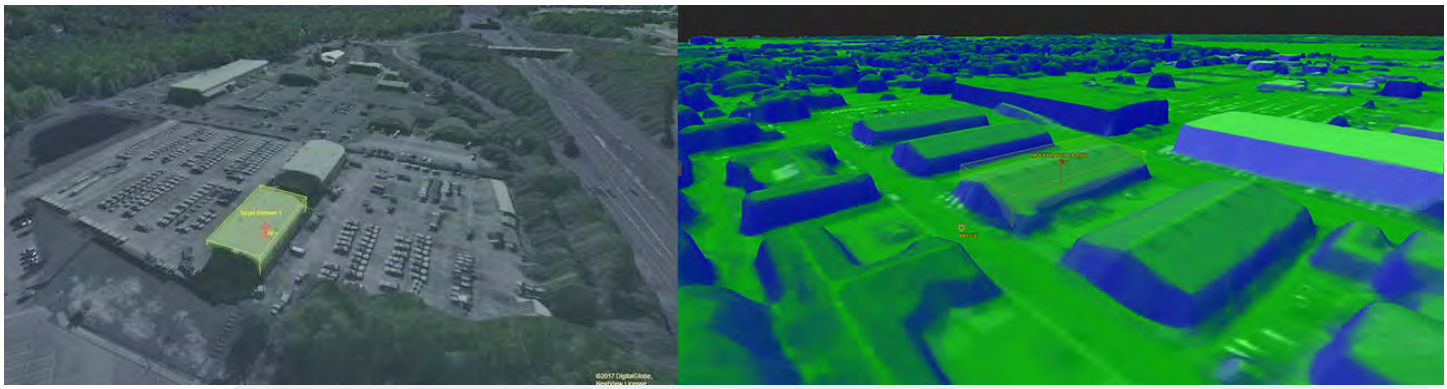


Figure 1. Examples of native 3D viewing capability no longer requiring additional hardware

Solutions Package beta versions, and critical integration with third-party libraries and tools.

As part of the OUSD(I&S) and J-2 Joint Target Intelligence Modernization (JTIM) initiative, JTCG/ME initiated the development of a federated workflow management (WFM) tool streamlining the targeting enterprise production, tracking process while reducing costs. The WFM is a standalone web application and will be fully integrated through DIEE. DIEE and all other JTIM associated programs as well as leadership throughout the Joint Targeting Community will all have a dashboard and associated notifications using this tool.

Weaponeering

The JWS combines a series of weapon system characteristics, delivery accuracy, and target vulnerability data needed to estimate the final aimpoint, delivery conditions, and number of weapons on target necessary to achieve combatant commanders desired lethal effects. In FY23, JWS v2.4.1 continued sustainment efforts with the next planned release in early 2024 to support urgent operational needs. Capabilities of future versions of JWS include auxiliary tools and equipment fragility modeling to include structural target components and surface mobile targets. The next generation JWS product line continued the development of weaponeering capabilities including structural targets, interior and exterior personnel, and materiel targets, and integration with DIEE.

CDE

In FY23, JTCG/ME made significant progress toward improving the ability of the DoD and coalition partners to accurately characterize the CDE associated with lethal effects of U.S. weapons. Specifically, JTCG/ME leveraged the multi-year Enhanced Weaponeering and CDE test program to quantify the collateral effects resulting from munitions detonating either in the ground or beneath structures. Data sets from the Enhanced Weaponeering and CDE test program were used to improve, verify, and validate high fidelity digital tools used to predict building debris mass and velocity distributions from multiple structure types, along with crater ejecta, ground shock, and blast pressure for various soil types and munition burial configurations. The uncertainty in these predictions must be minimized, as they are the foundation for fast-running engineering models used by the DCiDE tool and JWS to estimate weapon collateral damage and lethality. In FY23, JTCG/ME conducted several tests, depicted in Figures 2 through 4, to further the understanding of munition burial and building debris effects on personnel and nearby structures. These live data supported the evaluation of the combined effects of a kinetic impact and subsequent below-ground detonation, along with the mitigation of blast and fragmentation effects and the hazards from secondary debris enhancing the validation of the weaponeering and CDE tools.

Battle Damage Assessment (BDA)

JTCG/ME continued the multi-year effort to verify, validate, and advance the effectiveness of JMEM

Figure 2. Kinetic impact test conducted in partnership with the U.S. Army Engineer Research and Development Center's Mobile Ballistic Research System at Fort Polk, Louisiana

Figure 3. Follow-on test with buried ordnance at Aberdeen Proving Ground, Maryland

Figure 4. Two-story over-burial building debris test at Aberdeen Proving Ground, Maryland

weaponeering tools by capturing otherwise perishable combat assessment data for future analysis. The goal of the BDA program is to enable credible post-strike analysis to ensure commander's intent has been achieved while capturing strike details (as directed by the Civilian Harm Mitigation Response – Action Plan) for future reference and use by the targeting enterprise. To meet this intent, JTCG/ME continued to collect BDA data, not only to analyze strikes and inform reach-back support, but also to support weaponeering tool verification and validation, training, and expenditure analysis.

In FY23, JTCG/ME used automated data collection to collect over 90,000 strike products in the U.S. Central Command, the U.S. Africa Command, and the U.S. European Command areas of responsibility. An Optical Character Recognition tool was developed to quickly and efficiently assist in the process of identifying and databasing strike products. These strike products are stored in the Joint Battle Damage Analysis Repository (JBAR), via an Army cloud environment (c-Army), with an interactive web mapping dashboard for use by the joint community.

An application programming interface is in development that will allow DIEE to directly connect to, and expedite storage of, newly produced strike products. This direct connection will facilitate accurate strike product archival for future use through the JBAR web mapping interface.

Lethal Effect Estimates

JTCG/ME continues to leverage the Advanced Warhead Characterization (AWC) project to improve the fidelity of weapons' lethal effect data. In FY23, the program initiated the Validated Munitions

Effectiveness Model (VMEM) series, which includes high-fidelity modeling and simulation (M&S), advanced test diagnostics, data analysis, and munition model validation. Advanced test diagnostics tools (e.g., computed tomography, digital image correlation, X-ray, photon Doppler velocimetry, pressure measurements, and optical fragment tracking, as shown in Figure 5) support efficient data collection and high-fidelity model validation for munitions.

The AWC project is continuing to build, refine, and document the techniques, processes, and procedures, which will be provided to the JTCG/ME Systems Characteristics Working Group for use in approved warhead characterization procedures. VV&A of the munition model is the goal of the VMEM process.

In FY23, JTCG/ME also leveraged the small-scale blast test program initiated by the JLF program to provide a tailorable scale target model that will be used to efficiently collect larger volume and higher fidelity lethality data as compared to current models and processes. The JLF program also continued to execute the Multiphase Blast Explosive (MBX) program with the purpose of increasing the ability of weaponeering tools to estimate MBX lethal effects used in low-collateral damage munitions.

Lethal Effect Estimates - Hypersonic Weapons

In FY23, JTCG/ME continued addressing the shortfalls related to the evaluation of lethality and associated weaponeering tool capabilities for hypersonic weapons. JTCG/ME initiated the live data collection program to support the advancement and accreditation of high-fidelity digital tools intended to estimate hypersonic weapons lethal effects. Near-term efforts will account for weapon characterization, including terminal effects and delivery accuracy. 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. The JLF program continues to make progress in luminescent technology development and testing, which will enable optical characterization

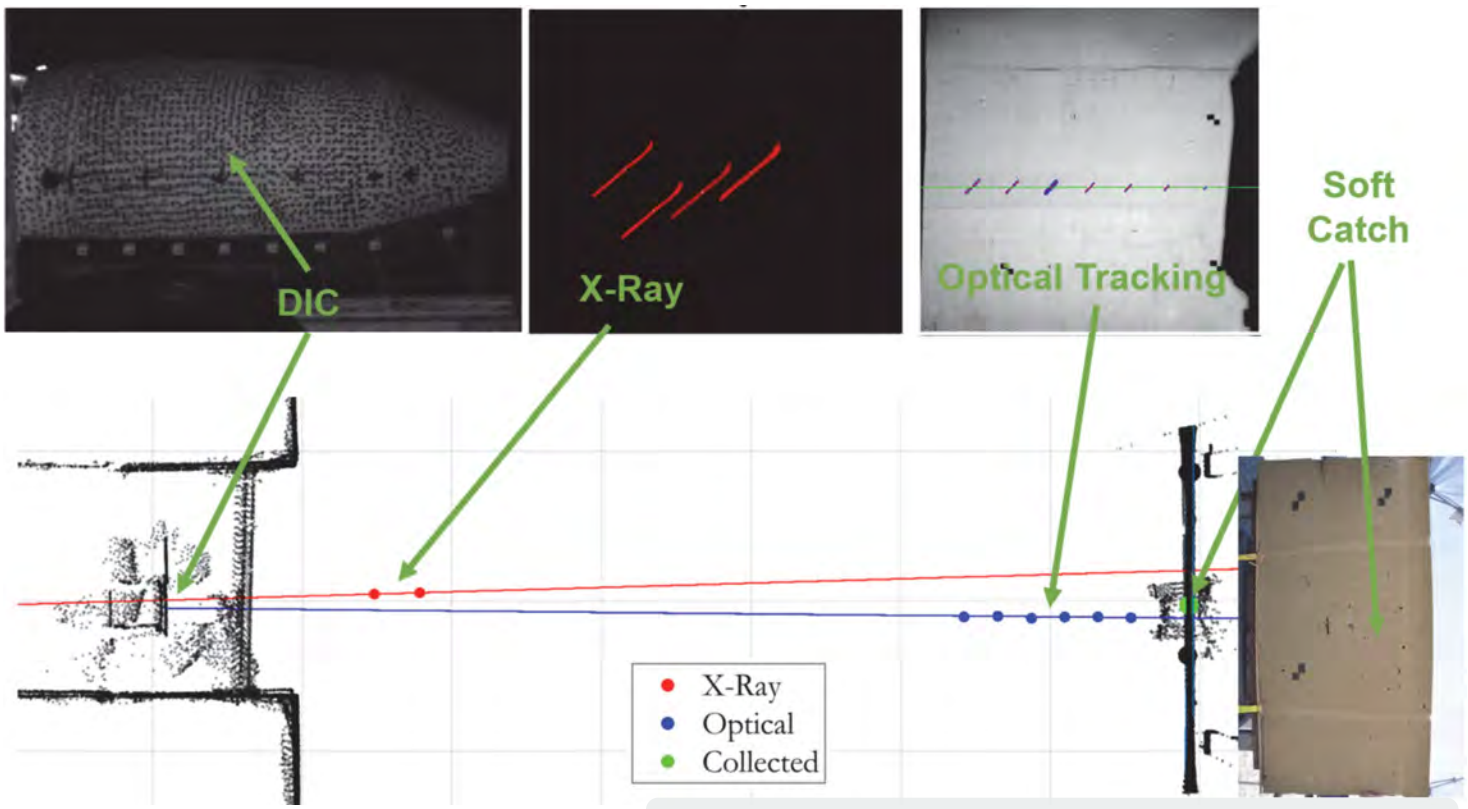


Figure 5. The use of a compilation of multiple advanced test diagnostics as part of the munition model validation process

of fragment dispersion in flight tests to adequately evaluate emerging hypersonic weapons.

Lethal Effect Estimates - Maritime Targets

In FY23, JTCG/ME continued the effort to enhance the ability of weaponeering tools to support the warfighter with credible and timely lethal effects estimates against adversary maritime (surface and subsurface) targets. Within this effort, JTCG/ME has developed weaponeering guides for several maritime targets not currently in JTCG/ME inventory. JTCG/ME also developed and delivered version 1.0 of the Target Damage Cards software, shown in Figure 6, for integration and fielding in DIEE, enabling new maritime weaponeering analysis tool for surface and ultimately subsurface targets.

JTCG/ME continues to execute a collaborative test program that procures data to close knowledge gaps, improve current analytical tools and methods, and develop advanced digital tools (e.g., the Next Generation Enterprise Maritime Lethality Tool) required to support the delivery and fielding of weaponeering tools against such targets. Other digital tools that will be advanced as part of this initiative include the Submarine Vulnerable Effects Model, Navy Enhanced Sierra Mechanics, and Dynamic System Mechanics Advanced Simulation. This effort increases weapons systems' lethality against foreign maritime threat platforms and will also support more effective and efficient survivability evaluation of U.S. ships and submarines in support of LFT&E objectives. Figure 7 shows the progression of the fidelity of models needed.

M&S VV&A

JTCG/ME continued the critical VV&A and uncertainty quantification (UQ) efforts in coordination with the U.S. Army, U.S. Air Force, U.S. Navy, and Lawrence Livermore National Laboratory representatives to develop standards of VV&A/UQ practices across the JTCG/ME product lines. VV&A experts

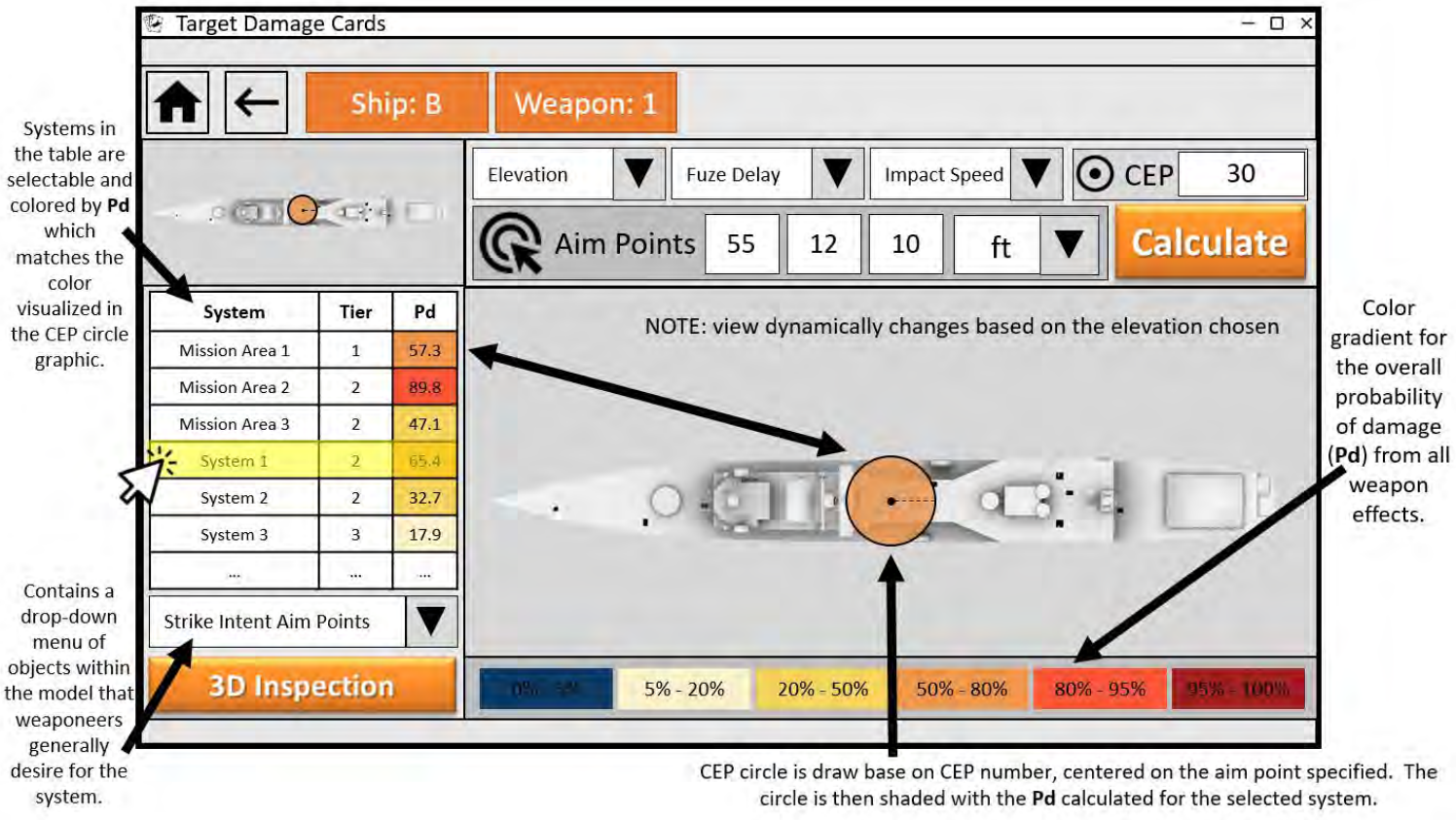


Figure 6. Maritime Target Damage Card visualization tool

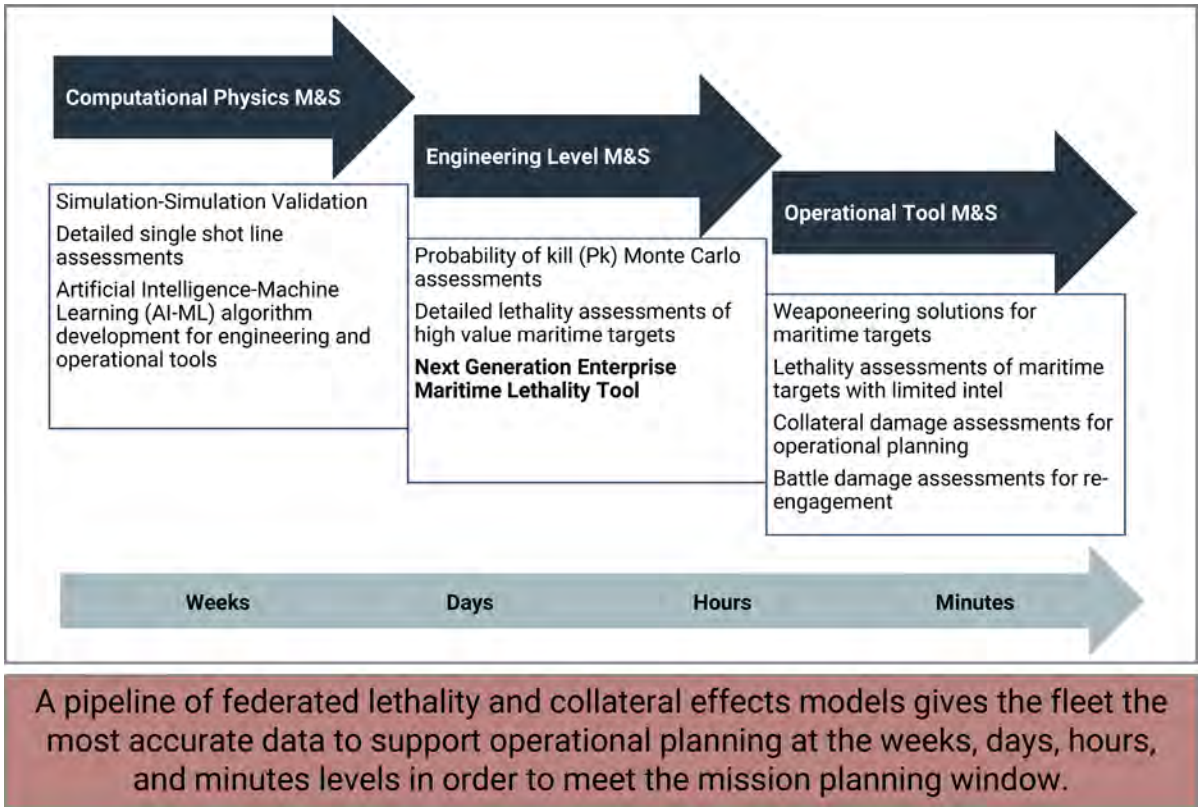


Figure 7. A Pipeline of federated models gives the fleet the most accurate data to support operational planning

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 reduce uncertainty in JTCG/ME, OT&E and LFT&E tools. JTCG/ME developed standardized documents to expand on the VV&A/UQ activities for next generation of JWS, Joint High-Power Microwave (HPM) Applied Weaponeering Knowledge Software (JHAWKS), Joint Laser Weaponeering Software (JLaWS), and document JTCG/ME's VV&A practices.

Data Management

To support the implementation of the DoD Data Management Strategy in FY23, JTCG/ME expanded the repositories for archival, review, approval, and access of lethality and vulnerability data, methodology, and documentation. The three following repositories serve multiple user communities with corresponding features and capabilities:

- For data, the Joint Analysis Repository and Visual Interface System (JARVIS) is a web-accessible repository with the authoritative data to support JTCG/ME's portfolio of warfighter applications. A critical requirement is to facilitate the data development and joint-Service review and approval processes. This repository also serves the T&E and acquisition community by providing JTCG/ME approved target vulnerability packages. In FY23, JTCG/ME deployed several updated versions of JARVIS that provided significant enhancements including data management capabilities for weapon characteristics and pre-generated weaponeering results.
- For methodology standards and practices, JTCG/ME created the Joint Effects Library (JEL), shown in Figure 8, as the official repository for all implemented methodology and supporting functions that are approved by JTCG/ME and use in weapon effects applications. Not only does it serve as an archive for all JTCG/ME approved modules, but it also enables the incorporation of standard acceptance workflow and supporting material. The intent is to improve quality, increase reusability and reliability, and finally reduce time to integrate modules into weaponeering applications. In FY23, JTCG/ME incorporated several additional modules into the JEL to support penetration

effects, cratering, material targets, and blast effects.

- For documentation, the Bugle is a wiki-style website built on Defense Technical Information Center's (DTIC's) DoDTechipedia platform. Hosting on DTIC makes JTCG/ME's technical reports, data requests, and model documentation accessible to the DoD community. In FY23, additional content was added to share information and collaborate on JTCG/ME products, models, and methodologies. In addition, JTCG/ME improved the site navigation and the overall user experience.

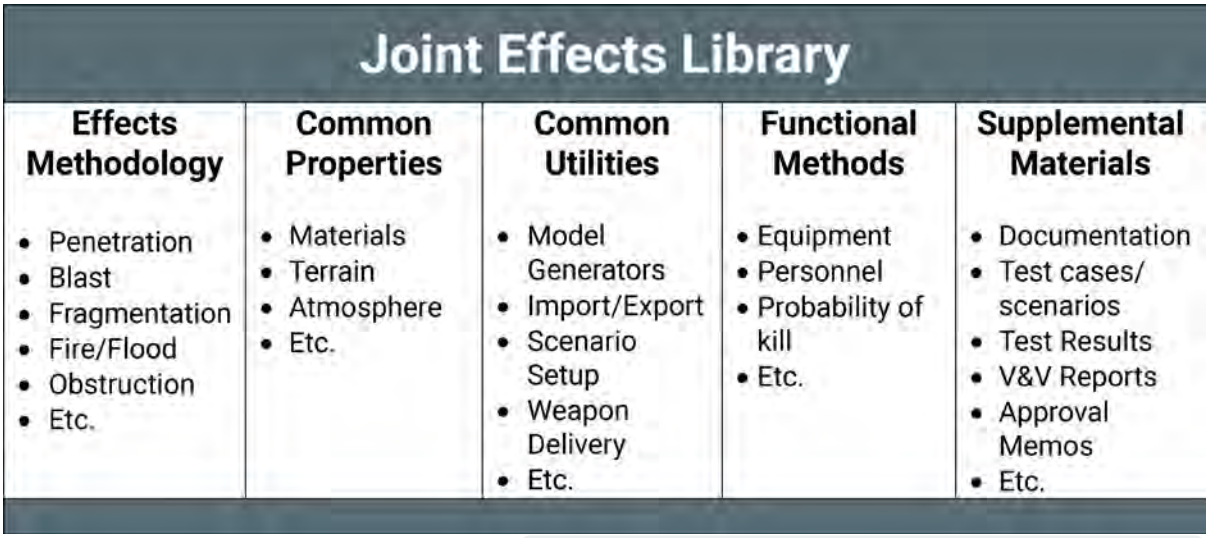


Figure 8. JEL Repository of JTCG/ME-accredited methodologies and documentation

These three repositories work in conjunction to provide joint-Service approved munition effectiveness data, methodology, and documentation within JTCG/ME and throughout the DoD.

In parallel, the JLF program continued to make progress towards establishing a framework capable of consolidating available and future LFT&E data in support of data mining and data analytics intended to effectively inform requirements, performance evaluations, and development of full-spectrum survivability and lethality tools. The U.S. Army Combat Capabilities Development Command Analysis Center is leveraging JARVIS to store tri-Service-developed and -approved target vulnerability data. Initial efforts focused on database structure development, user access controls, process flow and approval structure. This enhanced repository will be used to establish connections between Service-developed targets and the JTCG/ME products to enable access and sharing of more targets for the warfighter while facilitating military service data maintenance and control.

» ENABLING MULTI-DOMAIN SUPERIORITY WITH DEW, CYBER, INFLUENCE OPERATIONS, AND EMS FIRE WEAPONEERING TOOLS

JTCG/ME has made significant progress and worked in partnership with the Services, Department of Energy's National Laboratories (e.g., Sandia, Lawrence Livermore, Idaho), academia (e.g., Georgia Tech, Johns Hopkins Applied Physics Laboratory), and DOT&E field activities (e.g., Center for Countermeasures, JASP, Test and Evaluation Threat Resource Activity) to support 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, cyberattacks, and EMS fires, it has also initiated the plans to provide an architecture for a single JWS capable of estimating the appropriate number and type of either kinetic or non-kinetic weapons, and their combined effects, required to achieve superiority in a multi-domain operational environment.

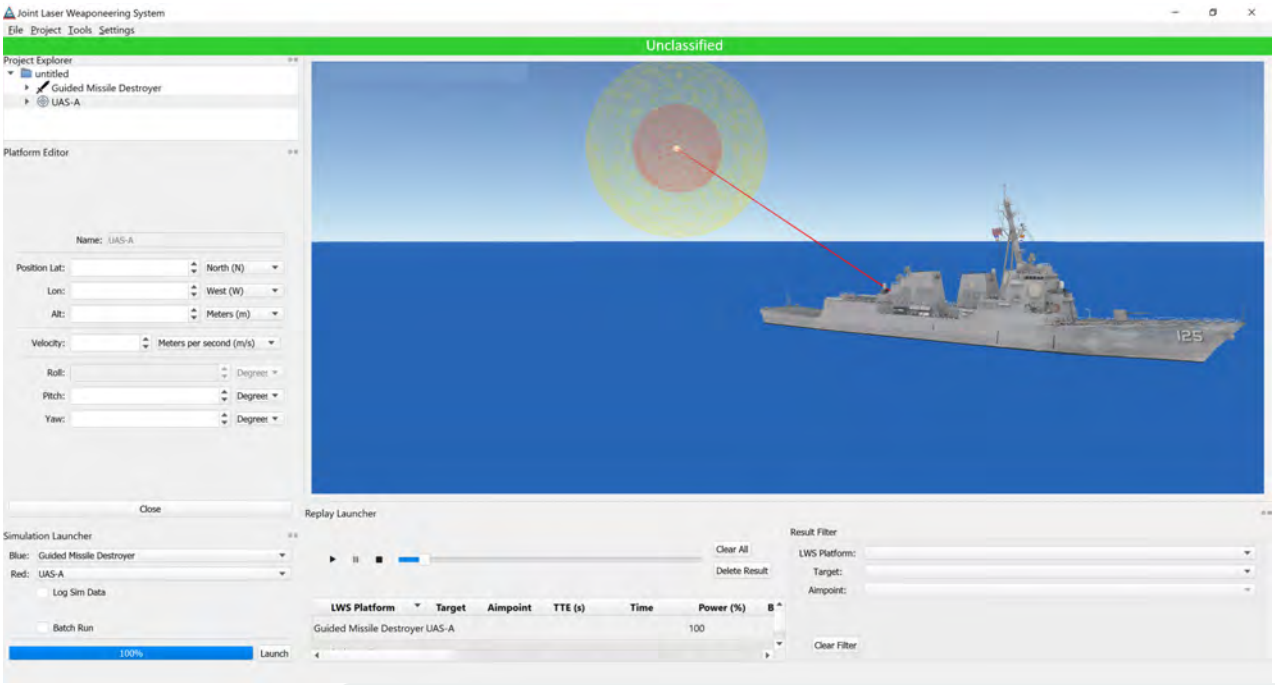


Figure 9. JLaWS simulation with HELRAT laser radiation hazard zones

DEW

In FY23, JTCG/ME continued to develop and validate DEW weaponeering tools – JLaWS and JHAWKS– to enable the CCMDs to estimate lethal effects using high energy lasers (HEL) and HPM.

JLaWS

JLaWS uses target data, weather effects, and optical risk characteristics to output associated vulnerability result and time to effect for solid state laser weapon systems. JLaWS considers the effect of weather on laser propagation by automatically downloading weather files from established services to account for location dependent weather conditions. JLaWS allows the user to calculate optical risk in the event of HEL reflections from targets using the High Energy Laser Risk Assessment Tool (HELRAT). HELRAT graphically portrays the risk distances around a target that contains reflected laser radiation levels that could cause ocular hazards to friendly forces in the area. Figure 9 shows a JLaWS graphical rendering of a ship-based Laser Weapon System (LWS) engagement with an unmanned aerial vehicle (UAV) target and the spherical zones around the target, as calculated by HELRAT, in which ocular hazards exist.

demonstrated JLaWS to multiple HEL LWS operational users to obtain operational feedback. As

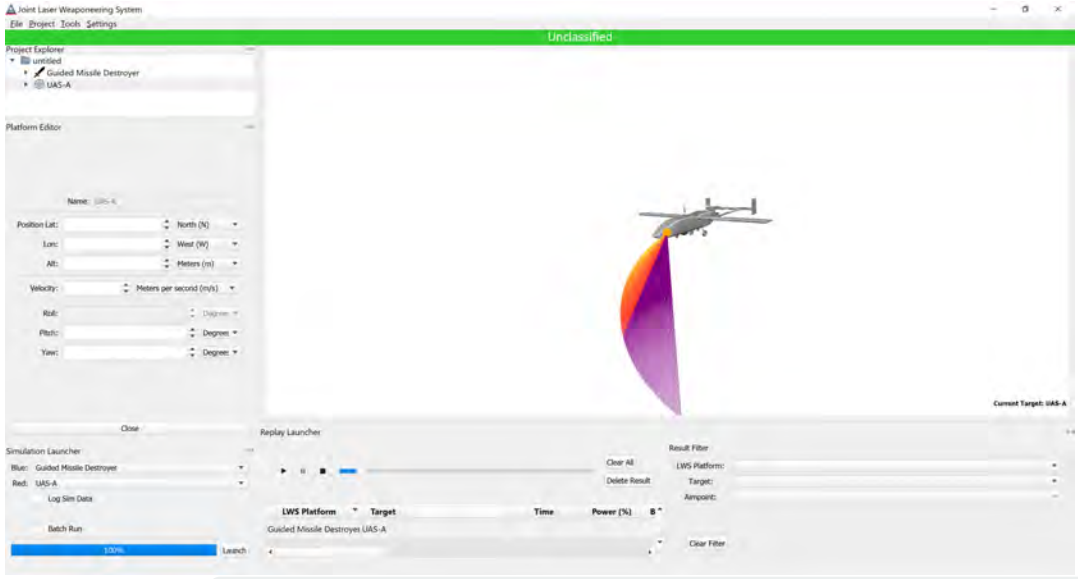


Figure 10. JLaWS Vulnerability Explorer and examples of shot lines

a result, JTCG/ME supplied operational users with JLaWS-developed target cards that displays optimal aimpoints on a target. Figure 10 shows an example JLaWS output for a UAV target. In FY23, JTCG/ME accredited HELRAT for use in functional domains, such as DoD exercises, training scenarios, and weapon system demonstrations.

JHAWKS

To advance the development and fielding of HPM weapon systems (HPMWS), JTCG/ME conducted several lethality tests against service-specific targets identified to fill data gaps. JTCG/ME conducted vulnerability and failure mode analyses to support M&S tool development and verification for both engagement level models and weaponeering tools. JTCG/ME identified and further developed an initial architecture for JHAWKS using the model-based systems engineering construct shown to the right of Figure 11. JTCG/ME continued further development of a tool for estimating collateral damage effects during HPMWS engagements and developed courses of action to integrate JLaWS and JHAWKS capabilities into DIEE.

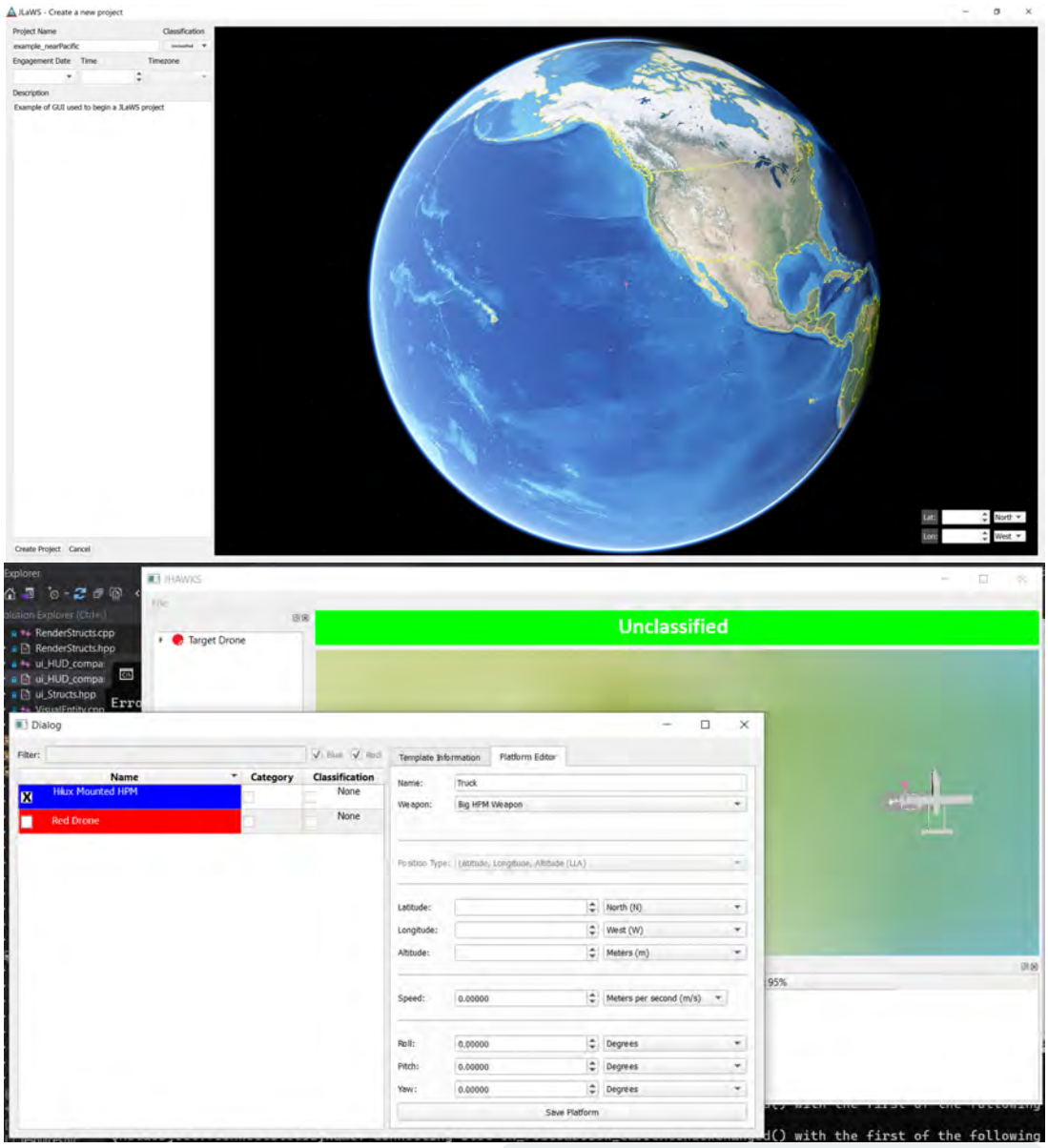


Figure 11. JHAWKS initialization windows

Cyber Operations Lethality and Effectiveness (COLE)

In FY23, JTCG/ME continued the development and fielding of cyber JMEM capabilities for the warfighter. The COLE tool is the foundational product, which enables commander operations decisions through advanced analytics used to adequately visualize, plan, evaluate, and assess the full spectrum of cyberspace activities. The COLE gateway delivers the DoD user with a comprehensive cyber effectiveness analysis capability for development, testing, and operational engagement.

JTCG/ME deploying v3.0 of the COLE tool on both classified and unclassified networks. COLE v3.0 enables mission planning allowing users to model cyber networks, characterize properties and associated uncertainties of network components, and model the effects of cyber capabilities against those networks. COLE's network characterization function allows users to create, manipulate, and share portrayals of network topologies for use in

planning cyber operations. COLE's mission planning function enables planners to devise attack options and routes through an adversary's network.

Major COLE improvements over the last year include continued development of the state and initial development of the functional model capabilities that allow planners to consider the dynamic state of the target network over time as well as considering access, and operational impact. These new features allow users to simulate and examine cascading effects within a network as multiple courses of action and different weapon-target pairings.

JTCG/ME also continued focus on user engagement with multiple Operational User Working Group and technical engagement sessions.

JTCG/ME continues to team with the JASP on the Machine Assisted Exploitability Simulation and Testing for Resilient Operations (MAESTRO) effort to further develop COLE's ability to assess cyber vulnerabilities of U.S. platforms. COLE for T&E provides a framework of models and tools to aid in examining aircraft cybersecurity.

In association with the JLF Cyber Automated Threat Discovery and Vulnerability Evaluation Reinforcement (CADAVER) program, the JNKE program continued its expansion of Enhanced Vulnerability Discovery abilities to assist in rapidly and automatically characterizing, discovering, and reporting cyber vulnerabilities within complex software configurations. CADAVER is intended to leverage AI/machine learning to allow identification of potential vulnerabilities to mitigate cyberattack access points through automated and semi-automated means. Combined, these programs ensure warfighters have the necessary tools to assess cyber effectiveness/vulnerability using tri-Service-approved data standards and streams. Leveraging technology and lessons learned of these three programs provide consistent, credible data and methodology for both offensive and defensive cyberspace operations.

Newly discovered vulnerabilities can be added to COLE's Common Vulnerability database to document and share Government-off-the-Shelf vulnerabilities amongst DoD organizations and cyber assessment teams.

In FY23, JTCG/ME also teamed with the DoD Test Resource Management Center to create a Cyberspace Effects and Enabling Capabilities Cyberspace Live-Fire Evaluation Framework (CLEF) to provide a realistic test environment for cyber capabilities generating accredited performance data. The CLEF effort will set the standards for generating and analyzing Cyber performance, analogous to kinetic area testing capabilities and standards for fragmentation.

Influence Operations

In FY23, JTCG/ME initiated a pathfinder for an influence operations JMEM aimed at considering how our military action affects an adversary's decision making towards achieving our own strategic aims. Behavioral influences analysis can help inform how the U.S. applies military force and what specific adversary elements to attack. Sandia National Laboratories has been developing a tool to assess how various populations and groups perceive U.S. actions. JTCG/ME's pathfinder works to expand capabilities in the dynamic multi-scale assessment tool for integrated cognitive-behavioral actions. JMEM pathfinder development focuses on the ability to assess influence operations on courses of action. This pathfinder effort will develop an approach to verify and validate an influence operations effectiveness digital tool that relies on integration of AI-engines, subject matter expertise-informed machine learning models, and extensive data sources to forecast how U.S. actions in all phases of operations will influence the decisions of adversary leadership.

EMS Fires

In FY23, JTCG/ME continued the development of weaponeering tools to enable mission planning and execution in contested, congested, and constrained EMS operations. These tools will estimate electronic attack (EA) effects and the ability of the warfighter to effectively prosecute adversary targets in contested, congested, and constrained EMS operations as shown in Figure 12.

JMEM for EMS Fires will allow mission planners and targeteers to assess weapon and combat effectiveness in the presence of adversary EA

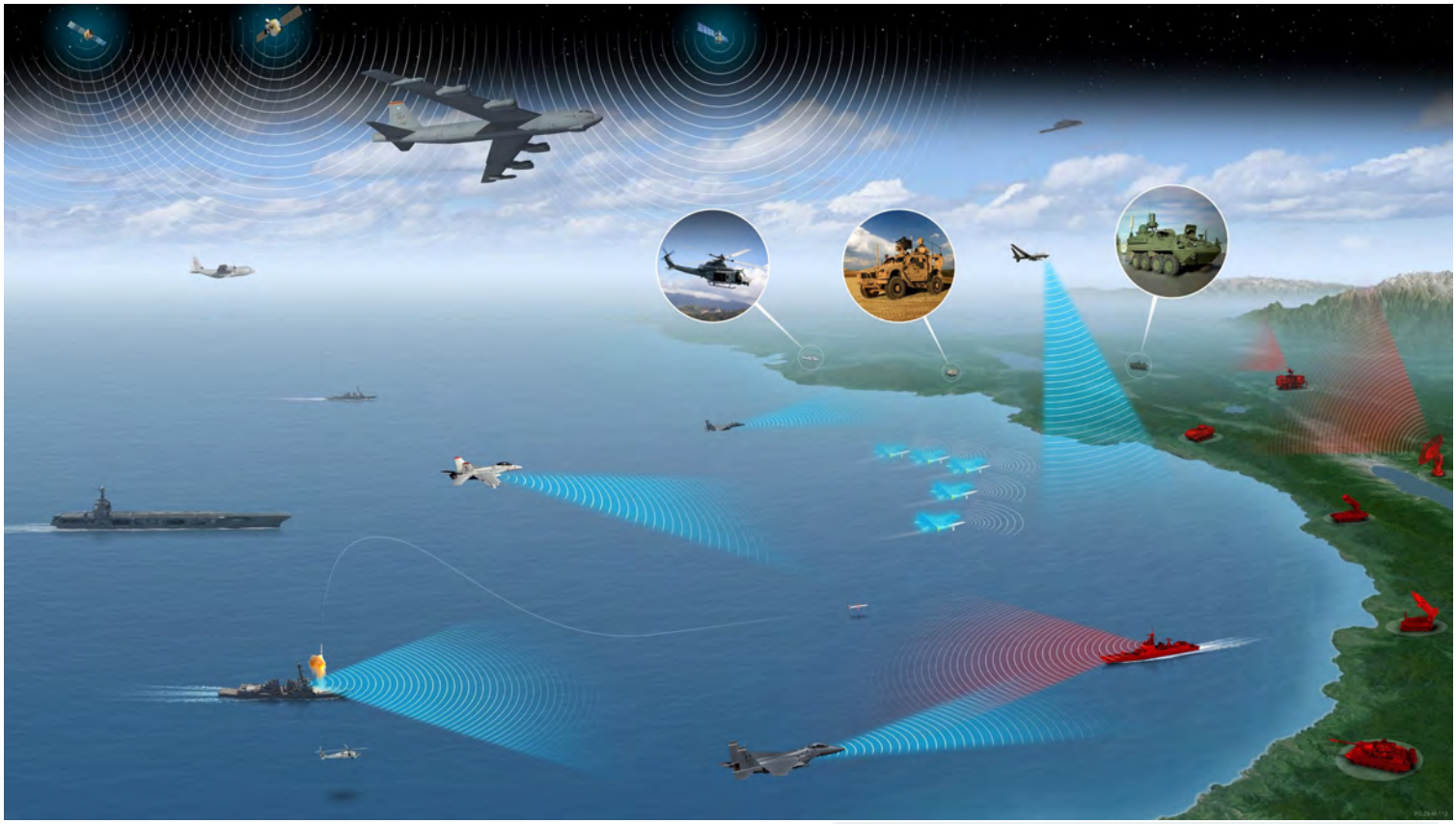


Figure 12. Sample notional EMS environment

(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 FY23, JTCG/ME further refined the program plan, data standards, capabilities requirements, and developed an initial cross service model to demonstrate EA effectiveness. The objective is to work towards developing an initial set of JMEM capabilities via the Joint EA Predictive tool by 1QFY24.

» SUPPLYING WEAPONEERING TOOLS TO SUPPORT INTEROPERABILITY WITH U.S. ALLIES AND PARTNERS

In FY23, JTCG/ME supported the delivery of weaponeering tools, data sets, and training to 25 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 that will help minimize collateral damage and reduce civilian casualties. These efforts directly supported the Presidential Conventional Arms Control Policy to build partner capacity and prevent civilian casualties. A second effort supported information exchange forums via information exchange annexes with coalition partners. These exchanges facilitate collaboration with partners on methodologies and efforts of mutual interest in weapons effectiveness and CDE for both kinetic and non-kinetic weapons. In FY23, multiple International Exchange Agreements were continued to provide weapons effectiveness analytical exchanges and to expand the scope of topics to better represent complex strategic and operational environments.

Joint Test and Evaluation (JT&E)

FY23 marked the reestablishment of the Joint Test and Evaluation (JT&E) Program and the return of the Joint Test process following the President's Budget 2023. The JT&E Program continued to execute warfighter-initiated test projects by managing 2 joint tests and 10 quick reaction tests (QRTs) to support development of non-materiel solutions to warfighter-identified problems. Specific FY23 activities demonstrated a trend toward addressing the integration of emerging weapons capabilities into tactics, techniques, and procedures (TTP), concepts of employment (CONEMPs), and concepts of operations (CONOPS).

PROGRAM OVERVIEW

The JT&E Program was established in 1972 in response to the 1970 Blue Ribbon Defense Panel Report recommending that responsibility for joint operational testing be vested in an OSD staff element. In 2002, management and responsibility for the JT&E Program transferred to DOT&E from the then Under Secretary of Defense for Acquisition, Technology, and Logistics. Today, the JT&E Program considers emerging technologies and the increasingly complex and dynamic, joint, multi-domain operational environment to plan and execute test projects intended to deliver non-materiel solutions and enhance the lethality, suitability, resilience, survivability, agility, and responsiveness of the joint force.

The Services and combatant commands (CCMDs) help identify critical challenges that need to be addressed in their areas of responsibility to maintain superiority across joint, multi-domain operations. The JT&E Program provides OT&E management and expertise to develop, test, and validate joint non-materiel solutions, including agile warfighting TTP, CONEMPs, and CONOPS. In turn, the Services and CCMDs provide leadership and support to the planning and execution of JT&E projects and their successful transition to the warfighter.

The JT&E Program focuses on joint requirements that cannot be economically or effectively tested within each of the individual Services and CCMDs. Given the increased integration and dependencies of platform, network, and command and control (C2) solutions across the domains, JT&E's mission and unique focus on system-of-systems testing is becoming increasingly critical to the Department's strategic objectives. JT&E's extensive use of OT&E testing techniques, workforce talents, and reach-back are essential to the adequate evaluation of the effectiveness of proposed solutions needed in operational plans across the CCMDs.

MISSION

The JT&E Program assists the warfighter in solving joint operational problems and issues by developing and testing proposed solutions using OT&E methodology. The resulting products are non-materiel solutions and reports detailing the operational performance of the joint force in contested, multi-domain operations.

FY23 KEY ACTIVITIES

» JOINT TESTS

During FY23, the JT&E Program started two joint test projects following the reestablishment of the JT&E Program in the President's Budget 2023. A joint test averages about two years in duration and is preceded by a six-month joint feasibility study.

Joint CONUS Directed Over-The-Horizon Radar (J-CONDOR)

Joint forces will face challenges in maintaining freedom of maneuver in complex multi-domain anti-access/area denial environments. Adversary and friendly forces have fielded variations of over-the-horizon radar (OTHR) that can detect air and surface targets at long ranges. The OTHR operates by transmitting high frequency radio waves that are reflected off the ionosphere into a surveillance area that can provide target cueing for adversary long-range weapon systems. In August 2023, JT&E initiated the J-CONDOR Joint Test to develop an overarching CONOPS that informs combatant commanders of adversary OTHR capabilities and mitigation strategies. The J-CONDOR CONOPS will include TTP for tactical commanders that synergizes maneuver with electronic systems and capabilities to counter detection and tracking by adversary OTHR. The J-CONDOR Joint Test includes several test events over the course of the two-year project utilizing air, maritime, and electromagnetic warfare resources to evaluate the J-CONDOR CONOPS and TTP.

Joint Conventional Nuclear Integration (J-CNI)

Conventional and nuclear integration requires seamless planning and operation of joint and combined conventional and nuclear forces, in sequence and in parallel, across the spectrum of conflict, up to and through a nuclear exchange environment. The scope of planning and execution of such operations encompasses more than conventional support to nuclear operations and requires full-spectrum integration of non-nuclear capabilities to enhance or complement nuclear options. In August 2023, JT&E initiated the J-CNI Joint Test to develop, test, and evaluate a CONOPS for defining integrated conventional and nuclear options that are executable within a pre-synchronized timeline and effectively assign these missions to the responsible organizations. The J-CNI Joint Test is expected to conclude in November 2025.

» QUICK REACTION TESTS

During FY23, the JT&E Program managed 10 QRT projects. QRTs provide a faster response to urgent joint needs but must focus their objectives to execute within the shortened, 12-month contract duration.

Automated Tactical Targeting and Counterfire Kill-Web System (ATTACKS)

During large-scale combat operations, tactical operators within the U.S. Forces Korea Counterfire Task Force Air Component Command must employ and disseminate counterfire against North Korea's long-range artillery threats efficiently, at scale, and within their vulnerability window. The ATTACKS uses joint sensors and the existing Combined Joint All-Domain Command and Control (CJADC2) software to automate data transfer between disparate counterfire systems using machine learning. By automating disparate data links, U.S. forces in South Korea can reduce the total time required to neutralize the long-range artillery threat from minutes to seconds, preventing potential catastrophic loss of life in the Greater Seoul Metropolitan Area.

In March 2023, JT&E initiated the ATTACKS QRT to develop and validate TTP to optimize the automation provided by ATTACKS to support the Counterfire Task Force mission. FY24 testing will use a multi-domain counterfire team, airborne fighter/reconnaissance aircraft, and surface counterfire platforms with the Advanced Field Artillery Tactical Data System. The Tactical Air Control Party and Tactical Command and Control systems will integrate this software into current C2 systems aiming to nest ATTACKS with emerging CJADC2 efforts including Advanced Battle Management System, Project Convergence, and Project Overmatch. ATTACKS will address tactical C2, voice and data link communication, and fire support coordination measures required to employ the system most efficiently against two brigade-size long-range artillery forces attacking simultaneously both within and outside of defined garrison boundaries.

The ATTACKS QRT will enable broader CJADC2 by operationally optimizing a multi-domain kill-web of mobile C2 nodes, sensors, and shooters. The QRT is intended to prove that U.S. Forces Korea C2 of counterfires are more redundant and survivable than a structure reliant on fixed facilities. The ATTACKS-developed TTP will propose changes to Combined Air Component Commander Wartime Baseline Special Instructions and the Combined Forces Command Publication 3-1-1, Combined Joint Fires. The QRT team is expected to complete development of the initial ATTACKS TTP in 1QFY24.

CONOPS for Novel Information Warfare Capabilities (CNIWC)

U.S. Strategic Command (USSTRATCOM) and overall DoD mission success relies on the ability to optimize information warfare capability. In October 2022, JT&E initiated the CNIWC QRT to develop and test a Joint Information Warfare CONOPS that will be executed by USSTRATCOM. CNIWC began work in September 2023 to support development, testing, and validation of a stand-alone CONOPS, which is expected to result in changes to multiple joint and Service doctrine by 4QFY24.

Joint Aviation Signature Management Analysis, Application and Rehearsals Tool (JA-SMAART)

The U.S. Army Aviation Center of Excellence requires a standardized and repeatable test methodology to evaluate electromagnetic signatures of slow flying, joint tactical aircraft. In FY23, JT&E initiated the JA-SMAART QRT to develop TTP and a series of models to directly improve aircraft survivability in contested, congested, and constrained electromagnetic spectrum operations. Assisted by Air Force and Navy organizations that have electromagnetic signatures modeling capabilities, JA-SMAART will produce standardized models by aircraft type and configuration that support current mission planning analysis tools. The resulting models are intended to increase aviation combat survivability through a reduction in aircraft susceptibility in mission planning and use in multi-domain operations. Upon completion in FY24, the project is expected to deliver a validated test methodology for future use as well as accurate, realistic susceptibility models that have an immediate benefit to the warfighter and use in joint aviation mission planning software suites.

Joint Development of Hypersonic Weapons Employment (J-DoHE)

USSTRATCOM J3 requires a hypersonic weapons CONEMP that addresses decision timeline, fire request procedures, and communication paths for hypersonic weapons. In January 2022, JT&E initiated the J-DoHE QRT to develop and test a CONEMP based on the CONOPS developed by the Joint Hypersonic Strike Planning, Execution, Command and Control Joint Test in 2020. During FY23, the QRT team conducted two field tests at Offutt AFB, Nebraska, to validate the J-DoHE Hypersonic Weapons CONEMP, which focused on decision and execution communication flow at the operational level. Upon completion in July 2023, the J-DoHE QRT delivered the CONEMP to position USSTRATCOM to successfully plan and employ long-range hypersonic weapons upon initial fielding.

Joint Distributed Command and Control (J-DC2)

Changes in military capabilities, resource allocations, and emerging technologies will dictate how the United States plans and executes a future J-DC2 capability. In response to these changes, USSTRATCOM J8 and the Nuclear Command, Control, and Communications Enterprise Center require a CONOPS for a future nuclear C2 capability that is flexible, resilient, and distributed. In July 2022, the J-DC2 QRT began work with the sponsor, other CCMDs, the Joint Staff, U.S. agencies, the U.S. Navy, the U.S. Air Force, and additional relevant stakeholders to develop a draft CONOPS for future nuclear C2. The J-DC2 QRT conducted tabletop exercises at Offutt AFB, Nebraska, in June and August 2023 to evaluate and validate the CONOPS. The final product is a validated CONOPS that will inform the development and implementation of future nuclear C2 operations to achieve positive operational outcomes for J-DC2 platforms.

Joint-Global Hypersonic Operational Sensor Tasking (J-GHOST)

The joint warfighter requires doctrine to deconflict, coordinate, and integrate attacks that include emerging technologies and newly fielded capabilities within emerging Space Domain Awareness, Missile Defense, and Missile Warning doctrine. In October 2022, JT&E initiated the J-GHOST QRT to develop, test, and deliver validated Space Domain Awareness CONOPS and associated TTP to rapidly task external sensors and internal missile defense sensors in real-time during advanced trans-regional threat events. The goal is to operationally improve responsiveness for no-notice tasking of Missile Warning, Missile Defense, Space Domain Awareness, and other sensors to support detection and improve track custody and reporting of time-sensitive, multi-domain, trans-regional, advanced threats, and high-interest space events. J-GHOST began test activities in August 2023 to support the Missile Defense Agency and U.S. Space Command in jointly delivering tested and validated CONOPS and TTP to enable warfighters to detect, track, and report on advanced threats. The J-GHOST team includes participants from six CCMDs, the Services, the Missile Defense

Agency, and Australian defense organizations. The team expects to complete the QRT in 4QFY24.

Joint Interface Control Cell Resiliency (JICC-R)

Joint Interface Control Cell personnel need the ability to detect, respond to, and recover from issues on data links. In March 2023, JT&E initiated the JICC-R QRT to develop TTP for Joint Interface Control Cell personnel. JICC-R is focused on improving operational resilience in the event of data integrity loss across military activities. The QRT team began work in October 2023 to support testing, analysis, and evaluation required to produce the JICC-R TTP. The project is expected to conclude in 4QFY24.

Joint Operation NOBLE EAGLE Link-16 Tactical Data Link (JOLT)

Until recently, U.S. Coast Guard (USCG) Rotary Wing Air Intercept (RWAI) aircraft were not equipped with a tactical data link system and relied only on visual information and aural advisories from the Eastern and Western Air Defense Sectors. The Coast Guard Deputy Commandant for Operations, with advisory direction from North American Aerospace Defense Command (NORAD), established a requirement that all USCG MH-65 aircraft participating in RWAI missions have a tactical data link capability to enable real-time visual situational awareness among active air intercept participants. In October 2022, JT&E initiated the JOLT QRT to develop and assess TTP for RWAI missions flown in conjunction with Air Force or Navy aircraft and Army Ground Based Air Defenses controlled by the Eastern and Western Air Defense Sectors in the Continental NORAD Region. The JOLT QRT team is jointly developing the TTP with USCG and Joint Staff J6 using a test-fix-test approach with the first field test occurring at USCG facilities in Atlantic City, New Jersey, in November 2023. The JOLT QRT is expected to complete in 3QFY24.

Joint Operations in the Information Environment Playbook Toolkit (J-OPTiK)

Digital and social media have become the new battleground for Operations in the Information Environment (OIE). OIE cells face challenges in assessing social media, coordinating messaging, countering adversaries, and adapting strategies for commanders' intent essential for approved narratives and information advantage. OIE analyst procedures lack commander-aligned efficiency, which leads to coordination gaps among Service OIE cells and hinders timely actions. In January 2022, JT&E initiated the J-OPTiK QRT to formalize and validate TTP for digital and social media campaigns to cover deep analysis, course of action development, and synergistic messaging for use of social media accounts. The J-OPTiK developed tested products that include a TTP, BEND guidebook, and corresponding Spot Report. These products were based on the 16 information actions of the BEND framework known as "the four Bs" – back, build, bridge, boost; "the four Es" – engage, explain, excite, enhance; "the four Ns" – negate, neutralize, narrow, neglect; and "the four Ds" – dismiss, distort, dismay, distract.

The J-OPTiK products describe the process for planning multi-domain OIE series in the joint community at the tactical level to enhance warfighter effectiveness in the information environment. With the participation of OIE analysts from various Services, the two J-OPTiK field tests in California and Hawaii validated product effectiveness and support for OIE analysts in crafting recommended courses of action. These two events utilized synthetic data from Carnegie Mellon University's Center for Computational Analysis of Social and Organizational Systems, in partnership with the Office of Naval Research. The introduction of synthetic X (formerly known as Twitter) content into an OIE wargame training environment supported assessments of operator outcomes in real-world scenarios and their ability to effectively apply the results within the information environment. The J-OPTiK QRT team concluded that the tested and validated products empower OIE analysts to evaluate the information environment demonstrating effective responses and strategic information actions.

The following OIE cell participants have moved toward implementation of the products: Command Naval Forces Japan, the Army's 1st Multi-Domain

Task Force, I Marine Expeditionary Force Information Group Psychological Operations Company, the Air Force's 553 Intelligence Squadron, 188th Wing of the Arkansas Air National Guard, and the Publicly Available Information Center of Excellence. The J-OPTiK QRT test products transitioned to the Joint Information Operations Warfare Center in September 2023 to ensure seamless warfighter access to the products for daily operations. Possible integration of J-OPTiK products under consideration by Joint Information Operations Warfare Center for warfighter usability includes an annex in Joint Publication 3-04, Information in Joint Operations; conversion to an Air Land Sea Space Application Center multi-Service TTP; and inclusion in a Joint Knowledge Online course.

More Situational Awareness for Industrial Control Systems (MOSAICS)

The U.S. military is dependent on critical infrastructure to execute its mission. In the event of a contentious conflict, it is anticipated the adversary will conduct an unattributed cyberattack via proxy on U.S. critical infrastructure. The likely intent of such action is to slow the military's ability to generate forces and unleash logistics support of global operations in defense of allies. U.S. Indo-Pacific Command and U.S. Northern Command signed a joint letter in 2016 requesting development of capabilities to protect DoD Industrial Control Systems (ICS). In response, NORAD and U.S. Northern Command J4 requested the development of processes and procedures to enable ICS/Operational Technology operators and cyber defenders to fully detect, analyze, mitigate, and recover their systems from cyber interference or attack.

In January 2022, JT&E initiated the MOSAICS QRT to refine TTP and CONOPS to help prevent proxy cyberattacks and allow the U.S. projection of force to change the operational outcome. The MOSAICS QRT conducted two field tests at Port Hueneme, California, in March and June 2023, resulting in validated products that include a revised TTP and CONOPS for future MOSAICS systems employment across the DoD and private sector. Upon project completion in September 2023, the test products transitioned to Naval Facilities Engineering Systems Command as the initial product owner and user. The revised MOSAICS TTP and CONOPS have enhanced ICS cyber survivability education and training as well as security at locations where the U.S. Navy is programmed to install MOSAICS systems.

Test and Evaluation Threat Resource Activity (TETRA)

In FY23, the Test and Evaluation Threat Resource Activity (TETRA) continued with the evaluation of current and emerging threat system capabilities critical to OT&E and LFT&E of DoD systems and services. These included but were not limited to the capabilities of the contested electromagnetic spectrum (EMS) environment, the use of artificial intelligence (AI) in adversary systems, evaluations of the adversary order-of-battle, concept of operations, and tactics, techniques, and procedures (TTP). For example, TETRA kicked off an initiative to develop cognitive, AI-driven, and other high complexity threat models to enable T&E of cognitive and AI-driven electronic warfare (EW) systems. TETRA also initiated the development of high-fidelity space threat models and counterspace threat surrogates to support OT&E and LFT&E of space systems. TETRA managed the development of over 132 Intelligence authoritative analysis projects and delivered threat and target data to support the accreditation of physical surrogates and digital representations of threat and targets for use in OT&E and LFT&E.

PROGRAM OVERVIEW

TETRA is a joint duty activity between DOT&E and the Defense Intelligence Agency (DIA) that was established in 2000 to ensure that OT&E and LFT&E programs, as well as warfighter mission planning and training, are adequately informed by the latest and emerging intelligence data. TETRA is comprised of DIA analysts, engineers, modelers, and scientists responsible for supplying authoritative and timely intelligence assessments of the current and emerging multi-domain threat environment to the OT&E and LFT&E Enterprise. Specifically, TETRA: (1) generates artifacts that include intelligence-based analysis of current and emerging threats and targets; (2) facilitates the acquisition and exploitation of foreign materiel needed for testing or development of threat and target surrogates; (3) oversees threat and target surrogate verification, validation, and certification to include hardware surrogates and digital representations (e.g., models, simulations, digital twins); and (4) leverages emerging science and technologies to project expected threat and target capabilities. TETRA's position as a threat and intelligence liaison between the acquisition, test, and intelligence communities ensures unique intelligence support tailored to OT&E and LFT&E requirements.

MISSION

In coordination with the DIA and the Services' intelligence production centers, TETRA conducts analysis and supports the delivery of capabilities of threat and target digital representations, surrogates, and foreign materiel to meet the unique OT&E and LFT&E requirements.

FY23 KEY ACTIVITIES

» INTELLIGENCE ANALYSIS TO SUPPORT OT&E AND LFT&E

In FY23, TETRA continued to improve the capabilities of over 50 new and emerging threats and targets to support adequate evaluation of the operational effectiveness, suitability, survivability, and lethality of DoD systems and services:

- Completed two DIA analytic exercises addressing the emerging ballistic and hypersonic missile threat challenges in support of the Next Generation Interceptor (NGI) weapon system. The exercise resulted in two reports used by Missile Defense Agency and DOT&E to assess the defined threat space for the NGI program and the adequacy of the operational test plans for NGI.
- Led the Cyber Exercise Support Team (EST) to provide real-world threat and intelligence data to U.S. Indo-Pacific Command's (USINDOPACOM's) exercise PACIFIC SENTRY 2023 (PS23). The exercise was linked to another USINDOPACOM exercise designed to develop options in response to adversary capability in a cyber-contested environment.
- Provided analysis of emerging threats and changing adversaries' TTP of tactical, operational, and strategic significance to our U.S. forces with focus on new threat capabilities for EW, AI, cognitive EW, joint communications, cyber, navigation warfare improvements, and kinetics from artillery and anti-tank guided munitions. The investment roadmap, projects, reports, and analysis were delivered to DOT&E, the Operational Test Agencies, Test Resource Management Center, OSD Cost Assessment and Program Evaluation (CAPE), and other senior officials in the DoD.
- Assessed threat scenarios to meet Missile Defense Agency operational test planning objectives defining adversarial order-of-battle, force laydown, and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities for specific areas of responsibility. This increased the T&E community's awareness of stressing threat systems needed to inform realism for operational testing.
- Assessed performance capabilities, flight profile characteristics, and employment tactics for multiple stressing foreign antiship cruise missiles to aid establishing operational test design criteria for evaluating naval area and

point defense antiship missile defense systems against operationally realistic threat missile performance and employment capabilities.

- Provided the analytical support to enable and accelerate the development of a new threat representative surrogate to emulate adversaries' naval countermeasure systems.
- Supported the characterization of the small boat threat to meet OT&E and LFT&E requirements including small boat design characteristics, armament, performance capabilities, operational employment tactics, and order-of-battle.

» KEEPING PACE WITH EMERGING THREATS AND TARGETS

In FY23, TETRA:

- Developed the first blue force and red threat cognitive EW and AI model and cognitive EW digital and hardware-in-the-loop test environment and analysis toolsets to support the T&E of advanced EW systems that sense and prosecute unknown radio frequency (RF) threats using AI. These efforts directly supported the EC-37B Compass Call and the F-35 programs. For example, the efforts helped to identify and evaluate existing tools that may be used to solve the data environment challenges the EW OT&E community faces. By designing and constructing reusable solutions and guidance for the establishment of a threat environment for cognitive capability test and development, DOT&E is meeting many of the goals of the DOT&E Strategy Implementation Plan.
- Developed a roadmap and demonstrated progress in solving test capability gaps for the evaluation of U.S. space systems' resiliency to potential counterspace electronic warfare threats and RF-enabled cyber threats to satellite communications (SATCOM) and satellite telemetry, tracking, and command. The capabilities developed in this ongoing effort will enable resiliency testing of military satellite communications and tracking, telemetry, and control signals – which affect all DoD space programs – in digital, hardware-in-the-loop, and open-air environments. The roadmap met the requirements identified in the DoD Ranges Workshop; the National Space Test and Training Complex and U.S. Space Force needs; and the 2021 and 2022 National Academies of Sciences, Engineering, and Medicine's "range of the future" reports.[1]

» ACQUIRING ACTUAL FOREIGN THREATS

OT&E and LFT&E programs rely on the availability of actual, foreign materiel threat systems to either test our systems against or to reverse engineer the threat or target to support the development of threat or target surrogates (either physical or digital). In the absence of the actual threat, TETRA supplies the best available Intelligence data on the threat or target characteristics and capabilities critical to the development of their surrogates.

To secure actual systems for Intelligence analysis and use in operational testing, TETRA works directly with the Joint Foreign Materiel Program Office, overseen by the OUSD(I&S), as well as other foreign materiel organizations and the Intelligence Community. In coordination with the OT&E and LFT&E community, TETRA supplies a prioritized and coordinated list of foreign materiel required for upcoming operational and live fire tests to inform Intelligence Community collection opportunities. The Joint Foreign Materiel Program is a critical link between the T&E community, DIA, and the Department of State that increases the visibility of T&E requirements in support of operationally representative testing and warfighter training. Foreign materiel requirements span all warfare areas. In FY23, TETRA monitored and coordinated over 100 acquisition efforts. The demand for a wide array of foreign man-portable air-

1 "Range of the future" reports refer to both: (1) National Academies of Sciences, Engineering, and Medicine. 2021. *Necessary DoD Range Capabilities to Ensure Operational Superiority of U.S. Defense Systems: Testing for the Future Fight*. Washington, DC: The National Academies Press. and (2) National Academies of Sciences, Engineering, and Medicine. 2022. *Enabling DoD's Test Ranges and Infrastructure to Meet Threats and Operational Needs in the 21st Century*. Washington, DC: The National Academies Press.

defense systems (MANPADS) continues to be high for: (1) the development of MANPADS surrogates to enable adequate testing of countermeasures, (2) representative missile seekers and software for use in hardware-in-the-loop laboratories, and (3) LFT&E to test the vulnerability of U.S. weapon systems when engaged by such a threat. Foreign antitank guided missiles have also been in high demand to support the testing of the evolving Active Protection System employed by ground combat vehicles. GPS jammers have been in demand for testing of GPS-guided weapons. Very high frequency radars have been required for programs such as the F-35, in order to determine how to counter longer acquisition range and low probability of intercept threat systems. Decoys of foreign surface-to-air missile systems are in recent demand for threat density and operational realism. In FY23, TETRA:

- Developed and managed a highly successful foreign materiel acquisition essential to delivering threat density for U.S. and allied OT&E range capability critical to F-35, B-21, and over 50 other DoD systems and services acquired via the Defense Acquisition System.
- Led critical foreign materiel acquisition and delivery of essential systems for U.S. support to an ally in a wartime environment.

» ACCREDITED THREAT AND TARGET MODELS AND SURROGATES

In the absence of actual foreign threats, which can be difficult to acquire, TETRA supports the OT&E and LFT&E community with Intelligence data (e.g., EW techniques, threat models) required to develop and accredit threat and target surrogates, either physical or digital replicates. In accordance with DoD Instruction 5000.61 and DOT&E policy on M&S verification, validation, and accreditation, TETRA oversees the threat surrogate verification, validation, and certification process to assess the uncertainties of the threat surrogate compared to the actual threat system that the warfighter would encounter in combat. TETRA 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 ensures threat and target 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 FY23, TETRA provided threat intelligence, validation and certification expertise, and oversight for more than 14 joint and Service threat validation efforts, including:

- The Navy's Maritime Survivability Library.
- The Next-Generation Jammer to develop a method to validate and certify the radar electronic attack countermeasure tool.
- The M&S gaps and verification, validation, and accreditation in support of Missile Defense System ground testing.

In FY23, TETRA also continued the development, validation, and delivery of 10 radio frequency and 10 infrared high-priority threat models, as well as over 25 high-fidelity, closed-loop, EW-capable, emulative threat models using ITEAMS assessments. These included four laboratory intelligence-validated emulators (LIVEs), four within-engagement EW (WEEWs), and seven common high-assurance internet protocol encryptor interoperable manager for efficient remote administration (CHIMERA) models.

TETRA is leading a partnership between the Intelligence Productions Centers and the Space Force to produce counterspace threat models supporting OT&E of space systems in the National Space Test and Training Complex. In FY23, TETRA initiated a model development effort for a high priority counterspace threat to facilitate operational testing of DoD space systems' defensive measures and operator TTPs against a threat that cannot be tested in a live environment due to security, safety, and policy constraints. This model, as well as others produced under the partnership, will form the foundation for evaluating the capability and resiliency of U.S. space programs in the contested space domain.

APPENDIX

This page intentionally left blank.

Oversight List

This page intentionally left blank.

DOT&E Oversight List as of September 30, 2023

- 120MM Advanced Multi-Purpose (AMP), M1147, High Explosive Multi-Purpose with Tracer (HEMP-T) (M1147 AMP)
- Abrams M1A1 SA; M1A2 SEP; APS
- AC-130J High Energy Laser
- Advanced Airborne Sensor
- Advanced Anti-Radiation Guided Missile - Extended Range
- Advanced Arresting Gear
- Advanced Battle Management System
- Advanced Field Artillery Tactical Data System (AFATDS)
- 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 (MRO)
- Air Force Next Generation Air Dominance
- Air Operations Center Weapon System Modifications
- Air Warfare Ship Self Defense Enterprise
- Air-Launched Rapid Response Weapon
- Amphibious Combat Vehicle (ACV) Family of Vehicles (FoV)
- AN/APR-39E(V2) Radar Warning Receiver
- AN/AQS-20X Minehunting Sonar and Tow Vehicle (all variants)
- AN/TPQ-53 Counterfire Target Acquisition Radar
- Armed Overwatch
- Armored Multipurpose Vehicle (AMPV)
- Assault Breaching System Coastal Battlefield Reconnaissance and Analysis System (all variants)
- B-21 Long Range Strike Bomber
- B-52 Radar Modernization Program (RMP)
- B-52J Commercial Engine Replacement Program (CERP)
- Barracuda Mine Neutralization System
- Booker Combat Vehicle (BCV)
- Bradley ECP; MOD; APS
- Cannon Delivered Area Effects Munitions (C-DAEM) Armor (Inc 1)
- Capability Set 21/23 Integrated Tactical Network - Rapid Fielding
- CH-47F Modernized Cargo Helicopter
- CH-53K King Stallion
- Close Terrain Shaping Obstacle Increment 1 (CTSO INC 1)
- CMV-22 Joint Services Advanced Vertical Lift Aircraft - Osprey -- Carrier Onboard Delivery (COD)
- Cobra Dane Automated Data Processing Equipment Rehost Phase II
- Columbia Class SSBN - including all supporting PARMs
- Command Post Computing Environment/ Tactical Services Infrastructure
- Common Infrared Countermeasures (CIRCM)
- Common Tactical Truck (CTT)
- Compact Rapid Attack Weapon

DOT&E Oversight List as of September 30, 2023

- Consolidated Afloat Networks and Enterprise Services
- Conventional Prompt Strike
- Cooperative Engagement Capability (CEC)
- Cooperative Engagement Capability Increment II
- Counter Insider Threat Capability
- 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)
- Deliberate and Crisis Action Planning and Execution System (DCAPES) Inc. 2B
- Digital Modernization Strategy (DMS) – Related Enterprise Information Technology Initiatives
- Dismounted Assured Positioning, Navigation, and Timing System (DAPS)
- Distributed Common Ground System - Army (DCGS-A)
- Distributed Common Ground System - Navy (DCGS-N)
- DoD Healthcare Management System Modernization (DHMSM)
- Dry Combat Submersible (DCS)
- E-2D Advanced Hawkeye
- E-7A Rapid Prototyping
- EA-18G - Airborne Electronic Attack
- EC-37B Compass Call Rehost
- Electro-Magnetic Aircraft Launching System
- Electronic Warfare Planning and Management Tool (EWPMT)
- Enhanced Polar System
- Enterprise Air Surveillance Radar
- Enterprise Business Systems Convergence
- Enterprise Space-Based Missile Warning
- Evolved Sea Sparrow Missile Block 2
- Evolved Strategic Satellite Communications
- Evolved Strategic Satellite Communications - Cryptologic Segment
- Evolved Strategic Satellite Communications Ground Segment
- 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 and Survivability System
- F-15EX
- F-16 AN/ALQ-257 Integrated Viper Electronic Warfare Suite
- F-16 Radar Modernization Program
- F-22 - RAPTOR Advanced Tactical Fighter Aircraft
- F-22 Capability Pipeline
- F-35 - Lightning II Joint Strike Fighter (JSF) Program
- Family of Advanced Beyond Line-of-Sight Terminals
- Family of Advanced Beyond Line-of-Sight Terminals Force Element Terminal
- Family of Medium Tactical Vehicles A2 (FMTV A2)
- FFG(62) Guided Missile Frigate
- Future Attack Reconnaissance Aircraft - Capability Set 1 (FARA CS1)
- Future Long Range Assault Aircraft MTA
- Future Operationally Resilient Ground Evolution Rapid Prototype
- Future Tactical Unmanned Aircraft System INC 1 (FTUAS INC 1)

DOT&E Oversight List as of September 30, 2023

- Future Tactical Unmanned Aircraft System INC 2 (FTUAS INC 2)
- Future Unmanned Aircraft System-Air Launched Effects (FUAS ALE)
- Future Unmanned Aircraft Systems - Scalable Control Interface (FUAS SCI)
- Future Vertical Lift (FVL) Future Unmanned Aircraft System (FUAS)
- Geosynchronous Space Situational Awareness Program
- Global Command & Control System - Joint (GCCS-J)
- Global Positioning System (GPS) Enterprise Oversight
- Global Positioning System III
- GPS III Follow-on Production
- GPS Next Generation Operational Control System Block 3F
- 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
- High Accuracy Detection and Exploitation System (HADES)
- 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 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 Air and Missile Defense of Guam
- Integrated Head Protection System (IHPS)
- 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 1.2 (IVAS 1.2)
- 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 Biological Tactical Detection System
- Joint Cyber Warfighting Architecture - Access Platform
- Joint Cyber Warfighting Architecture - Joint Cyber Command and Control
- Joint Cyber Warfighting Architecture - Persistent Cyber Training Environment
- Joint Cyber Warfighting Architecture - Unified Platform
- Joint Cyber Warfighting Architecture Enterprise
- Joint Cyber Weapons
- Joint Development Environment
- Joint Light Tactical Vehicle Family of Vehicles
- Joint Operational Medicine Information Systems
- Joint Planning and Execution System
- Joint Regional Security Stack (JRSS)
- KC-46A Tanker Modernization

DOT&E Oversight List as of September 30, 2023

- Key Management Infrastructure (KMI)
- Large Displacement Unmanned Undersea Vehicle (LDUUV)
- Large Unmanned Surface Vehicle
- LGM-35A Sentinel
- LHA 6 Flt I and associated PARMs
- Littoral Combat Ship (LCS) Mine-countermeasures (MCM) Mission Package
- Littoral Combat Ship (LCS) Surface Warfare (SUW) Mission Package
- Littoral Combat Ship (LCS), FREEDOM and INDEPENDENCE Variant Seaframes
- Long Range Hypersonic Weapon (LRHW)
- Long Range Stand Off Weapon
- Long Range Unmanned Surface Vessel
- 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 Landing Ship
- Medium Unmanned Surface Vehicle
- MH-139A Grey Wolf
- Mid-Range Capability (MRC)
- 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
- Mounted Assured Positioning, Navigation, and Timing System (MAPS)
- Mounted Mission Command - Software
- Mounted Mission Command-Transport (MMC-T)
- MQ-25 Stingray
- MQ-4C Triton
- MQ-8C Fire Scout Unmanned Aircraft System
- Multi-Function Electronic Warfare
- National Background Investigation System
- Naval Integrated Fire Control - Counter Air (NIFC-CA) From the Air
- Naval Maintenance, Repair and Overhaul Solution
- Naval Operational Supply System
- Navy Personnel and Pay System
- Next Generation Jammer - Mid-Band
- Next Generation Jammer Low Band
- Next Generation Large Surface Combatant
- Next Generation Operational Control System
- Next Generation Overhead Persistent Infrared Space
- Next Generation Squad Weapons Fire Control Rapid Fielding (NGSW FC RF)
- Next Generation Squad Weapons Rapid Prototyping (NGSW RP)
- Next Generation Squad Weapons Weapons and Ammunition Rapid Fielding (NGSW W&A RF)
- Nuclear Biological Chemical Reconnaissance Vehicle Sensor Suite Upgrade (NBCRV SSU)
- Nuclear Planning and Execution System
- Offensive Anti-Surface Warfare Increment 1 (Long Range Anti-Ship Missile)

DOT&E Oversight List as of September 30, 2023

- Offensive Anti-Surface Warfare, Increment 2 (Air and Surface Launch)
- Over The Horizon Weapon System
- Paladin/FASSV Integrated Management (PIM)
- Patriot Advanced Capability 3
- Precision Strike Missile (PrSM)
- Presidential and National Voice Conferencing Integrator
- Proliferated Warfighter Satellite Architecture Tranche 1 Transport Layer
- Protected Tactical Enterprise Service
- Protected Tactical SATCOM
- Public Key Infrastructure (PKI) Inc. 2
- Robotic Combat Vehicle-Light (RCV-(L))
- SBIRS - Space-Based Infrared System Program
- Sentinel A4 Mod (Sentinel A4 Mod)
- SF - Space Fence
- Ship Self Defense System (SSDS)
- Ship to Shore Connector
- Small Diameter Bomb Increment II
- Small Unmanned Undersea Vehicle - LIONFISH
- Space Based Infrared System (SBIRS) Survivable and Endurable Evolution (S2E2)
- Space Command and Control
- Stand In Attack Weapon
- Standard Missile 2 (SM-2) including all mods
- Standard Missile-6 Including all mods and variants
- Strategic Mission Planning and Execution System
- Stryker Family of Vehicles
- Submarine Torpedo Defense System (Sub TDS) including Next Generation Countermeasure System (NGCM)
- Surface Electronic Warfare Improvement Program AN/SLQ-32C(V)6
- Surface Electronic Warfare Improvement Program Block 2
- Surface Electronic Warfare Improvement Program Block 3
- Surface Mine Countermeasures Unmanned Undersea Vehicle (SMCM UUV)
- Surface Navy Laser Weapon System
- Survivable Airborne Operations Center E-4B Recap
- Synthetic Training Environment - Live Training Systems (STE-LTS)
- T-7 Advanced Pilot Training
- Tactical Intelligence Targeting Access Node
- Tactical Tomahawk Modernization and Enhanced Tactical Tomahawk (Maritime Strike) (includes changes to planning and weapon control system)
- T-AO 205 John Lewis Class Fleet Replenishment Oiler
- Teleport, Generation III
- Terrain Shaping Obstacles (TSO)
- Terrestrial Layer System Brigade Combat Team (TLS - BCT)
- Terrestrial Layer System Echelons Above Brigade (TLS - EAB)
- Theater Medical Information Program - Joint Increment 2
- Three-Dimensional Expeditionary Long-Range Radar
- Torso & Extremity Protection (TEP)
- Tranche 1 Tracking Layer
- Tranche 2 Enterprise
- Trident II (D-5) Sea-Launched Ballistic Missile
- UH-60V Black Hawk Digital Cockpit
- Unified Network Operations (UNO)
- Uniform Integrated Protection Ensemble Family of Systems General Purpose (UIPE FoS GP)
- Unmanned Influence Sweep System (UISS) include Unmanned Surface Vessel (USV) and Unmanned Surface Sweep System (US3)
- Upgraded Early Warning Radar
- VC-25B

- VH-92A Presidential Helicopter
- VIRGINIA Class SSN 774 and associated PARMS
- Vital Torso Protection (VTP)
- Weather Satellite Follow-on (WSF)
- Wideband Communications Services
- XM1170 30x173mm Armor Piercing, Fin Stabilized, Discarding Sabot with Trace
- XM1176 40mm High Velocity (HV) High Explosive Dual Purpose Air Burst (HEDP-AB) (40mm HEDP-AB)
- XM1182 30x173mm High Explosive Air Burst with Trace (HEAB-T) (XM1182 HEAB-T)
- XM30 Combat Vehicle (XM30)

DOT&E Activities

This page intentionally left blank.

Table 1. FY23 DOT&E Independent System Evaluation Reports

Program	Date
Early Fielding Reports (EFRs)	
DDG 1000 *Zumwalt*-Class Destroyer EFR	October 2022
Abrams M1A2 SEPv3 with TROPHY Active Protection System EFR	March 2023
Offensive Anti-Surface Warfare (OAsuW) Increment 1, Long Range Anti-Ship Missile (LRASM) 1.1 EFR	April 2023
CVN 78 *Ford*-Class Aircraft Carrier EFR	April 2023
MQ-4C Triton EFR	August 2023
F/A-18 E/F System Configuration Set H18 EFR	August 2023
F/A-18E/F and EA-18G System Configuration Set H16 Version 4.0.4 EFR	September 2023
Follow-on Operational Test and Evaluation (FOT&E) Reports	
AIM-120 SIP-3 Test Report	December 2022
F-22 R1 OFP Test Report	December 2022
VH-92A Patriot Presidential Helicopter Program FOT&E Report	January 2023
LHA 6 Flight 0 Amphibious Assault Ship FOT&E Report	February 2023
Mk 48 Mod 7 Heavyweight Torpedo with Advanced Processor Build 5+ Software FOT&E Report	August 2023
Initial Operational Test and Evaluation (IOT&E) Reports	
UH-60V Black Hawk IOT&E II Report	December 2022
120mm M1147 Advanced Multi-Purpose (AMP) Cartridge, High Explosive Multi-Purpose with Tracer Combined IOT&E and LFT&E Report	December 2022
CH-53K King Stallion Combined IOT&E and LFT&E Report	December 2022
Armored Multi-Purpose Vehicle (AMPV) Combined IOT&E and LFT&E Report	January 2023
Army Integrated Air and Missile Defense (AIAMD) IOT&E Report	March 2023
HH-60W Jolly Green II Combined IOT&E and LFT&E Report	March 2023
Mk 54 Mod 1 Lightweight Torpedo IOT&E Report	April 2023

Table 1. FY23 DOT&E Independent System Evaluation Reports, continued

Program	Date
Freedom-Variant Littoral Combat Ship with Increment 3 Surface Warfare Mission Package IOT&E Report Cyber Addendum	June 2023
Trident II (D5) Sea-Launched Ballistic Missile Life Extension Program IOT&E Report	July 2023
Standard Missile-3 Block IIA IOT&E Report	September 2023
Mounted Mission Command – Software Version 3.1 IOT&E Report	September 2023
Live Fire Test and Evaluation (LFT&E) Reports	
USS *Gerald R. Ford* (CVN 78) Full Ship Shock Trial Report	December 2022
AGM-158B Joint Air-to-Surface Standoff Missile – Extended Range Electronic Safe and Arm Fuze LFT&E Report	March 2023
Operational Assessment (OA) Reports	
Integrated Visual Augmentation System (IVAS) 1.0 Operational Demonstration Report	October 2022
Handheld, Manpack, and Small-Form Fit (HMS) Programs – Leader Radio and Manpack Soldier Touchpoint Report	November 2022
Dismounted Assured Positioning, Navigation, and Timing System (DAPS) Limited User Test Report	March 2023
FFG 62 *Constellation*-Class Frigate Early OA Report	March 2023
Aerosol and Vapor Chemical Agent Detector (AVCAD) OA Report	April 2023
Joint Biological Tactical Detection System (JBTDS) OA Report	July 2023
Operational Test and Evaluation (OT&E) Reports	
Public Key Infrastructure (PKI) Increment 2 Cyber Survivability Interim Annex	January 2023
Space Command and Control Warp Core Cyber Survivability Report	June 2023
Special Reports	
MH-139A Grey Wolf Observation Report	February 2023

Table 2. Other FY23 DOT&E Reports

Program/Topic	Date
Legislative Reports/Responses	
Integrated Visual Augmentation System (IVAS) Fiscal Year 2022 Special Interest Report (FY22 NDAA Section 115)	October 2022

Table 2. Other FY23 DOT&E Reports, continued

Program/Topic	Date
Certification of Appropriateness and Risk Assessment of Services' Planned Test Strategies for Approved Middle Tier of Acquisition (804) and Accelerated Acquisition Programs	March 2023
Development and Implementation of Digital Technologies for Survivability and Lethality Report and Brief (FY22 NDAA Section 223)	April 2023
Assessment of the DoD's and Services' Funding of Test Infrastructure, Assets, and Personnel to Support Agreed-Upon Test and Evaluation of Programs on the DOT&E Oversight List	June 2023
Missile Defense System Report	
FY22 Missile Defense System Annual Assessment	February 2023
Special Reports	
U.S. Africa Command Cyber Assessment Report	January 2023
U.S. Navy Cyber Assessment Report	February 2023
FY14-21 Observations on the Compromise of Cyber Credentials Report	April 2023
U.S. Central Command Cyber Assessment 2022 Report	June 2023
U.S. Africa Command Cyber Assessment Report	July 2023
Critical Vulnerabilities Associated with Commercial Cloud Access Findings Memorandum	July 2023
Vulnerabilities Associated with Active Directory Certificate Services Findings Memorandum	August 2023

Table 3. FY23 DOT&E-Approved Test and Evaluation Master Plans (TEMPs) and Test Strategy Documents (Live Fire test strategies marked with an *)

Program Document	LF
AIAMD SAMP Annual T&E Annex	
AIAMD Simplified Acquisition Management Plan (SAMP)	
Armed Overwatch TEMP	*
CATMS - HAF-230308-DGZK - Weather System Follow-on Microwave (WSF-M) TEMP	
COLUMBIA LFT&E Management Plan Rev. A	*
COLUMBIA SSBN 826 – TEMP Update	*
Dismounted Assured Positioning, Navigation, and Timing System (DAPS) TEMP	

Table 3. FY23 DOT&E-Approved Test and Evaluation Master Plans (TEMPs) and Test Strategy Documents, continued (Live Fire test strategies marked with an *)

Program Document	LF
F-15EX Program Strategy Document	
F-35 Block 4 Classified TEMP (CTEMP) Annex 2	
F-35 Block 4 TEMP Annex 2	
FA-18E/F and EA-18G System Configuration Set H18 TEMP	
HH-60W TEMP Update	*
Integrated Master Test Plan version 24.0	
Integrated Master Test Plan version 24.1 (IMTP v24.1)	
Integrated Master Test Plan version 25.0	
Joint TEMP (1902) for the MK 54 Mod 2 Advanced Lightweight Torpedo (ALWT)	*
MH-139A TEMP Update	*
Mine Countermeasures Unmanned Surface Vessel with Minehunt Payload (MCM USV + MH) TEMP	
MQ-4C TEMP Update	
National Background Investigation Services (NBIS) Evaluation Strategy	
Next Generation Squad Weapons TEMP	
Over-The-Horizon Weapon System (OTH-WS) Test and Evaluation Identification Number (TEIN) 1886 IOT&E TEMP	*
Slip-Sheet Update to TEMP Update for the Javelin Antitank Weapon System G-Model Missile and Light Weight Command Launch Unit (LW CLU)	
TEMP for Command Post Computing Environment (CPCE) and Tactical Server Infrastructure (TSI)	
TEMP for Mounted Mission Command - Software	
TEMP for the Abrams System Enhancement Package v4 (M1A2 SEPv4)	*
TEMP for the M88A3 Combat Recovery Vehicle	*
TEMP for the Sentinel AN/MPQ-64A4 System	
TEMP Supporting a Milestone C / LRIP Decision for the Joint Biological Tactical Detection System (JBTDS) Acquisition Category (ACAT) II	

Table 3. FY23 DOT&E-Approved Test and Evaluation Master Plans (TEMPs) and Test Strategy Documents, continued (Live Fire test strategies marked with an *)

Program Document	LF
TEMP Supporting a Milestone C Decision for the Aerosol and Vapor Chemical Agent Detector (AVCAD)	
Three-Dimensional Expeditionary Long-Range Radar (3DELRR) Test & Evaluation Strategy	
Tomahawk Weapon System TEMP, TEIN 251-4, Revision 1	

Table 4. FY23 DOT&E-Disapproved TEMPs and Test Strategy Documents

Program Document
F/A-18E/F and EA-18G System Configuration Set (SCS) H18 TEMP #1787, TAB 4

Table 5. FY23 DOT&E-Approved Test Plans

Program Document
AARGM-ER Cyber Test Plan
Adversarial Assessment (AA) test plan approval for the Space Based Infrared System (SBIRS) Survivable and Endurable Evolution (S2E2) program
Aegis ACB 16 and CEC Final Operational Test Plan (OTP)
Aegis Ashore Poland Missile Defense Complex Poland Cyber Survivability Test Plan Approval
Air and Missile Defense Radar (AMDR) Operational Assessment (OA) Test Plan
Armed Overwatch Alternate Test Plan (ATP)
Army Integrated Air and Missile Defense (AIAMD) Regression Testing
CANES Submarine version OT plan approval
Change Transmittal 1 to Initial Operational Test and Evaluation Test Plan for CH-53K Program
CMV-22B COMM Upgrade Follow-on Operational Test and Evaluation (FOT&E) Cyber Test Plan
CMV-22B Follow-On Operational Test and Evaluation Test Plan
Consolidated Afloat Networks and Enterprise Services (CANES) Cyber Survivability Test Plan

Table 5. FY23 DOT&E-Approved Test Plans, continued

Program Document
Cooperative Vulnerability and Penetration Assessment (CPVA) and Adversarial Assessment (AA) OTP for the Extended Range Guided Multiple Launch Rocket System (ER GMLRS)
CPVA OTP for the Stryker Double-V Hull Infantry Carrier Vehicle (ICVVA1) 30-millimeter (mm) Engineering Change Proposal (ECP)
CVPA and AA of Sea-Based X-Band Radar 4.2 Operational Test Plan Approval
CVPA OTP for the Stryker Nuclear, Biological, Chemical, and Radiological Reconnaissance Vehicle (NBCRV) Sensor Suite Upgrade (SSU)
CVPA Test Plan (TP) for the Mounted Mission Command - Software (MMC-S) Mounted Computing Environment (MCE)
CVPA TP approval for the Space Based Infrared System (SBIRS) Survivable and Endurable Evolution (S2E2) program
CVPA TP for the Dismounted Assured Position, Navigation, Timing (PNT) System (DAPS) Generation (GEN) 2
Cybersecurity Annex Presidential and National Voice Conferencing Multi-Service Operational Test and Evaluation (MOT&E) Plan
DDG 1000 Cyber Survivability Test Plan
Defense Enterprise Office Solution (DEOS) Impact Level 6 Cyber Survivability Operational Cyber Test Plan Annex A
Detailed Test Plan (DTP) for the Developmental Test/Operational Test (DT/OT) of the Stryker Nuclear, Biological, and Chemical Reconnaissance Vehicle (NBCRV) Sensor Suite Upgrade (SSU) Modification Work Order (MWO) System Level Testing, US Army Test and Evaluation Command (ATEC) Project Number 2021-DT-DPG-IAVNB-H9883, West Desert Test Center (WDTC) Document Number WDTC-CTD-DTP-053
DT/OT Operational Test Agency Test Plan for the Nuclear, Biological, and Chemical Reconnaissance Vehicle (NBCRV) Sensor Suite Upgrade (SSU) Vehicle Integrated Platform Enhanced Radiation (VIPER) and Mounted Enhanced Radiac Long-Range Imaging Network (MERLIN) Component Level Testing
E-2D Delta System Software Configuration-4 (DSSC-4) Data Collection Plan Extension
E-2D Delta System Software Configuration-4 FOT&E Test Plan
Eagle Passive Active Warning Survivability System (EPAWSS) Hardware-in-the-Loop (HITL) Test Plans
F-15 Eagle Passive Active Warning and Survivability System IOT&E Plan
F-15EX Test Plan Deviation
F-22 Raptor Release 3 (R3) Operational Flight Program (OFP) Force Development Evaluation (FDE) Test Plan
F-35 JSE Test Approval
Future Tactical Unmanned Aircraft System (FTUAS) Increment 1 CVPA Plan
FY22-23 F-35 OT Cyber Test Plan

Table 5. FY23 DOT&E-Approved Test Plans, continued

Program Document
HH-60W FOT&E Plan
Integrated Testing Data Collection Plan for CH-53K Secondary Missions
Joint Operational Medicine Information Systems (JOMIS) Medical Common Operating Picture (MedCOP) Operational Assessment Test Plan
Long Range Discrimination Radar IOT&E Plan Approval
MHS GENESIS RevX Test Plan
Mk 48 APB 5/5+ SWUB QRA Test Plan
MQ-4C IOT&E Plan
MQ-25 EOA Strategy Response Memo
Multi-Service Operational Test and Evaluation (MOT&E) Plan for Presidential and National Voice Conference Program
OTP for the Dismounted Assured Positioning, Navigation, and Timing System Limited User Test
OTP for the Family of Medium Tactical Vehicles (FMTV) A2 Follow-On Operational Test (FOT) 2023-FO-MSS-FMTVX-G9330
OTP for the Integrated Tactical Network Operational Demonstration (ITN OD) 2023-OD-MC-ITNIS-I1983
OTP for the Javelin Lightweight Command Launch Unit Limited User Test (Javelin LW CLU LUT) 2023-LU-MTD-JVCLU-H8132
OTP for the Javelin Lightweight Command Launch Unit Initial Operational Test (Javelin LW CLU IOT) 2023-OT-MTD-JVCLU-H8067
OTP for the Mounted Mission Command-Software
OTP for the Stryker Nuclear, Biological, and Chemical Reconnaissance Vehicle Sensor Suite Upgrade Limited User Test (NBCRV SSU CSD LUT) 2023
OTP for the Terrestrial Layer System - Brigade Combat Team Operational Demonstration
SDB II QRA Test Plan Change Letter
SEWIP Block 2 FOT&E (DDG 1000) Test Plan
Ship to Shore Connector (SSC) IOT&E Test Plan
Space C2 ATLAS OUE Test Plan
T-AO 205 IOT&E Test Plan

Table 5. FY23 DOT&E-Approved Test Plans, continued

Program Document
TAO-205 Cyber Survivability Test Plan
Tomahawk Weapon System (TWS) Follow-On Operational Test & Evaluation Test Plan
USS *Gerald R. Ford* OT-CS1-2 Land Based Cyber Test Plan
USS *Gerald R. Ford* Test Plan Revision 1 Approval Memo

Table 6. FY23 DOT&E-Disapproved Test Plans

Program Document
Missile Defense System (MDS) Campaign Cybersecurity Test Plan

Service Secretary Comments

This page intentionally left blank.

SECRETARY OF THE ARMY
WASHINGTON

08 JAN 2024

MEMORANDUM FOR Director, Operational Test and Evaluation, 1700 Defense Pentagon, Washington, DC 20301-1700

SUBJECT: Department of the Army Response to the Fiscal Year 2023 Director, Operational Test and Evaluation Annual Report

1. Thank you for the opportunity to respond to the Director, Operational Test and Evaluation (DOT&E) Fiscal Year 2023 Annual Report.

2. I appreciate the thoroughness of the report and the coordination between DOT&E and the Army. The Army acknowledges the importance of the oversight role of OSD activities. It is also imperative that the management and execution of test capabilities to address new technology challenges is best retained at the Service level, thereby appropriately aligning authority, responsibility, and resources. In general, this report accurately reflects the status of oversight programs in the Department of the Army with the following comments on the Distributed Common Ground System-Army (DCGS-A) Capability Drop 2 (CD2) article.

a. The Army is focused on data-driven decision making and supports DOT&E's recommendation to acquire automated data collection, reduction, and analysis capabilities, especially in support of high-priority network-related systems.

b. The Army disagrees with DOT&E assessment on the sufficiency of the data collected for DCGS-A CD2. The Army submits that the operational utility assessment in October 2022 was sufficient to support an evaluation of effectiveness, suitability, and survivability for a conditional material release.

3. We look forward to working with your office to ensure we continue to provide effective capabilities to our Soldiers in support of the Joint force. Thank you for your continued support of Army programs and our Soldiers.

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

This page intentionally left blank.

THE SECRETARY OF THE NAVY
WASHINGTON DC 20350-1000

January 22, 2024

MEMORANDUM FOR DIRECTOR, OPERATIONAL TEST AND EVALUATION

SUBJECT: Department of the Navy Comments on the Fiscal Year 2023 Director Operational Test & Evaluation Annual Report

Thank you for the extensive collaboration between your staff and mine over the past four months to create this report. I appreciate the effort to ensure Controlled Unclassified Information content was not published in the report. I find that this report provides a factual assessment of the Navy and Marine Corps systems covered in the report.

I look forward to continuing and strengthening the collaboration with the Services, Director, Operational Test & Evaluation, and Under Secretary of Defense Research & Engineering to develop and implement comprehensive Integrated Test and Evaluation policy and processes.

Carlos Del Toro

Copy to:
ASN (RD&A)
PCD/PMD ASN (RD&A)
DASN (RDT&E)

This page intentionally left blank.

SECRETARY OF THE AIR FORCE
WASHINGTON, DC

26 Jan 24

MEMORANDUM FOR THE DIRECTOR, OPERATIONAL TEST AND EVALUATION

SUBJECT: Department of the Air Force Response to Fiscal Year (FY) 2023 Director, Operational Test and Evaluation (DOT&E) Annual Report

I appreciate the opportunity to review the FY23 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.

I welcome the clear delineation of Air Force and Space Force programs in dedicated sections of the report. Moving forward, I would like to continue to work with you to ensure our joint activities remain effective and well characterized in congressional reporting.

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

This page intentionally left blank.

Index of Programs

This page intentionally left blank.

#

120mm Advanced Multi-Purpose (AMP) Cartridge, High Explosive Multi-Purpose with Tracer, M1147 83

A

Abrams M1A2 System Enhancement Package version 4 (SEPv4) Tank 85
Advanced Anti-Radiation Guided Missile – Extended Range (AARGM-ER). 145
AGM-183A Air-Launched Rapid Response Weapon (ARRW) 263
Aegis Modernization Program 148
Aerosol and Vapor Chemical Agent Detector (AVCAD) 29
AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM). 266
AIM-9X Block II Sidewinder. 152
Air and Missile Defense Radar (AMDR) / AN/SPY-6 154
Air Operations Center – Weapon System (AOC-WS) 268
AN/AQS-20X Minehunting Sonar and Tow Vehicle (all variants) 157
Armored Multi-Purpose Vehicle (AMPV). 88
Army Integrated Air & Missile Defense (AIAMD) 91

B

B-52 Radar Modernization Program (RMP) 272
B-52J Commercial Engine Replacement Program (CERP) 275

C

Center for Countermeasures (CCM) 345
CH-53K® King Stallion® 159
CMV-22B Joint Services Advanced Vertical Lift Aircraft – Osprey – Carrier Onboard Delivery 162
Consolidated Afloat Networks and Enterprise Services (CANES) 165
Conventional Prompt Strike (CPS). 168
Cooperative Engagement Capability (CEC). 172
CVN 78 *Gerald R. Ford*-Class Nuclear Aircraft Carrier 175
Cyber Assessment Program (CAP) 351

D

DDG 1000 *Zumwalt*-Class Destroyer 183
Defense Enterprise Accounting and Management System (DEAMS) 278
Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives 32
Dismounted Assured, Positioning, Navigation, and Timing System (DAPS). 94
Distributed Common Ground System – Army (DCGS-A) Capability Drop 2 (CD2) 97
Distributed Common Ground System – Navy (DCGS-N) 186
DoD Healthcare Management System Modernization (DHMSM®) 97
DOT&E Strategy Implementation Plan (I-Plan) 13
Dry Combat Submersible (DCS) 329

| E |

E-2D Advanced Hawkeye 189

| F |

F-15 Eagle Passive Active Warning and Survivability System (EPAWSS) 281
F-15EX Eagle II 284
F-16 Radar Modernization Program (RMP). 288
F-22A – Raptor Advanced Tactical Fighter Aircraft 291
F-35 Joint Strike Fighter (JSF) 40
F/A-18 Infrared Search and Track (IRST) Block II. 192
F/A-18E/F Super Hornet and EA-18G Growler 195
Family of Medium Tactical Vehicles A2 (FMTV A2). 100
FFG 62 *Constellation*-Class Guided-Missile Frigate 199

| G |

Global Command & Control System - Joint (GCCS-J) 56
Global Positioning System (GPS) Enterprise 317

| H |

HH-60W Jolly Green II 294

| I |

Infantry Squad Vehicle (ISV). 104
Integrated Personnel and Pay System – Army (IPPS-A) Increment 2 106
Integrated Tactical Network (ITN) 109
Integrated Visual Augmentation System (IVAS). 112
International Test and Evaluation Program (ITEP). 360

| J |

Javelin Antitank Missile System – Medium 115
Joint Air-to-Ground Missile (JAGM). 119
Joint Aircraft Survivability Program (JASP) 370
Joint Biological Tactical Detection System (JBTDS). 59
Joint Cyber Warfighting Architecture (JCWA) 62
Joint Operational Medicine Information Systems (JOMIS) 65
Joint Planning and Execution System (JPES) 68
Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) Program 376
Joint Test and Evaluation (JT&E). 389

| K |

KC-46A Pegasus. 297
Key Management Infrastructure (KMI) 71

L

LHA 6 Flight 0/Flight 1 Amphibious Assault Ship 202
Littoral Combat Ship (LCS) 205
Long Range Hypersonic Weapon (LRHW) – Dark Eagle 122
Long Range Unmanned Surface Vessel (LRUSV). 257

M

Massive Ordnance Penetrator (MOP) Modification 301
MH-139A Grey Wolf 303
Missile Defense System 331
Mk 48 Torpedo Modifications. 208
Mk 54 Lightweight Torpedo Upgrades Including the High Altitude Anti-Submarine Warfare Weapon Capability (HAAWC) 212
Mounted Mission Command – Software (MMC-S) 125
MQ-25 Stingray Carrier Based Unmanned Aerial System (CBUAS) 215
MQ-4C Triton. 218
MQ-8C Fire Scout 221

N

National Background Investigation Services (NBIS) 74
Next Generation Jammer Mid-Band (NGJ-MB) 224
Next Generation Squad Weapons (NGSW) Weapons and Ammunition (W&A) 129

O

Offensive Anti-Surface Warfare (OASuW) Increment 1 227

P

Public Key Infrastructure (PKI) Increment 2 77

S

Ship Self-Defense System (SSDS) Mk 2 Integrated Combat Systems. 230
Ship to Shore Connector (SSC). 234
Small Diameter Bomb Increment II (SDB II) 307
Soldier Protection System (SPS) 135
Space Command and Control System (Space C2) 323
Standard Missile 2 (SM-2) Block IIIC and Block IIICU 237
Surface Electronic Warfare Improvement Program (SEWIP) Block 2 240

T

T-7A Advanced Pilot Training (APT). 310
T-AO 205 *John Lewis*-Class Fleet Replenishment Oiler 243
Test and Evaluation Resources 21
Test and Evaluation Threat Resource Activity (TETRA). 395

Three-Dimensional Expeditionary Long-Range Radar (3DELRR) 313
Tomahawk Weapon System (TWS) 246
Trident II (D-5) Sea-Launched Ballistic Missile – Life Extension Program Variant. 249

U

UH-60V Black Hawk Digital Cockpit. 138

V

VH-92A® Patriot® Presidential Helicopter 251

This page intentionally left blank.

www.dote.osd.mil