Director, Operational Test and Evaluation

FY 2018 Annual Report

December 2018

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.

Robert F. Behler
Director

FY 2018 Annual Report

The freedom and security of our nation depends on the lethality and readiness of our military. Our warfighters must be prepared for combat, equipped with secure, credible weapon systems, and trained to employ those systems effectively and decisively. As the Director of Operational Test and Evaluation (DOT&E), I ensure that our weapon systems are systematically tested across a range of operational conditions that warfighters are likely to encounter in combat. Establishing combat credibility through realistic testing gives warfighters the confidence their weapons and equipment will work when they need them. I have been in this position for just over one year and, during this time, have informed 92 acquisition and 25 fielding decisions for the Department. When I was appointed to this position, I committed to increasing collaboration between DOT&E and other agencies within the defense community. Looking back, I have been most impressed with the "spirit of cooperation" between OSD and the military Services. With an attitude of teamwork, we are working towards the ability to field combat credible systems at the speed of relevance.

During the past year, my office collaborated with other OSD offices and the test and evaluation (T&E) community to increase combined approaches to testing programs. We worked with the OSD Director of Developmental T&E (DT&E) and the Services' Operational Test Agencies (OTAs) to develop streamlined guidance for Test and Evaluation Master Plans (TEMPs). We are constructing a risk assessment policy to determine the level of oversight that DOT&E will exercise for middle-tier and traditional acquisition programs. I reviewed the existing DOT&E oversight list and retained oversight of those capabilities that are most critical to our current and future national security needs. My goal in each case was to facilitate more rapid development and deployment of weapon systems without sacrificing the integrity or independence of the T&E community. Following this review, I established policy to clarify criteria to both place and remove a program on the oversight list.

Building on the work of the past year, my initiatives for this next year center on several key focus areas. Software-intensive systems and their cybersecurity implications remain a high priority. Collaborating with DT&E to conduct operational T&E (OT&E) earlier in the system development and acquisition process, adapting T&E for emergent technologies, improving our testing environments, and enhancing the workforce required to support T&E are other key focus areas.

SOFTWARE-INTENSIVE SYSTEMS AND CYBERSECURITY

Most of the capabilities of current weapon systems are defined by software. This trend will continue as more complex and capable software platforms and algorithms make their way into the battlespace. However, as more software is incorporated into weapon systems, their vulnerability to cyber-attacks increases. Also, the cyber-attack surface of our systems increases as they become more interconnected and interdependent. Therefore, it is important to evaluate both the performance and cybersecurity of software-intensive capabilities within systems of systems as these drive operational effectiveness, suitability, and survivability.

Effectiveness and Suitability

Software-intensive systems cannot rely solely on manual, platform-focused testing to evaluate performance. T&E strategies need to integrate accredited modeling and simulation (M&S) and automated testing of software wherever possible to achieve continuous evaluation of software code and system capabilities. M&S of systems allows greater platform testing across a variety of operational and threat scenarios. Also, accredited automated testing and M&S can overcome some of the limitations of manual testing by evaluating systems across multiple operational contexts faster than real-time processes.

Repeatable automated testing will reduce man-hours required for testing system changes and enable delivery of software at the speed of relevance. It will enable evaluating the effect system changes or failures have on the safety and capabilities of the warfighter. Repeatable automated testing will improve system sustainability and cost through early detection and resolution of deficiencies. To facilitate these improved software development considerations, the DOD should implement an iterative, incremental approach to acquisition and T&E, such as Development Security Operations (DevSecOps). During DevSecOps, stakeholders (i.e., system developers, acquirers, developmental and operational testers, cybersecurity experts, and warfighters) collaborate across the entire system lifecycle, from development and test to operations and sustainment.

Cybersecurity Survivability

Any data exchange with a software-intensive system opens avenues for cyber-attacks that could adversely affect the confidentiality, integrity, or availability of the data. Cyber is a challenging man-made domain that requires seamless integration of technology with the cyber warrior to identify and defeat cyber adversaries. My office continues to emphasize the need to test all systems having

data exchanges for the resilience to complete missions in a cyber-contested environment. Also, I will continue to help improve the cybersecurity of mission-critical networks and systems through our Congressionally mandated Cybersecurity Assessment Program.

It is important that programs continue to conduct Cooperative Vulnerability and Penetration Assessments and Adversarial Assessments to fully characterize the cybersecurity of weapon systems. To aid this effort, I am advocating for improved training for cyber warriors and the development and use of automated tools for cybersecurity T&E. These tools should include the ability to examine deployed network and system configurations and identify flaws in software code. My office will continue to explore and advocate for cyber vulnerability assessment technologies that expand cybersecurity test scope while reducing test time. Concurrently, we will advocate for personnel with the skills needed to apply these tools effectively.

Human-System Interaction (HSI)

As systems become increasingly software intensive, the warfighter continues to be the most critical component in accomplishing the mission. We depend on our warfighters to be adaptable and find ways to accomplish the mission even when the systems we field have deficiencies. However, weapon systems that are difficult to use or that increase operator workload could reduce mission effectiveness or cause physical harm. As recently as 2017, the Navy's Fleet Forces Command cited poor HSI as a key factor in two U.S. Navy ship accidents, including the loss of 17 sailors.

I plan to update existing DOT&E guidance to encourage credible, systematic evaluations of HSI, consistent with Fiscal Year (FY) 2019 National Defense Authorization Act (NDAA) Section 227, Human Factors Modeling and Simulation Activities. I will encourage programs to incorporate warfighter feedback into the full system lifecycle from development and testing to operations and sustainment. I will align operational test of HSI with modern industry and scientific standards.

CONDUCT OT&E EARLIER IN SYSTEM DEVELOPMENT

To deploy combat credible systems at the speed of relevance, I recommend a DevSecOps approach for software and the host hardware systems. This approach enables the OT&E community to engage with program managers early in system development to construct testable, operationally relevant requirements. I am encouraging the T&E community to adopt a combined testing approach in order to collect operationally relevant test data as early as possible during system development for both traditional and Middle Tier Acquisition (MTA) programs. Combined testing encourages developmental and operational testers to collaboratively plan and execute test events whenever possible to support their independent T&E goals and use resources efficiently. By performing operationally representative T&E early and often in the acquisition process, developers will identify performance shortfalls and cyber vulnerabilities when they are significantly cheaper and easier to fix.

Implementing a DevSecOps approach and combined T&E will be key to achieving the goals of the MTA approaches defined in FY16 NDAA Section 804. The overall goal of MTA is to expedite the development and fielding of capabilities to the warfighter. A combined test approach that incorporates the use of M&S is necessary to demonstrate and evaluate the performance of systems that pursue the MTA pathways. The operational demonstrations (OpsDemos) required by the NDAA provide programs the opportunity to establish combat credibility while keeping pace with rapid acquisition timelines. The size and scope of the OpsDemos should vary based upon the acceptable risk of the system to the mission and to the warfighter. The goal should continue to be delivering new capabilities rapidly without sacrificing performance of those capabilities that are most critical to the warfighters.

My office is working with the military Services to establish policy on OpsDemos that is tailorable to the speed and risk of the program. We have also initiated efforts to identify methods to tailor live fire test and evaluation (LFT&E) survivability and lethality assessment methods in support of MTA programs. The level of test for OpsDemos and LFT&E will vary in complexity and speed; from analysis of existing data primarily from prior test events, to an evaluation of a demonstration event, to a dedicated operational or live fire test. The level of test will be tailored to the program based on a risk analysis conducted by the lead OTA. I encourage all programs, middle tier and traditional, to use warfighter risk in determining the appropriate level of test.

ADAPTING T&E FOR EMERGENT TECHNOLOGIES

As we conduct OT&E earlier in system development, the accelerating pace of emergent technologies will challenge T&E in new ways. The DOD has placed a renewed emphasis on advancing the capabilities of weapon systems using a range of new technologies, including hypersonic capabilities, directed energy, autonomy and artificial intelligence, and quantum systems. The T&E community must be prepared to evaluate these new systems and characterize their operational performance across a range of potential concepts of operations. This will require improvements in T&E infrastructure, novel T&E methods, and new skills in our T&E workforce.

As these technologies are incorporated into weapon systems, I will provide guidance on how to evaluate their unique capabilities during operational testing. While new technologies may present challenges, T&E of some have been ongoing. For example, the

Department has developed, tested, and fielded systems incorporating autonomous functions for several decades. In accordance with DOD Directive 3000.09, *Autonomy in Weapon Systems*, DOT&E is developing OT&E standards for autonomy in weapon systems. As military Services develop operational employment concepts for these emerging technologies, DOT&E will provide guidance on considerations for adequate OT&E.

IMPROVING OUR TESTING ENVIRONMENTS

The closer our OT&E emulates the warfighters' combat environment, the better we can anticipate how the integrated warfighter system will perform. Creating operationally realistic conditions requires T&E infrastructure that can represent current and future capabilities. Often, existing T&E infrastructure provides limited replication of current threats or ineffective integration of currently fielded friendly capabilities. This problem is especially significant for threats to space systems. I witnessed this first-hand as I visited a number of our test ranges including the Pacific Missile Range Facility in Hawaii, Pacific Alaska Range Complex, White Sands Missile Range in New Mexico, Aberdeen Proving Ground in Maryland, and the Nevada Test and Training Range. These ranges were developed to test our systems against legacy threats, but are now inadequate to test against current and emerging threats.

Such shortfalls make it difficult to determine how systems will perform in the face of existing near-peer threats or in the context of integrated Joint Force or coalition operations. Fixing T&E infrastructure deficiencies and emulating a modern battlespace will require innovative approaches and a greater use of accredited M&S. My office continually works to improve the fidelity of OT&E and LFT&E M&S tools to enable virtual T&E of the effectiveness, suitability, lethality, and survivability of systems. Physical ranges and actual systems assure the evaluation of real-world effects during T&E, but can be limited in the variety of threats and capabilities or scale of operations. M&S mitigates some of these limitations, but must be continuously verified, validated, and accredited against real systems' and environmental performance data.

To overcome these challenges, programs must prioritize M&S validation early in development. Developers, acquirers, testers, and operators should fully understand the capabilities and limitations of any M&S. Early collaboration between all stakeholders and combined testing will support a more efficient and effective model-test-model process.

WORKFORCE

In addition to adequate evaluation tools and methodology, credible T&E requires the right personnel to plan, execute, and analyze the tests. As OTAs maintain a skilled workforce through relevant training opportunities, knowledge is needed for systems that incorporate emerging technologies. We will continue to enhance workforce readiness and proficiency by developing and delivering training to the OTAs that focuses on current and future T&E needs.

Additionally, I am working to recruit and retain the most skilled personnel within the DOD for cybersecurity. I am looking to incorporate expertise from outside the DOD, including making use of our connections with the National Laboratories, University-Affiliated Research Centers, and Federally Funded Research and Development Centers. Expanding these partnerships can help us achieve the correct technical talent mix even in a highly competitive environment. I am committed to working with the OTAs to develop solutions to these challenges.

CONCLUSION

Over the past year, I have been honored to be on the DOD team and support our warfighters. Through objectivity and independence, DOT&E will continue to evaluate the combat credibility of our weapon systems and equipment our men and women will use to accomplish the mission. As the authoritative source for DOD weapon systems' operational capabilities, I provide the unvarnished truth to DOD leaders and the Congress to ensure the taxpayers' investment in our nation's security is well spent. I look forward to continuing this important contribution to our national defense and stand ready to provide any additional information requested by members of the Congress or Congressional defense committees.

Robert F. Behler
Director

Contents

Navy Programs

Air Force Programs

Ballistic Missile Defense Programs

FY18 TABLE OF CONTENTS

DOT&E Activity and Oversight

DOT&E Activity and Oversight

FY18 Activity Summary

DOT&E activity for FY18 involved oversight of 232 programs, including 23 Major Automated Information Systems (MAIS). Oversight activity begins with the early acquisition milestones, continues through approval for full-rate production, and, in some instances, during full production until removed from the DOT&E oversight list.

Our review of test planning activities for FY18 included approval of 30 Test and Evaluation Master Plans (TEMPs) and 92 Operational Test Plans. DOT&E also disapproved the following Test Plan:

- Distributed Common Ground System – Army (DCGS-A) Capability Drop 1 (CD 1) Limited User Test (LUT)

In FY18, DOT&E prepared 22 reports for Congress and SECDEF: 2 Combined IOT&E/LFT&E Reports; 1 Cybersecurity report, 6 Early Fielding reports, 3 FOT&E reports, 5 IOT&E reports, 3 LFT&E reports, 1 special report, and the Ballistic Missile Defense System Annual Report. Additionally, DOT&E prepared 21 non-Congressional reports for DOD stakeholders: 5 Cybersecurity reports, 3 FOT&E reports, 2 IOT&E reports, 1 LFT&E report, 9 Operational Assessment (OA) reports, and 1 OT&E report. Some of these non-Congressional reports were submitted to Defense Acquisition Board (DAB) principals for consideration in DAB deliberations.

During FY18, DOT&E met with Service operational test agencies, program officials, private sector organizations, and academia; monitored test activities; and provided information to Congress, SECDEF, the Deputy Secretary of Defense, Service Secretaries, USD(A&S), DAB principals, and the DAB committees. DOT&E evaluations are informed in large part through active on-site participation in, and observation of, tests and test-related activities. In FY18, DOT&E's experts joined test-related activities on 227 local trips within the National Capital Region and 918 temporary duty assignment trips in support of the DOT&E mission.

Security considerations preclude identifying classified programs in this report. The objective, however, is to ensure operational effectiveness and suitability do not suffer due to extraordinary security constraints imposed on those programs.

TEST AND EVALUATION MASTER PLANS/STRATEGIES APPROVED (LF STRATEGIES MARKED WITH *)

Advanced Pilot Training (APT) Program TEMP

AN/BQQ-10(V) Sonar System Advanced Processing Build 2015 TEMP Number 908-8/9 Revision F

AN/SQQ-89A(V)15 Surface Ship Undersea Warfare 9 USW Combat System Program TEMP

Common Infrared Countermeasure System (CIRCM) Milestone C TEMP

C-130J Block Upgrade 8.1

DDG 1000 TEMP Revision E

Defense Agency Initiative (DAI) Increment 3 (Inc 3) TEMP

Defense Enterprise and Accounting Management System (DEAMS) Increment 1 TEMP

Defense Healthcare Management System Modernization (DHMSM) TEMP v. 2.0

Department of the Navy Large Aircraft Infrared Countermeasures (DON LAIRCM) Program TEMP Number 1755 Revision B

Dry Combat Submersible (DCS) TEMP Milestone C

F-15 Eagle Passive/Active Warning and Survivability System (EPAWSS) Milestone B TEMP Version 2.1

F-15C Infrared Search and Track (IRST) TEMP

Global Positioning System (GPS) Enterprise TEMP - Revision B

Improved Turbine Engine Program (ITEP) TEMP*

Indirect Fire Protection Capability (IFPC) Increment 2-I Milestone B TEMP Update*

Integrated Personnel and Pay System - Army (IPPS-A) Increment 2 Post Milestone B TEMP

Joint Air-to-Ground Missile (JAGM) Milestone C TEMP*

Joint Light Tactical Vehicle (JLTV) Annex D to Milestone C TEMP*

Joint Project Manager Information Systems (JPM-IS) Joint Warning and Reporting Network (JWARN) Increment 2 TEMP

Littoral Combat Ship (LCS) TEMP Number 1695 Revision B

Lower Tier Air and Missile Defense Sensor (LTAMDS) TEMP

Public Key Infrastructure (PKI) Spiral 4 TEMP Addendum

RQ-21A Blackjack TEMP No. 1719

Ship Self-Defense System (SSDS) TEMP Revision C

Spider Increment 1A (SI1A) Milestone C TEMP Change Memorandum*

Stryker Double-V Hull (DVH) A1 Engineering Change Proposal (ECP) TEMP*

Torpedo MK 48 Mod 7 Heavyweight Undersea Weapon Improvements Increment 1 Joint TEMP

UH-1N Replacement TEMP*

XM17/XM18 Modular Handgun System (MHS) TEMP Amendment*

OPERATIONAL TEST PLANS APPROVED

30 mm Family of Ammunition Live Fire Test and Evaluation (LFT&E) Test Plan (TP)

Abrams Full-Up System-Level (FUSL) Live Fire Detailed Test Plan (DTP)

Abrams System Enhancement Package Version 3, Engineering Change Proposal 1a (SEPv3 ECP1a) LFT&E Operational Test Agency Test Plan (OTA TP)

AC-130J Combat Systems Officer Workstation and Defensive System Upgrade Operational Assessment Test Plan (OATP)

Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI) AN/BQQ-10 Sonar System Advanced Processing Build 2015 Follow-on Operational Test and Evaluation (FOT&E) TP

Aegis Weapon System Advanced Capability Build-16 (ACB-16) Initial Operational Test and Evaluation (IOT&E) Cyber Survivability TP

ACB-16 SPY-1A Baseline 9.A2A Build 24 (Phase 0) (Cruiser) Operational Test and Evaluation Plan (OTEP)

Air Operation Center (AOC) 10.1.15 Force Development Evaluation (FDE), Appendix H, Cybersecurity Adversarial Assessment (AA) TP

AOC 10.1.15 FDE and Cooperative Vulnerability and Penetration Assessment (CVPA) TP

Amphibious Combat Vehicle (ACV) OATP

AN/BQQ-10(V) Operator-In-The-Loop Testing Integrated Test Data Collection Plan

Armored Multipurpose Vehicle (AMPV) Ballistic Hull (BH) OTA TP

AMPV CVPA TP

AMPV OTA TP

AMPV System-Level Test Phase 1 Live Fire OTA TP

Army Tactical Missile (ATACMS) System Modification (MOD) CVPA TP

ATACMS MOD OTA TP

ATACMS MOD OTA TP for AA

Autonomic Logistics Information System Software (ALIS) Version 3.0 Operational Cybersecurity Testing

Ballistic Missile Defense System (BMDS) Integrated Master Test Plan (IMTP) and Annex

BMDS IMTP Version 19.1

BMDS IMTP v19.1 Annex

Bold Quest 17-2 (BQ 17-2) Final Assessment Plan

Bradley Fighting Vehicle (BFV) A4 Engineering Change Proposal (ECP) Live Fire DTP

C-130J BU 8.1 TP

Coastal Battlefield Reconnaissance and Analysis (COBRA) Block I Cybersecurity IOT&E

COBRA Block I IOT&E Plan, Change 1

Command Post Computing Environment (CPCE) CVPA TP

Defense Agencies Initiative (DAI) Increment 2 FOT&E and Cybersecurity Annex

Defense Enterprise Accounting and Management System (DEAMS) Operational Utility Evaluation (OUE) Plan Update

Distributed Common Ground System – Army (DCGS-A) Capability Drop 1 (CD 1) Limited User Test (LUT)

DOD Healthcare Management System Modernization (DHMSM) Operational Cybersecurity TP Annex

Enhanced Polar System (EPS) Cyberspace AA Plan

EPS Multi-Service OTEP

F-35 Joint Strike Fighter (JSF) Pre-IOT&E Cold Weather Deployment Test Planning

F-35 JSF Mission Data Optimization (MDO) TP

F-35 JSF Training Systems Cybersecurity OTP: AA Plan for Operating Environments

Global Command and Control System - Joint (GCCS-J) v6.0.1.0 OTP

Global Positioning System (GPS) Block 0 Integrated Cyber Test Plan

Ground/Air Task Oriented Radar (G/ATOR) Block 1 OTP

G/ATOR Block 2 OATP

HH-60G Distributed Aperture Infrared Countermeasures (DAIRCM) System FDE TP

Integrated Head Protection System (IHPS) Expanded DTP

IHPS Live Fire Testing OTA TP

IHPS Lot Acceptance Test (LAT) TP

Integrated Strategic Planning Analysis (ISPAN) Increment 4 Mission Planning and Analysis (MPAS) OTP

ISPAN Increment 4 OTP

JLF Air T-16-01, V-22 Wing Fire Protection System (FPS) Effectiveness TP

Joint Air-To-Ground Missile (JAGM) LUT OTA TP

JAGM Cybersecurity AA OTA TP

Joint Assault Bridge (JAB) LFT&E OTA TP

Joint Light Tactical Vehicle (JLTV) OTA TP

Joint Operations Planning and Execution System (JOPES) Version (v) 4.2.0.4 Operational Test Cybersecurity TP Annex

Joint Precision Approach and Landing System (JPALS) OATP

Joint Regional Security Stack (JRSS) 1.5 OA Plan

Joint Warning and Reporting Network (JWARN) 2 IOT&E Plan

Key Management Infrastructure (KMI) Capability Increment (CI)-2 FOT&E Cybersecurity Plan

KMI CI-2 FOT&E Plan

Littoral Combat Ship (LCS) *Freedom* Variant with Surface Warfare Mission Package Increment III IOT&E TP

M109 Family of Vehicles Initial Operational Test 2 OTA TP

M109A7 Family of Vehicles (FoV) AA OTA TP

MK 48 Mod 7 Common Broadband Advanced Sonar System Torpedo with Advanced Processor Build 5 Software FOT&E TP

MQ-1C Extended Range Gray Eagle Unmanned Aircraft System (UAS) FOT&E 2 OTA TP

MQ-4C Triton Unmanned Aerial System OTAP (1731-OT-C1)

P-8A Multistatic Active Coherent (MAC) TP

P-8A Poseidon Multi-Mission Maritime Aircraft FOT&E Plan (1813-OT-D4)

Public Key Infrastructure (PKI) Increment 2 Operational Assessment (OA) and FOT&E Plan

RQ-4B Block 30 Multi-Spectral Intelligence OUE Plan

Small Diameter Bomb II (SDB II) Multi-Service Operational Test & Evaluation (MOT&E) Phase 1 TP

Soldier Protection System (SPS) Live Fire Test, Blast Overpressure Testing of the Integrated Head Protection System (IHPS) DTP

SPS Live Fire Test, Torso and Extremity Protection (TEP) Full-Up System-Level (FUSL) Test Deviation

Spider M7E1, Dispensing Set, Munition, Network Command 1A OTA TP

Stryker Double-V Hull (DVH) A1 ECP CVPA TP

Stryker DVH A1 ECP FOT&E OTA TP

Stryker Infantry Carrier Vehicle Dragoon (ICVD) Early User Test (EUT) and Common Remotely Operated Weapon Station - Javelin (CROWS-J) AA OTA TP

Stryker ICVD Updates to Live Fire Test Program

Stryker ICVD 30mm and CROWS-J EUT OTA TP

System Configuration Set H14 for the F/A-18E/F and EA-18G FOT&E Plan

TEIN 1593 MQ-8C Fire Scout UAS Endurance Baseline TP

Teleport G3P3 OT&E Plan

Terminal High-Altitude Area Defense (THAAD) System Cybersecurity Assessment Plan

The Missile Defense Agency (MDA) CVPA TP for the Command and Control, Battle Management, and Communications (C2BMC) Spiral 8.2-3 and the Ballistic Missile Defense System (BMDS) Overhead Persistent Infrared (OPIR) Architecture (BOA) 6.1

TRIDENT II D5 Demonstration and Shakedown Operations - 28 (DASO-28) Flight Test Support Plan for OT&E

TRIDENT II D5 Life Extension (LE) Commander Evaluation Test-1 (CET-1) Flight Test Support Plan for OT&E

UH-60V BLACK HAWK Helicopter CVPA OTA TP

UH-60V BLACK HAWK LUT OTA TP

United States Indo-Pacific Command, Pacific Sentry 2018-3 Final Capstone Event Plan

United States Strategic Command (USSTRATCOM) Global Thunder 2018 (GT18) Capstone Event Plan

Unmanned Influence Sweep System (UISS) Operational Assessment (OT-B1) Test Plan

USS *Iwo Jima* Amphibious Ready Group (ARG) Composite Training Unit Exercise (C2X) Cybersecurity Assessment Plan

USSOUTHCOM Exercise PANAMAX 2018 Assessment Plan

VH-92A OATP

Vigilant Shield 18 Final Capstone Event Plan

TABLE 1. FY18 REPORTS TO CONGRESS	
PROGRAM	**DATE**
Combined Initial Operational Test and Evaluation and Live Fire Test and Evaluation Report	
Expeditionary Sea Base (T-ESB)	October 2017
M57E1 Army Tactical Missile System (ATACMS) Modification (MOD)	September 2018
Cybersecurity Report	
Defensive Cyberspace Operations: Findings from Department of Defense (DOD) Operational Tests and Assessments in Fiscal Year 2014 through Fiscal Year 2016	October 2017
Early Fielding Reports	
LHA 6 Amphibious Assault Ship	November 2017
Ship Self-Defense of LSD 41/49-Class Ships Equipped with the Ship Self-Defense System MK 2 Mod 5	November 2017
Massive Ordnance Penetrator (MOP)	November 2017
Ground/Air Task Oriented Radar (G/ATOR)	February 2018
Surface Ship Torpedo Defense (SSTD) System: Torpedo Warning System (TWS) and Countermeasure Anti-Torpedo (CAT)	April 2018
Offensive Anti-Surface Warfare (OASuW) Increment 1 Long Range Anti-Ship Missile (LRASM)	September 2018
Follow-on Operational Test and Evaluation Reports	
Advanced Processing Build 2013 (APB-13) Version of the AN/BQQ-10(V) Acoustic Rapid Commercial Off-the-Shelf (A-RCI) Sonar System	June 2018
Standard Missile-6 (SM-6) Block 1	August 2018
P-8A Poseidon Multi-Mission Maritime Aircraft Engineering Change Proposal (ECP) 2	August 2018
Initial Operational Test and Evaluation Report	
PATRIOT PAC-3 - Patriot Advanced Capability 3 Post-Deployment Build 8 (PDB-8)	April 2018
AC-130J	April 2018
Next Generation Diagnostic System Increment 1 (NGDS Inc 1)	May 2018
Paladin Integrated Management (PIM) Family of Vehicles with classified Annex	July 2018
Rolling Airframe Missile (RAM) Block 2	September 2018
Live Fire Test and Evaluation Reports	
Soldier Protection System (SPS) Vital Torso Protection (VTP)	April 2018
Soldier Protection System (SPS) Integrated Head Protection System (IHPS)	May 2018
M109A7 Family of Vehicles	June 2018
Special Report	
Army Tactical Network Modernization Strategy Assessment	April 2018
Ballistic Missile Defense System Report	
FY17 Assessment of the Ballistic Missile Defense System	February 2018

TABLE 2. OTHER FY18 REPORTS (NOT SENT TO CONGRESS)	
PROGRAM	**DATE**
Cybersecurity Reports	
Austere Challenge 2017 United States European Command	November 2017
2016 and 2017 Cybersecurity Assessment of U.S. Pacific Command	February 2018
2018 Cybersecurity Assessment of North American Aerospace Defense (NORAD) and U.S. Northern Command (NORTHCOM)	March 2018
2018 Cybersecurity Assessment of U.S. Strategic Command	April 2018
Cybersecurity Assessment for USS *Iwo Jima* Amphibious Readiness Group (ARG)	June 2018
Follow-On Operational Test and Evaluation Reports	
Warfighter Information Network - Tactical (WIN-T) Increment 2 Network Operations Security Center - Lite, Tactical Communication Node - Lite with classified Annex	November 2017
Public Key Infrastructure (PKI) Increment 2 Spiral 3	December 2017
Navy Multiband Terminal Program (NMT) with classified Annex	January 2018
Initial Operational Test and Evaluation Reports	
Mission Planning Systems (MPS) Increment (Inc) 5 C-17 Joint Mission Planning System (JMPS)	December 2017
Military Healthcare System (MHS) Genesis	April 2018
Live Fire Test and Evaluation Report	
Javelin Spiral 2 Interim LFT&E Report	October 2017
Operational Assessment Reports	
Assault Amphibious Vehicle - Survivability Upgrade (AAV-SU) with classified Annex	October 2017
DOD Healthcare Management System Modernization (DHMSM)	January 2018
Department of Navy Large Aircraft Infrared Countermeasures (DON LAIRCM) Advanced Threat Warner (ATW) MV-22 Installation	February 2018
Joint Regional Security Stack (JRSS)	March 2018
Key Management Infrastructure (KMI) Capability Increment 2, Spiral 2 Spin 3	March 2018
Joint Air-to-Ground Missile (JAGM)	April 2018
Amphibious Combat Vehicle Phase 1 Increment 1 (ACV 1.1) with classified appendices	June 2018
Joint Warning and Reporting Network (JWARN) Increment 2	August 2018
Common Infrared Countermeasures (CIRCM)	September 2018
Operational Test and Evaluation Report	
Air Force Distributed Common Ground System (AF-DCGS)	February 2018

Program Oversight

DOT&E is responsible for approving the adequacy of plans for operational test and evaluation and for reporting the operational test results for all Major Defense Acquisition Programs (MDAPs) to the Congress, SECDEF, Service Secretaries, Under Secretary of Defense for Research and Engineering, and the Under Secretary of Defense for Acquisition and Sustainment. Any program that meets the criteria established in section 2430 of title 10, United States Code (10 USC 2430) is considered an MDAP. DOT&E may designate any other programs as MDAPs for the purpose of test and evaluation oversight, review, and reporting in accordance with 10 USC 139(a)(2)(B). DOT&E was responsible for overseeing the OT&E of 232 acquisition programs during FY18.

DOT&E simplified its criteria for testing oversight in FY18. DOT&E selects a program for OT&E oversight if it meets one or more of the following criteria:

- Program exceeds or has the potential to exceed the dollar value threshold for a major program, to include MDAPs, designated major subprograms, as well as highly classified programs and pre-MDAPs.
- Program has a high level of Congressional or DOD interest.
- Weapons, equipment, or munitions that provide or enable a critical mission warfighting capability or is a militarily significant change to a weapon system.

DOT&E is also responsible for the oversight of LFT&E of programs, in accordance with 10 USC 139. The DOD uses the term "covered system" to include all categories of systems or programs identified in 10 USC 2366 as requiring LFT&E. In addition, systems or programs that do not have acquisition points referenced in 10 USC 2366, but otherwise meet the statutory criteria, are considered covered systems for the purpose of DOT&E oversight. DOT&E was responsible for overseeing the LFT&E of 84 acquisition programs during FY18.

DOT&E determined a covered system, for the purpose of LFT&E oversight, meets one or more of the following criteria.

- A major system, as defined in 10 USC 2302(5), that is:
  - User-occupied and designed to provide some degree of protection to the system or its occupants in combat
  - A conventional munitions program or missile program
- A conventional munitions program for which more than 1 million rounds are planned to be acquired.
- A modification to a covered system that is likely to affect significantly the survivability or lethality of such a system.

DOD PROGRAMS

5th Generation Aerial Target

AC-130J High Energy Laser & Tactical Offboard Sensing

Ballistic Missile Defense System Program (BMDS)

Chemical Demilitarization Program - Assembled Chemical Weapons Alternatives (CHEM DEMIL-ACWA)

Defense Agency Initiative (DAI)

Defense Enterprise Accounting and Management System - Increment 1 (DEAMS - Inc. 1)

Defense Medical Information Exchange (DMIX)

Defense Security Assistance Management System (DSAMS) - Block 3

DoD Healthcare Management System Modernization (DHMSM)

Explosive Destruction System (EDS)

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

Joint Aerial Layer Network

Joint Biological Tactical Detection System

Joint Information Environment

Joint Light Tactical Vehicle Family of Vehicles

Joint Operational Medicine Information Systems

Joint Regional Security Stack (JRSS)

Joint Warning and Reporting Network (JWARN)

Key Management Infrastructure (KMI)

Long-Range Discrimination Radar

milCloud

Mission Partner Environment - Information System

Multi-Functional Information Distribution System (includes integration into USAF & USN aircraft)

Public Key Infrastructure (PKI) Incr 2

SOCOM Dry Combat Submersible Medium (DCSM)

Teleport, Generation III

Theater Medical Information Program - Joint (TMIP-J) Block 2

ARMY PROGRAMS

120MM Advanced Multi-Purpose (AMP), XM1147
3rd Generation Improved Forward Looking Infrared (3rd Gen FLIR)
Abrams M1A1 SA; M1A2 SEP; APS
Advanced Field Artillery Tactical Data System (AFATDS) Version 7
Advanced Threat Detection System
Aerosol and Vapor Chemical Agent Detector
AH-64E Apache Remanufacture/New Build
AN/TPQ-53 Radar System (Q-53)
Armored Multipurpose Vehicle (AMPV)
Armored Truck - Heavy Equipment Transporter (HET)
Army Contract Writing System
Army Integrated Air & Missile Defense (AIAMD)
Army Tactical Missile System-Modernization
Assured - Positioning, Navigation, & Timing (Assured - PNT)
Biometrics Enabling Capability (BEC) Increment 1
Biometrics Enabling Capability Increment 0
Black HAWK (UH-60M) - Utility Helicopter Program
Bradley ECP; MOD; APS
Cannon Delivered Area Effects Munitions (C-DAEM) Family of Munitions
CH-47F Block II Chinook
Command Post Computing Environment (CPCE)
Common Infrared Countermeasures (CIRCM)
Distributed Common Ground System - Army (DCGS-A)
Electronic Warfare Program Management Tool (EWPMT)
EXCALIBUR - Family of Precision, 155 mm Projectiles
Extended Range Cannon Artillery (ERCA)
Family of Medium Tactical Vehicles A2 (FMTV A2)
Future Unmanned Aircraft System
Future Vertical Lift Family of Systems (FVL FoS)
Gator Landmine Replacement Program (GLRP)
Global Combat Support System Army (GCSS-A)
Ground Mobility Vehicle 1.1 (GMV 1.1)
Guided Multiple Launch Rocket System Family of Munitions Including Alternative Warhead (AW); Unitary; Extended Range (ER)
HELLFIRE
High Mobility Artillery Rocket System (HIMARS)
Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs)
Improved High Explosive Dual Purpose 40 mm Cartridge
Improved Turbine Engine Program (ITEP)
Indirect Fire Protection Capability Increment 2 - Intercept (IFPC Inc 2-I)
Integrated Personnel and Pay System - Army (IPPS-A) Increment 2
Javelin Antitank Missile System - Medium
Joint Air-to-Ground Missile (JAGM)
Joint Assault Bridge (JAB)
Joint Battle Command Platform (JBC-P)
Joint Tactical Radio System, Handheld, Man pack, and Small Form Fit [Leader Radio]
Joint Tactical Radio System, Handheld, Man pack, and Small Form Fit [Manpack]
Limited Interim Missile Warning System
Logistics Modernization Program (LMP)
M270A1 Multiple Launch Rocket System (MLRS)
M88A2 Heavy Equipment Recovery Combat Utility Lift Evacuation System (Hercules)
Mobile / Handheld Computing Environment (M/HCE)
Mobile Protected Firepower Increment 1 (MPF Inc 1)
Modular Handgun System (XM17/XM18)
Mounted Computing Environment (MCE)
MQ-1C Unmanned Aircraft System Gray Eagle
Multi-Function Electronic Warfare (MFEW) Air Large
Near Real Time Identity Operations
Nett Warrior
Paladin/FASSV Integrated Management (PIM)
PATRIOT PAC-3 - Patriot Advanced Capability 3
Precision Guidance Kit Family of Fuzes
Precision Strike Missile (PrSM)
RQ-7B SHADOW - Tactical Unmanned Aircraft System
Soldier Protection System
Spider XM7 Network Command Munition
Stryker Family of Vehicles to include all variants
Stryker M1135 NBC Reconnaissance Vehicle (NBCRV) (to include Sensor Suite Upgrade and components)
UH-60V BLACK HAWK
WIN-T INCREMENT 2 - Warfighter Information Network - Tactical Increment 2
XM1158 7.62 mm Cartridge

NAVY PROGRAMS

Acoustic Rapid COTS Insertion for SONAR
Advanced Airborne Sensor
Advanced Arresting Gear
AEGIS Modernization (Baseline Upgrades)
AGM-88G Advanced Anti-Radiation Guided Missile Extended Range
AIM-9X - Air-to-Air Missile Upgrade Block II
Air and Missile Defense Radar (AMDR)
Air Warfare Ship Self Defense Enterprise

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

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

AN/SQQ-89A(V) Integrated USW Combat Systems Suite

Assault Breaching System Coastal Battlefield Reconnaissance and Analysis System (all variants)

Barracuda Mine Neutralization System

CANES - Consolidated Afloat Networks and Enterprise Services

Carrier Based Unmanned Air System

CH-53K - Heavy Lift Replacement Program

CMV-22 Joint Services Advanced Vertical Lift Aircraft - Osprey -- Carrier Onboard Delivery (COD)

Columbia-Class SSBN - including all supporting PARMs

Cooperative Engagement Capability (CEC)

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

DDG 1000 - *Zumwalt*-Class Destroyer - includes all supporting PARMs and the lethality of the LRLAP and 30 mm ammunition

DDG 51 Flight III and associated PARMS

Distributed Common Ground System - Navy (DCGS-N)

E-2D Advanced Hawkeye

Electro-Magnetic Aircraft Launching System

Enterprise Air Surveillance Radar

Evolved Sea Sparrow Missile Block 2

F/A-18E/F - SUPER HORNET Naval Strike Fighter

Frigate-Class Small Surface Combatant

Future Pay and Personnel Management Solution (FPPS)

Ground/Air Task Oriented Radar (G/ATOR)

Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs)

Infrared Search and Track System

Joint Precision Approach and Landing System

LHA 6 - *America Class* - Amphibious Assault Ship - includes all supporting PARMs

LHA 8 Amphibious Assault Ship (*America*-Class with well deck)

Light Armored Vehicle

Littoral Combat Ship (LCS) Seaframes both variants; *Freedom* and *Independence* and 57 mm and OTH ammunition lethality

Littoral Combat Ship (LCS) Anti-submarine Warfare (ASW) Mission Package to include all associated vehicles, communications, sensors, weapon systems, support equipment, software, & support aircraft that are in development

Littoral Combat Ship (LCS) Mine-countermeasures (MCM) Mission Package to include all associated vehicles, communications, sensors, weapon systems, support equipment, software, and support aircraft that are in development

Littoral Combat Ship Surface Warfare (SUW) Mission Package to include all associated vehicles, communications, sensors, weapon systems, support equipment, software, & support aircraft in development, 30 mm, SSMM/Longbow HELLFIRE/ammunition lethality

LSD 41/49 Replacement

MK 54 torpedo/MK - 54 VLA/MK 54 Upgrades Including High Altitude ASW Weapon Capability (HAAWC)

MK 48 CBASS Torpedo including all upgrades

Mobile User Objective System (MUOS)

MQ-4C Triton

MQ-8 Fire Scout Unmanned Aircraft System

Multi-static Active Coherent (MAC) System

MV-22 Joint Services Advanced Vertical Lift Aircraft - Osprey

Naval Integrated Fire Control - Counter Air (NIFC-CA) From the Air

Navy Expendable Airborne Electronic Attack (EA2)

Navy Multiband Terminal Program (NMT)

Next Generation Jammer - Increment 1 (Mid-Band)

Next Generation Jammer - Increment 2 (Low Band)

Next Generation Land Attack Weapon

Offensive Anti-Surface Warfare Increment 1

Offensive Anti-Surface Warfare, Increment 2 (Air and Surface Launch)

Over The Horizon Weapon System

Rolling Airframe Missile Block 2 Program

RQ-21A Unmanned Aircraft System (UAS)

Ship Self-Defense System (SSDS)

Ship to Shore Connector

Standard Missile 2 (SM-2) including all mods

Standard Missile-6 (SM-6)

Submarine Torpedo Defense System (Sub TDS) including Next Generation Countermeasure System (NGCM)

Surface Electronic Warfare Improvement Program Block 2

Surface Electronic Warfare Improvement Program Block 3

Surface Mine Countermeasures Unmanned Undersea Vehicle (also called Knifefish UUV) (SMCM UUV)

Tactical Tomahawk Modernization and Enhanced Tactical Tomahawk (Maritime Strike) (includes changes to planning and weapon control system)

T-AO 205 Oiler

TRIDENT II MISSILE - Sea Launched Ballistic Missile

Unmanned Influence Sweep System (UISS) include Unmanned Surface Vessel (USV) and Unmanned Surface Sweep System (US3)

USMC MRAP-Cougar

USSOCOM JUONS- Navy and USAF Development/Integration of the Distributed Aperture Infrared Countermeasure System on the USAF HH-60G, Army A/MH-6, Navy MH-60S, AH-1Z, UH-1Y

VH-92A Presidential Helicopter

Virginia-Class SSN (all variants)

AIR FORCE PROGRAMS

Advanced Pilot Trainer

AEHF - Advanced Extremely High Frequency (AEHF) Satellite Program

AIM-120 Advanced Medium-Range Air-to-Air Missile

Air Force Integrated Personnel and Pay System (AF-IPPS)

Air Force Organic Depot Maintenance, Repair and Overhaul Initiative (MROi)

Air Operations Center - Weapon System (AOC-WS) 10.1

Air-Launched Rapid Response Weapon

B-2 Defensive Management System Modernization (DMS-M)

B-21 Long Range Strike Bomber

B-52 Commercial Engine Replacement Program (CERP)

B-52 Radar Modernization Program (RMP)

B61 Mod 12 Life Extension Program

C-130J - HERCULES Cargo Aircraft Program

Combat Rescue Helicopter (CRH)

Command and Control Air Operations Suite (C2AOS)/Command and Control Information Services (C2IS) (Follow-on to Theater Battle Management Core System, new capabilities for AOC and joint software suites)

Deliberate and Crisis Action Planning and Execution Segments (DCAPES) Inc. 2B

Enhanced Polar System (EPS)

Evolved Strategic Satellite Communications

F-15 Eagle Passive Active Warning Survivability System

F-15C Infrared Search and Track (IRST)

F-16 Radar Modernization Program

F-22 - RAPTOR Advanced Tactical Fighter

F-35 - Lightning II Joint Strike Fighter (JSF) Program

FAB-T - Family of beyond Line-of-Sight Terminals

GBS - Global Broadcast Service

Geosynchronous Space Situational Awareness Program

Global Positioning System (GPS) Enterprise Oversight

Global Positioning System (GPS) III Space Vehicle

Global Positioning System (GPS) Next Generation Operational Control System

Ground Based Strategic Deterrent

Hypersonic Conventional Strike Weapon

Identification Friend or Foe Mark XIIA Mode 5 (all development and integration programs)

Integrated Strategic Planning and Analysis Network (ISPAN) Increment 4

Integrated Strategic Planning and Analysis Network Increment 5

Joint Air-to-Surface Standoff Missile Electronic Safe Arm and Fuze

Joint Space Operations Center Mission System (JMS)

Joint Surveillance Target Attack Radar System (JSTARS) Recapitalization (Recap)

KC-46 - Tanker Replacement Program

Light Attack Aircraft

Long Range Stand Off (LRSO) Cruise Missile

Massive Ordnance Penetrator (MOP)

Military Global Positioning System (GPS) User Equipment

Military Personnel Data System

Next Generation Overhead Persistent Infrared

Nuclear Planning and Execution System

Presidential National Voice Conferencing

Protected Tactical Enterprise Service

Protected Tactical Satellite Communications (SATCOM)

RQ-4 Global Hawk Unmanned Aircraft System Multi-Spectrum-177 Sensor

Small Diameter Bomb, Increment II

Space Based Infrared System Program (SBIRS)

Space Based Infrared System Mobile Ground Terminal

Space Fence (SF)

Stand In Attack Weapon (SiAW)

Three-Dimensional Expeditionary Long-Range Radar (3DELRR)

UH-1N Replacement

VC-25B Presidential Aircraft

Weather Satellite Follow-on (WSF)

Wide Area Surveillance (WAS) Program

DOD Programs

DOD Programs

International Test and Evaluation (IT&E) Program

DOT&E, under the authority of section 2350(1), title 10, U.S. Code in 2001, manages the International Test and Evaluation (IT&E) program for the DOD. This program directly aligns with the FY18 National Defense Strategy second Line of Effort – strengthen alliances and attract new partners. Since 2002, over 185 test projects have been executed under IT&E program bilateral and multinational agreements. These projects benefit the United States and our allied partners by enabling access to environments and facilities to achieve coalition and joint force operational realism; sharing T&E technologies, data, and costs; and standardizing test and analytical procedures. By engaging international partners, IT&E projects address warfighter needs in the expected operational environments and improve interoperability among coalition and joint forces. The IT&E bilateral and multilateral agreements allow for:

- Cooperative Test and Evaluation (CTE) Project Arrangements (PAs)
  - Each nation has an interest in a system's performance and agrees to share the test planning, conduct, data analysis, reporting, and costs on an equitable basis.
- Reciprocal Use of Test Facilities (RUTF) PAs
  - Use of another nation's test facilities on a "fee-for-service" and "cost-to-test" basis.
- Equipment and Material Transfer Agreements
  - Loan of one nation's test equipment and tools to another nation for testing.
- Working Groups
  - Data exchanges and discussions to develop PAs or address other mutual warfighter concerns.

PAs authorize U.S. and partner nation test organizations to conduct test planning, conduct, and data sharing. The PA identifies the systems being tested, the test location, and the test organizations and their responsibilities, including points of contact, estimated test dates, and financial, legal, and security arrangements.

CTE and RUTF PAs allow the use of test environments and test facilities that best represent the operational environment where the warfighter will use the system to accomplish the mission.

The RUTF PAs are not available under any other international agreement.

The United States has bilateral agreements with Australia, Canada, Denmark, Finland, France, Germany, Italy, the Netherlands, Norway, Sweden, and the United Kingdom. During FY18, IT&E bilateral discussions continued with two additional allied nations pursuant to developing two new bilateral agreements.

Built upon the success of past IT&E bilateral agreements, in 2015 DOT&E negotiated its first multinational T&E agreement among the defense establishments of the United States, Australia, Canada, New Zealand, and the United Kingdom. The Multinational Test and Evaluation Program (MTEP) leverages the goodwill, expertise, and experience of the bilateral agreements and accommodates changes in the evolving international security environment. It expands and simplifies T&E cooperation, beyond just one-on-one agreements, to the benefit of multiple international partners. The MTEP paves the way for the five participating nations to access ranges, test facilities, and natural environments in circumstances where they may not be available within a particular country. Test results and information of mutual interest is shared, thus the MTEP creates an efficient "test-once and use-by-all" T&E framework for participating nations.

The MTEP allows all five nations to test together, but also for testing to be developed bilaterally, or among three or four of the MTEP nations. Most testing is completed at the unclassified level, but may be conducted up to TOP SECRET when justified and properly approved. Considering budgetary issues, and the threat environment, the MTEP has become the "go-to" agreement for efficient testing of common interest systems that promote interoperability among participating partners.

The impetus for creating the MTEP was the need for open-air testing of aircraft survivability systems. This testing is technically complicated and requires specific natural environments. Alone, each of the participating nations could not fill all of the test environment requirements. The MTEP and its inherent "sharing" concept is also well suited for projects in other areas such as integrated tactical avionics systems; integrated air and missile defense (IAMD) systems; and chemical, biological, and radiological systems. As an example, MTEP provides the mechanism for Australia, Canada, the United Kingdom, and the United States to test aircraft survivability equipment together on a recurring basis in a common operating environment. Recent PAs reflect autonomous and robotic systems, and determining how to integrate these new technologies into joint systems and coalition operations.

The successful implementation of the MTEP provides a working model for more multinational agreements with other partner nations who share interest in expanding international cooperation that will enhance coalition warfare capabilities and mutual defense interests. In FY18, DOT&E initiated negotiation on a multinational Trans-Atlantic MTEP among France, Germany, Italy, the United Kingdom, and the United States. Additional Trans-Atlantic countries may be added by amendment following the implementation of this agreement. Table 1 identifies the existing bilateral and multinational IT&E agreements.

TABLE 1. BILATERAL AND MULTINATIONAL IT&E AGREEMENTS

PARTNER COUNTRY	BEGIN DATE
Italy	2017 (December)
Sweden	2017 (June)
Denmark	2017 (March)
Finland	2017 (January)
Germany	2017 (January)
Norway	2014 (December)
United Kingdom	2006 (November)
Netherlands	2004 (February)
Australia	2003 (April)
France	2003 (January)
Canada	2002 (September)
Australia, Canada, New Zealand, United Kingdom	2015 (April)

During FY18, DOT&E approved 19 CTE and RUTF PAs. The RUTF PAs were particularly useful for partner nations to test new capabilities in geographic environments not available in home countries. For example, due to lack of tropical or desert-like conditions, the German military used a RUTF PA to validate their night vision goggles (NVG) under such conditions at the U.S. Army Test and Evaluation Center (ATEC) Tropical Region Test Center (TRTC) in Panama. Following the success of that assessment, German Special Operation Forces performed an operational test of the G95K Rifle and NVG at the ATEC TRTC in jungle conditions and at the ATEC Yuma Test Center in desert conditions.

Figure 1 – Night Vision Goggle Image

In FY18, Norway used a RUTF PA to test the Joint Strike Missile (JSM) to qualify the JSM for integration with the F-35 Joint Strike Fighter. The Air Force conducted the testing for the Norwegian government at the Utah Test and Training Range using an F-16 aircraft.

Figure 2 – A JSM Launched From an F-16 Scores a Direct Hit on Its Target

In FY18, Australia used a RUTF PA to conduct testing of the U.S. Assault Breacher Vehicle (ABV), the Joint Assault Bridge (JAB), and new vehicle subsystems. The testing occurred in representative operational conditions at Aberdeen Proving Ground, Maryland. This testing supported decisions to field the ABV and JAB and to acquire additional vehicle capabilities.

Figure 3 – Assault Breacher Vehicle Risk Reduction Testing

For recurring test events, DOT&E established an Omnibus concept as an efficient and timesaving approach to managing PAs. The Omnibus concept establishes an overarching project arrangement for recurring testing over an extended period or for similar testing to be conducted on various platforms. Each repetition is detailed in an Annex to the Omnibus PA instead of creating a new PA. The security sections, legal aspects, and financial provisions of the project are only negotiated once. This streamlines administrative processing. Omnibus RUTF PAs are currently used for the long-standing Combat Archer and Combat Hammer testing of Canadian aircraft and missiles as well as collaboration between the United States and Canada to add IED protection to Tactical Armored Patrol Vehicles.

A recent and revealing example of a recurring test was the U.S. – United Kingdom IAMD testing conducted at the Hebrides Test Range in the United Kingdom in the fall of 2017. While the testing was clearly successful, the IAMD example showcased an important limitation of bilateral agreements. This testing was conducted during the multinational exercise "Formidable Shield" involving assets of nine nations. But, under the bilateral agreement, information and results could only be shared between the U.S. and the United Kingdom. Multinational data sharing with the other participating nations was administratively difficult and would require multiple, unrelated bilateral international agreements. In response to the 2017 IAMD test events, the United Kingdom executed bilateral

Figure 4 – *USS Donald Cook* (DDG 75) Fires an SM-3 Block IB

PAs with the other participating nations. The Trans-Atlantic MTEP, currently in the early stages of technical discussions, would establish an agreement simplifying the administration of future multinational IAMD tests.

The above PAs are examples of how IT&E enabled partner nations to conduct effective and efficient testing in representative environments. Other bilateral and multinational IT&E projects initiated or conducted in FY18 are listed in Table 2 below.

TABLE 2. IT&E PROJECT ARRANGEMENTS IN EFFECT IN FY18

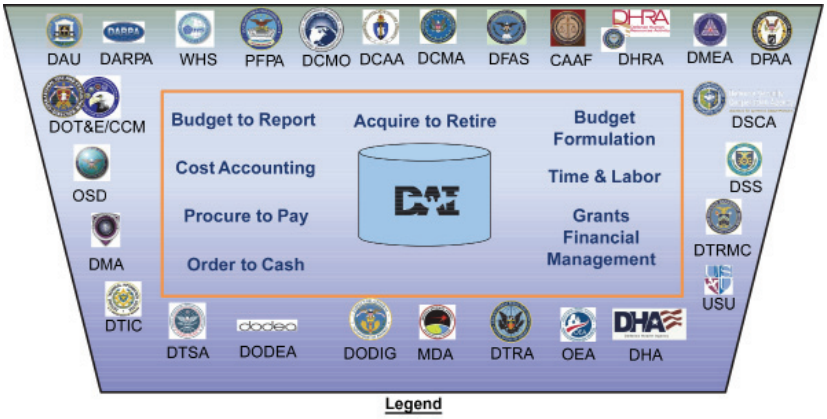
INTERNATIONAL TEST AND EVALUATION PROJECTS	U.S. AGREEMENT DATE	TEST ACTIVITY DATES
Special Operations Engineer Regiment Chemical and Biological Defence Tactics, Techniques, and Procedures RUTF PA (Australia)	September 26, 2018	September 24 to October 26, 2018, and FY19, 20, 21, 22
Performance Characterization of Aerosol Referee Equipment RUTF PA (Norway)	September 24, 2018	October 2018 to March 2019
LOGAN Virtual Simulation System Validation RUTF PA (Canada)	September 27, 2018	September 17 - 28, 2018
International Novel Threat Agent Characterization Trials CTE PA Amendment 1 (Australia, Canada, and the United Kingdom)	August 29, 2018	September 2017
T&E of Shipboard Jammer and Off-Board Decoy Electronic Countermeasure - Electronic Attack Techniques RUTF PA Amendment 1 (Canada)	August 16, 2018	October 2015 to September 2022
CH-147F Radar Warning Receiver Assessment and Characterization Trial RUTF PA (Canada)	August 10, 2018	Fall 2018 over a 2-week period
OT&E Rifle and Night Vision Goggles (NVG) in Desert Conditions RUTF PA (Germany)	June 19, 2018	July 17 - 23, 2018
OT&E Rifle and NVG in Tropical Conditions RUTF PA (Germany)	June 19, 2018	August 1 - 9, 2018
Hypervelocity Gun Weapons System Sub-Sonic Cruise Missile Surrogate Intercept RUTF PA (Australia)	June 13, 2018	July 23 to August 2, 2018
Global Biosurveillance Technology Initiative/Targeted Acquisition of Reference Materials Augmenting Capabilities RUTF PA (Australia)	April 30, 2018	October 2018 to June 2021 (est.)
Sophos/Kydoimos Challenge IV RUTF PA (Australia)	April 30, 2018	May 7 - 18, 2018
Sophos/Kydoimos Challenge IV RUTF PA (Canada)	April 11, 2018	May 7 - 18, 2018
Combat Hammer Omnibus RUTF PA (Canada)	April 4, 2018	April 27 to May 4, 2018
Simulation Testing of Energy Attenuating Crew Seats RUTF PA (United Kingdom)	January 31, 2018	March to May 2018 & May to July 2018
Low Frequency Acoustic Characteristics RUTF PA (United Kingdom)	December 20, 2017	Various test periods between 2018 and 2022
OT&E NVG in Tropical Conditions RUTF PA (Germany)	December 15, 2017	Jan 14 - 19, 2018
Assault Breacher Vehicle Risk Reduction Activity RUTF PA (Australia)	November 30, 2017	April 28 to August 13, 2018 (est.)
T&E Joint Air Delivery Unit Parachute Test Team Exercise Winter Rider - High Altitude Parachute T&E from a C-130 Aircraft RUTF PA (United Kingdom)	October 25, 2017	November 14 to March 1, 2018 (est.)
Tropical Performance of the Joint Effects Targeting System RUTF PA (Australia)	October 20, 2017	October 16 to November 10, 2017 (est.)

Finally, there was activity within three working groups in FY18. The Partnership for Autonomous Robotic Test Instrumentation Working Group with Germany was signed on March 18, 2018. In February 2018, stakeholders for the KC-46A Tanker Aircraft Refueling Interoperability Working Group with France met to discuss potential aerial refueling certification with multirole French fighter aircraft, the Mirage 2000 and the Rafale. Later in August 2018, the Flight Test Working Group with Canada convened for discussions on topics for future PAs.

Defense Agencies Initiative (DAI)

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted FOT&E of Defense Agencies Initiative (DAI) Increment 2 from March 5 through April 6, 2018.
  - During the FOT&E, JITC evaluated new and existing capabilities implemented by DAI-equipped defense agencies, DOD field activities, and other defense organizations (collectively referred to here as Agencies).
  - JITC also evaluated new functionality for Agencies that recently migrated to DAI (Washington Headquarters Services and Defense Contract Audit Agency).
- DAI is operationally effective. The system successfully completed 99 percent of all critical tasks within 7 business process areas throughout all operational testing.
- Operational suitability for DAI is marginal. Overall system availability was high and DAI supported the audit readiness of the DOD; however, usability and system responsiveness ranged from marginal to not acceptable.
  - Limited regression testing of a security patch to address an Information Assurance Vulnerability Alert (IAVA) led to increased sporadic system latency during FOT&E.
  - Based on the System Usability Scale Survey for 7 out of 22 Agencies using DAI, Agencies that migrated to DAI during Increment 1 assessed DAI usability as marginal and Agencies that migrated to DAI during Increment 2 assessed DAI usability as not acceptable.
  - DAI exceeded system availability requirements with 99 percent system availability.
  - Agency representatives responsible for audit readiness agree that DAI supports audit readiness through its financial reporting and transaction traceability.
  - Help desk metrics indicate the DAI system is sustainable. However, most Agencies provide additional funding to sustain Tier 1 (local) help desk support, functional and system training, and support for new capability development, which masks the true cost of DAI sustainment for the DOD enterprise.
- JITC and the Defense Logistics Agency Information Operations, Cybersecurity (J61) Penetration Test Team conducted a modified Cooperative Vulnerability and Penetration Assessment (CVPA) from February 12 to March 16, 2018, to verify remediation of open findings from previous cybersecurity testing.
  - Based on previous testing and the remediation of five of six open findings, DAI is secure against a cyber threat having limited to moderate capabilities. However, the overall survivability assessment remains undetermined until the final open finding is remediated and verified.



Legend

CAAF - Court of Appeals for the Armed Forces
DAI - Defense Agencies Initiative
DARPA - Defense Advanced Research Projects Agency
DAU - Defense Acquisition University
DCAA - Defense Contract Audit Agency
DCMA - Defense Contract Management Agency
DCMO - Deputy Chief Management Officer
DFAS - Defense Finance and Accounting Service
DHA - Defense Health Agency
DHRA - Defense Human Resources Activity
DMA - Defense Media Activity
DMEA - Defense Microelectronics Activity
DODEA - Department of Defense Education Activity
DODIG - Department of Defense Inspector General
DOT&E/CCM - Director, Operational Test & Evaluation including Center for Countermeasures (CCM)
DPAA - Defense Prisoner of War/Missing In Action Accounting Agency
DSCA - Defense Security Cooperation Agency
DSS - Defense Security Service
DTIC - Defense Technical Information Center
DTRA - Defense Threat Reduction Agency
DTRMC - Defense Test Resource Management Center
DTSA - Defense Technology Security Administration
MDA - Missile Defense Agency
OEA - Office of Economic Adjustment
OSD - Office of the Secretary of Defense
PFPA - Pentagon Force Protection Agency
USU - Uniformed Services University of the Health Sciences
WHS - Washington Headquarters Services

System

- DAI is an integrated financial management solution that provides a real-time, web-based system of integrated business processes used by defense financial managers, program managers, auditors, and the Defense Finance and Accounting Service. The DAI core functionality is based on commercially available enterprise resource planning solutions.
- DAI subsumes many systems and standardizes business processes for multiple DOD Agencies. It modernizes these business processes by streamlining management capabilities to address financial reporting material weaknesses, and support financial statement auditability.
- The Defense Information Systems Agency (DISA) provides facilities, network infrastructure, and the hardware operating system for DAI servers at DISA data centers.
- Agencies employ DAI worldwide and across a variety of operational environments via a web portal using each Agency's existing information system infrastructure.
- The DAI program is delivering capability incrementally:
  - Increment 2 had four software releases, each adding capabilities and deploying to additional Agencies. With the completion of Increment 2 Release 4 fielding in October 2017, DAI provides services to 22 Agencies with 39,342 users at 1,148 locations worldwide.

  - The DAI Program Management Office (PMO) has begun development and fielding of Increment 3 to provide additional capabilities to existing Agencies and to add DISA, the Defense Commissary Agency, and potentially other Agencies from FY18 through FY23. DISA went live with Time and Labor capabilities in June 2018 as part of Increment 3 Release 0.1, and increased the DAI user base to 45,725 users at 1,834 locations worldwide.
- DAI supports financial management requirements in the Federal Financial Management Improvement Act and DOD Business Enterprise Architecture and is a key tool for helping DOD Agencies have their financial statements validated as ready for audit.

Mission

Financial Managers in defense agencies use DAI to transform their budget, finance, and accounting operations to achieve accurate and reliable financial information in support of financial accountability and effective and efficient decision-making.

Major Contractors

- CACI – Arlington, Virginia
- International Business Machines – Armonk, New York
- Northrop Grumman – Falls Church, Virginia
- Intellipoint Consulting, Inc. – Ashburn, Virginia

Activity

- On October 3, 2017, the USD(AT&L) issued a Full Deployment Decision for DAI Increment 2 and a development Authority to Proceed for DAI Increment 3.
- The DAI PMO conducted six developmental test events in FY18:

  DAI Increment 3 Release 0.1
  - Development integration test from December 22, 2017, through March 2, 2018
  - System integration test from March 12 through April 6, 2018
  - User acceptance test from May 7 through June 1, 2018

  DAI Increment 3 Release 1
  - Development integration test from March 30 through June 12, 2018
  - System integration test from June 25 through July 27, 2018
  - User acceptance test from August 6 through September 7, 2018
- In coordination with DISA, the DAI PMO conducted its annual Continuity of Operations (COOP) tabletop exercise on January 19, 2018. Both JITC and DOT&E observed the event and assessed the DAI COOP capability as meeting requirements. DAI PMO briefed the COOP results to all Agencies with no concerns noted.
- From March 5 through April 6, 2018, JITC conducted an FOT&E of DAI Increment 2 in accordance with a DOT&E-approved test plan. Interoperability Certification data were collected from November 2017 through May 2018.
- From February 13 through March 16, 2018, JITC and the Defense Logistics Agency (DLA) Information Operations, Cybersecurity (J61) Penetration Test Team conducted a modified CVPA to verify that actions taken by the DAI PMO successfully corrected open findings from IOT&E. The DAI PMO deferred the data fraud analysis portion of the Cyber Economic Vulnerability Assessment (CEVA) until Increment 3 testing.
- DOT&E published its "Defense Agencies Initiative Increment 2 Release 4" FOT&E report in November 2018.
- JITC and the DAI PMO are planning an operational assessment (OA) and cybersecurity testing during 2Q-3QFY19 for Increment 3 Release 1. The OA will focus on new Agencies, new functionality, and those measures of performance that were not tested or that were inconclusive at the end of Increment 2 testing. The cybersecurity testing will consist of a validation of corrected actions based upon findings from Increment 2 testing, a CVPA, an Adversarial Assessment, and a COOP exercise.
- On September 26, 2018, the USD(A&S) issued an Acquisition Decision Memorandum delegating Milestone Decision Authority to DLA for DAI Increment 3 and all future program increments.

Assessment

- DAI is operationally effective and has made significant improvements compared to previous T&E events.
  - During the Increment 2 FOT&E, IOT&E, and two OAs combined, DAI successfully completed 2,447 of 2,466 critical tasks (99 percent). The 19 unsuccessful tasks included hardware, software, or system errors that the PMO has corrected, and user errors that better training and user documentation could address.
  - The DAI Increment 2 Business Case defines the High Level Outcomes (HLOs) that establish the rationale for DAI Increment 2. During the FOT&E, DAI reported on 11 of 18 HLOs. In some cases, Agencies are not using the full suite of Increment 2 capabilities, are not monitoring the HLO dashboard, or have not achieved the HLO thresholds. DOT&E will reassess the HLOs during Increment 3 testing.
  - DAI Increment 2 added functionality for Budget Formulation and Grants Financial Management Accounting, but the PMO has yet to measure the effectiveness of those functionalities. DAI Budgeting Formulation is still maturing with five Agencies leveraging the capability.
- The operational suitability for DAI is marginal. Auditability, reliability, availability, maintainability, and sustainability of the help desk support were all acceptable. However, the

mission effects from periods of high system latency resulted in not acceptable user experiences.

- The DAI PMO introduced a software security patch in January 2018 that resulted in sporadic system latency. Correcting the system required several planned and unplanned maintenance outages during the test period, negatively affecting users. Automated regression testing and performance testing could reduce the risk of future patches negatively affecting the production environment.
- DAI exceeded system availability requirements with 99 percent system inherent availability. System inherent availability is the percentage of time a system is available, while operational availability is the percentage of time that a system is capable of performing its mission. DAI also exceeded the performance requirements for other reliability, availability, and maintainability measures during FOT&E. Ten system failures occurred over a 6-month period from November 2017 to April 2018 and the mean time between system failures was 410 hours. The mean time to repair the 10 system failures was 4.5 hours. The 11 scheduled maintenance periods and the 10 unplanned maintenance periods averaged 14 hours each and resulted in an operational availability of 93 percent.
- The DAI PMO has a goal of one 27-hour maintenance period completed during one weekend per month. Achieving that goal would improve operational availability to 96 percent. This would better support worldwide operations and improve weekend operations during peak periods, especially during the critical closeout period near the end of the fiscal year.
- In spite of the improvements in the DAI system, users continue to give the program a marginal System Usability Scale score. Users from the three Increment 1 Agencies surveyed assessed usability as marginal, whereas users from the four Increment 2 Agencies surveyed assessed usability as not acceptable. Factors causing the not acceptable user ratings include:
  - Experience is a statistically significant factor. Four out of seven Agencies surveyed during FOT&E had used DAI for less than 3 years. Users at those four Agencies assessed usability to be not acceptable (less than 50 percent). Agencies with more experience scored DAI higher.
  - Frequent user comments on DAI functionality related to system slowness and difficulty of entering data and generating DAI reports, queries, and search requests.
  - Sporadic system latency during January and February 2018 from an operating system security patch to address an IAVA resulted in poor user experiences.
- DAI Help Desk support for the Agency help desks is acceptable, but most Agencies provide additional funding to obtain additional staff for help desk support, training, and support for new capability development. This user funding masks the true cost of DAI sustainment for the DOD enterprise.
- The DAI Help Desk processed 6,850 service requests between November 1, 2017, and May 1, 2018, with the number of open tickets increasing from 697 to 821 during that period. Although the DAI Help Desk is sustainable, the DAI PMO needs to allocate more resources so that the ticket resolution rate (37 per day) is on par with the ticket submission rate (38 per day).
- Customer satisfaction with the DAI Help Desk was 77 percent, compared to 75 percent for the local Agency help desk support.

- DAI is secure against a cyber threat having limited to moderate capabilities, but the overall survivability assessment remains undetermined since more testing is required.
  - During the modified CVPA, JITC and the DLA Information Operations, Cybersecurity (J61) Penetration Test Team verified that the DAI PMO had corrected five out of the six findings from the IOT&E Adversarial Assessment.
  - JITC did not test the cybersecurity defender's ability to detect and mitigate Red Team activities; therefore, net defense will remain unassessed until the Adversarial Assessment during Increment 3 testing.
- During the Increment 2 CEVA, Agencies' financial experts concluded that the existing technical checks would make it difficult to exploit known or potential vulnerabilities to commit fraud. DOT&E is monitoring the DOD Inspector General FY18-19 Financial Audits of Agencies on DAI to assist with CEVA requirements.
- Per DISA and DLA Chief Information Officer policy, the DAI PMO conducts a remote recovery exercise once every 3 years, with a tabletop exercise conducted in the years between.
- During both the FY17 and FY18 COOP exercises, the DAI PMO and DISA conducted a tabletop exercise where personnel reviewed and updated the Information Security Contingency Plan. Previously in FY16, DAI PMO testers successfully executed selected business functions on alternate site servers, which verified that the alternate site could restore mission essential business functionality. DAI will test select business functions at the alternate site in January 2019.

Recommendations

The full list of recommendations is available in the November 2018 DOT&E DAI FOT&E report.
The DAI PMO should:

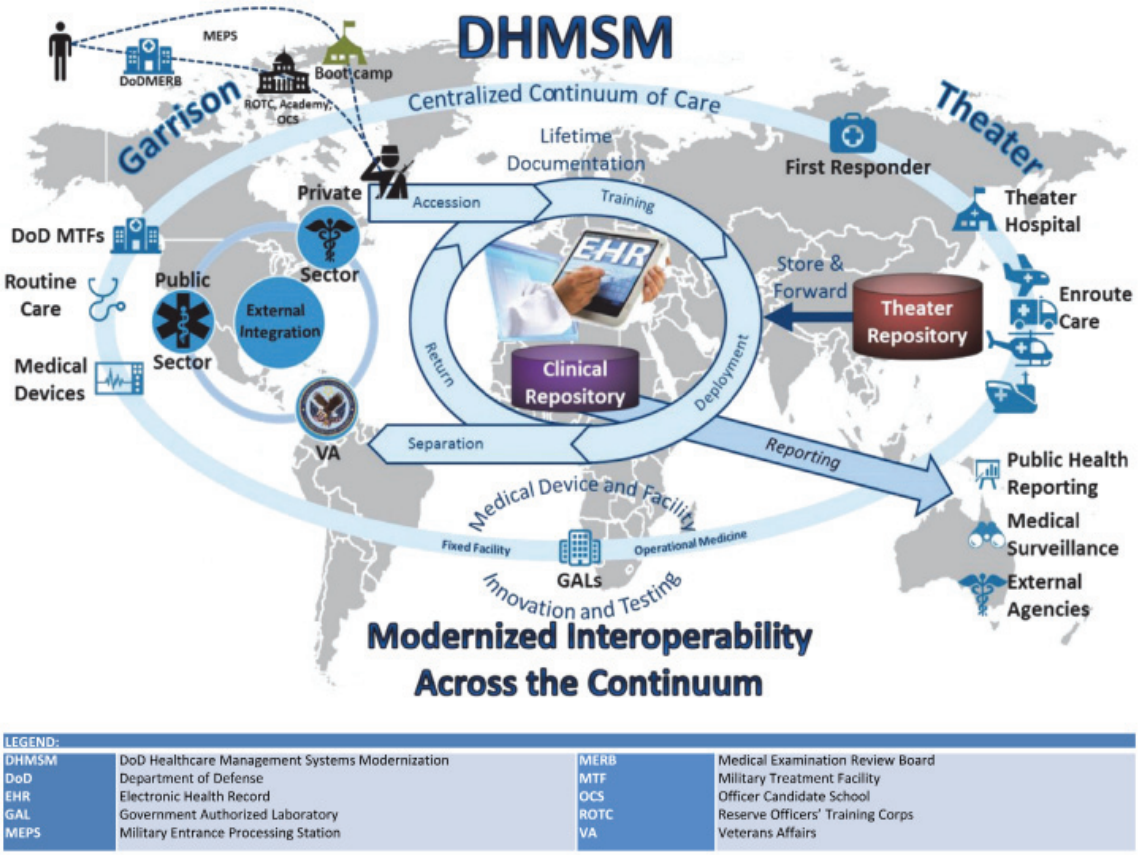
1. Improve both regression and performance testing in order to reduce the risk of introducing misconfigured code into the production environment.
2. Work with the Office of the Under Secretary of Defense (OUSD) Comptroller to mature DAI budget formulation capabilities.
3. Work with DISA to improve system responsiveness.
4. Along with OUSD Comptroller and the Agencies, track the progress of the Agencies and the Department to achieve HLO thresholds.
5. Allocate more resources so that the ticket resolution rate is at least on par with the ticket submission rate.

6. In conjunction with JITC, measure system responsiveness during operational testing to quantify the latency problems identified through user survey responses during Increment 2 testing.

DOD Healthcare Management System Modernization (DHMSM)

Executive Summary

- Military Health System (MHS) GENESIS is intended to transform the way the DOD and the Department of Veterans Affairs provide military and veteran healthcare missions by creating a single health care record for each patient, used by both agencies. Currently, health care records reside in multiple legacy systems, making it difficult for health care providers to understand a patient's complete medical history. MHS GENESIS provides an integrated health record and delivers new capabilities to increase patient safety, such as barcode medication administration and decision support tools.



LEGEND:			
DHMSM	DoD Healthcare Management Systems Modernization	MERB	Medical Examination Review Board
DoD	Department of Defense	MTF	Military Treatment Facility
EHR	Electronic Health Record	OCS	Officer Candidate School
GAL	Government Authorized Laboratory	ROTC	Reserve Officers' Training Corps
MEPS	Military Entrance Processing Station	VA	Veterans Affairs

- MHS GENESIS will be deployed to DOD hospitals and clinics worldwide. MHS facilities encompass 54 hospitals, 377 medical clinics, and 270 dental clinics. Over 205,000 medical staff members will use the system to deliver and document healthcare for 9.4 million beneficiaries.
- The DOD Healthcare Management System Modernization (DHMSM) Program Office deployed MHS GENESIS at four Initial Operational Capability (IOC) sites in Washington State between February and October 2017.
- The Joint Interoperability Test Command (JITC) conducted IOT&E, with Service Operational Test Agency (OTA) assistance, from September through December 2017, at three of the IOC sites.
  - MHS GENESIS was not operationally effective because it did not demonstrate enough workable functionality to effectively manage and document patient care. Users satisfactorily performed 56 percent of the 197 medical and administrative tasks used as measures of performance, and generated 207 incident reports, 156 of which were high priority.
  - MHS GENESIS was not operationally suitable because of poor system usability, insufficient training, and inadequate help desk support. Users gave MHS GENESIS usability an average score of only 37 out of 100 on the System Usability Scale (SUS), well below the threshold of 70 that indicates acceptable usability.
- The Program Office postponed the IOT&E at the fourth IOC site to improve system effectiveness and suitability in select clinical areas from January to March 2018. The Program Office closed over half (118 of 209) of the incident reports generated at the first three IOC sites. Of the 118 incident reports closed, 98 of these were high priority.
- The contractor implemented an upgrade to the core Millennium software within MHS GENESIS in April 2018.
- JITC completed the IOT&E at the fourth IOC site, with Service OTA assistance, in July 2018. This site is a larger hospital than the previous IOC sites, providing specialty and subspecialty care, with more MHS GENESIS functionality.

  - Although key MHS GENESIS functions improved and the system worked well in 18 of 70 clinical areas, MHS GENESIS is not yet operationally effective. Users satisfactorily performed 45 percent of the medical and administrative tasks used as measures of performance. Users generated 298 incident reports, 254 were high priority.
  - MHS GENESIS is not yet operationally suitable because of poor system usability and insufficient training and documentation. The Madigan Army Medical Center (MAMC) users gave MHS GENESIS usability an average score of 40 out of 100 on the SUS.
- JITC and Space and Naval Warfare Systems Command (SPAWAR) Red Team completed a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) from November 2017 through June 2018 and an Adversarial Assessment (AA) in September 2018.
  - MHS GENESIS is not survivable in a cyber-contested environment. JITC and the SPAWAR Red Team successfully executed three cybersecurity attacks against the system as an insider, near-sider, and outsider. The results of MHS GENESIS cybersecurity testing will be provided in a separate, classified report.
- Following the IOT&E, the Program Office and Defense Health Agency (DHA) have worked swiftly to resolve the open incident reports. As of December 14, 2018, DHA recommended 114 of 388 (34 percent) incident reports and 29 of 57 (51 percent) top priority incident reports for closure. DHA has recommended all top priority software defect incident reports for closure.
- The Program Office created a Cyber Integrated Work Group (CIWG) to improve the cybersecurity posture of MHS GENESIS. The working group identified 34 specific tasks assigned to the appropriate parties, focused upon incident response and intrusion detection as well as prioritization and mitigation of identified vulnerabilities.

System
- The Program Office plans to field MHS GENESIS, a modernized Electronic Health Records (EHR) system, to 205,000 Military Health System personnel providing care for 9.4 million DOD beneficiaries worldwide. MHS facilities encompass 54 hospitals, 377 medical clinics, and 270 dental clinics worldwide.
- MHS GENESIS comprises three major elements:
  - The Millennium suite of applications, developed by Cerner, which provides medical capabilities
  - Dentrix Enterprise, developed by Henry Schein, Inc., which provides dental capabilities
  - Orion Rhapsody Integration Engine, developed by Orion Health, which enables the majority of the external information exchanges
- MHS GENESIS will replace legacy healthcare systems including the Armed Forces Health Longitudinal Technology Application (AHLTA), Composite Health Care System (CHCS), and Essentris inpatient system. MHS GENESIS will replace legacy Operational Medicine components of the Theater Medical Information Program (TMIP) – Joint software suite including AHLTA-Theater, TMIP CHCS Caché, and AHLTA-Mobile.
- The Program Office established two program segments to support deployment of the DHMSM EHR System to the DOD enterprise:
  - Fixed Facility (Segment 1) supports all medical and dental services delivered by permanent inpatient hospitals and medical centers, ambulatory care clinics, and dental clinics.
  - Operational Medicine (Segment 2) supports theater hospitals, hospital ships, forward resuscitative sites, naval surface ships, and submarines. The Program Office will provide MHS GENESIS to the Joint Operational Medicine Information System Program Office for implementation of Segment 2.

Mission

DOD medical staff will use MHS GENESIS to manage delivery of enroute care, dentistry, emergency department, health, immunization, laboratory, radiology, operating room, pharmacy, vision, audiology, and inpatient/outpatient services. DOD medical staff will also use MHS GENESIS to perform administrative support, front desk operations, logistics, billing, and business intelligence.

Major Contractors
- Leidos – Reston, Virginia
- Cerner – Kansas City, Missouri
- Accenture Federal Services – Arlington, Virginia
- Henry Schein, Inc. – Melville, New York

Activity
- The Program Office completed MHS GENESIS Go-Live at all four IOC sites in 2017:
  - Fairchild Air Force Base (FAFB), Washington, on February 7, 2017
  - Naval Health Clinic Oak Harbor (NHCOH), Washington, on July 15, 2017
  - Naval Hospital Bremerton (NHB), Washington, on September 23, 2017
  - Madigan Army Medical Center (MAMC), Washington, on October 21, 2017
- JITC conducted IOT&E Phase 1, with Service OTA assistance, at FAFB and NHCOH from September 25 to October 6, 2017, and NHB from December 4 – 15, 2017, in accordance with a DOT&E-approved test plan.
- The Program Office postponed testing at MAMC to implement changes to MHS GENESIS to improve system effectiveness

and suitability of select clinical areas from January to March 2018.
- The contractor implemented an upgrade to the core Millennium software within MHS GENESIS in April 2018.
- JITC conducted IOT&E Phase 2, with Service OTA assistance, at MAMC from June 18 to July 12, 2018, in accordance with a DOT&E-approved test plan.
- JITC and SPAWAR Red Team completed a CVPA in three phases assessing the commercial data center at the Cerner Technology Center (CTC), Kansas City, Missouri, from November 4 – 15, 2017; assessing medical devices and peripherals connecting to MHS GENESIS at the Fixed Facility Government Approved Laboratory (FF GAL), Auburn, Washington, from April 14 – 25, 2018; and assessing the end-user environment at MAMC from June 18 – 29, 2018.
- JITC and SPAWAR Red Team conducted an AA in September 2018. The CVPA and AA were conducted in accordance with a DOT&E-approved test plan.

Assessment
- IOT&E Phase 1 was adequate to determine that MHS GENESIS was neither operationally effective nor operationally suitable.
  - MHS GENESIS was not operationally effective because it did not demonstrate enough workable functionality to effectively manage and document patient care. Users satisfactorily performed 56 percent of the 197 medical and administrative tasks used as measures of performance. Users generated 209 incident reports, 156 of which were high priority. Because each hospital had its own process for completing work, which sometimes conflicted with the enterprise processes inherent to MHS GENESIS, poorly defined user roles and workflows within MHS GENESIS resulted in an increase in the time required for health care providers to complete daily tasks. Some providers reported that they needed to work overtime and were seeing fewer patients per day due to delays caused by problems with MHS GENESIS. Some users questioned the accuracy of the information exchange between external systems and MHS GENESIS.
  - MHS GENESIS was not operationally suitable because of poor system usability, insufficient training, and inadequate help desk support. A lack of documentation forced users to develop their own operational workarounds. Users gave MHS GENESIS usability an average score of 37 out of 100 on the SUS, below the threshold of 70 that indicates acceptable usability.
  - System outages indicated that the end-to-end system and supporting network did not have sufficient availability to support operations at the four IOC sites. Users reported increased lag times when other IOC sites went live, suggesting the current system and supporting network configuration may not support the hundreds of additional sites planned for MHS GENESIS.
- IOT&E Phase 2 was adequate to determine that MHS GENESIS is not yet operationally effective or operationally suitable.
  - MHS GENESIS worked well in 18 of 70 clinical areas, and the Program Office fixed over half of the incident reports (118 of 209) generated during Phase 1 IOT&E. Of the 118 incident reports closed, 98 of these were high priority. However, users satisfactorily performed only 45 percent of the medical and administrative tasks used as measures of performance. Users generated 298 new Incident Reports, 254 of which were high priority.
  - MHS GENESIS was not operationally suitable because of poor system usability, insufficient training and documentation, and inadequate dissemination of system change information. MAMC users gave MHS GENESIS usability an average score of 40 out of 100 on the SUS. New users indicated that they needed more training with the system. Users did not receive information about updates or changes to the MHS GENESIS system.
  - Users did not report major system outages during the Phase 2 IOT&E. However, the Program Office did not provide detailed reliability, availability, and maintainability information for independent review. DOT&E was not able to evaluate these aspects of MHS GENESIS.
- MHS GENESIS is not survivable in a cyber-contested environment. JITC and the SPAWAR Red Team successfully executed three cybersecurity attacks against the system as an insider, near-sider, and outsider. The results of MHS GENESIS cybersecurity testing will be provided in a separate, classified report.
- Following the IOT&E, the Program Office and DHA categorized the 388 open high-priority incident reports into the following areas: configuration (25 percent), software defect (10 percent), enhancement (20 percent), policy/process (4 percent), knowledge deficit (32 percent), and other (8 percent). DHA further designated 57 of the 388 incident reports as their top priority for resolution.
- The Program Office and DHA have worked swiftly to resolve the OT&E incident reports. As of December 14, 2018, DHA recommended 114 of 388 (34 percent) incident reports and 29 of 57 (51 percent) top priority incident reports for closure. DHA has recommended all top priority software defect incident reports for closure.
- The Program Office created a CIWG to improve the cybersecurity posture of MHS GENESIS. The working group includes the major cybersecurity players including the Program Office, Leidos, Cerner, SPAWAR, and the DHA. The working group identified 34 specific tasks assigned to the appropriate parties in the following areas: configuration management, medical devices, recovery, detect and response, and incident response.

Recommendations

- The USD(A&S) should direct the Program Executive Office (PEO), Defense Healthcare Management Systems (DHMS) and DHA to provide a plan to resolve high-priority incident reports, and provide updates on the status of high-priority incident reports.
- The Surgeons General of each of the Services should provide their full support to DHA and the PEO DHMS to establish enterprise-wide workflows and training.
- The PEO DHMS and DHA:
  1. Develop a corrective action (burndown) plan for the Priority 1 and 2 incident reports.
  2. Provide the USD(A&S) and DOT&E updates on the status of high-priority incident reports, between now and the next fielding.
- The DHMSM Program Office, working with the military healthcare community, should continue their collaborative efforts to:
  1. Resolve Priority 1 and 2 Incident Reports prior to further fielding.
  2. In coordination with DOT&E, plan JITC-led assessments at current MHS GENESIS sites to verify high-priority incident report fixes.
  3. Work with DHA to implement a consistent method of notifying users of changes to the system.
  4. Improve training and documentation for both new site implementation and sustainment.
  5. Continue to resolve known cybersecurity deficiencies.
  6. Improve interoperability, focusing on database exchanges identified as problematic during IOT&E.
  7. Monitor reliability and availability to ensure the system meets users' needs.
  8. Continue to work with the DHA and the Defense Information Systems Agency to isolate network communications problems and reduce latency.
  9. Conduct FOT&E at the next fielding to further evaluate corrective actions and revised training, to inform further fielding decisions.

F-35 Joint Strike Fighter (JSF)

Executive Summary

Programmatics

- Block 3F Development
  - The program completed System Design and Development (SDD) flight testing in April 2018, but continued testing new modernization increments of software to address open deficiencies and improve performance.
  - The program and stakeholders reviewed open deficiencies between May and July, re-categorizing many of the 102 Category 1 deficiencies (as of May 2018) to Category 2, leaving 13 open Category 1 deficiencies for entry into IOT&E, which later became 15.
- IOT&E Readiness
  - The program focused on preparations for IOT&E readiness throughout FY18.
  - The Defense Acquisition Executive certified the program as ready for entry into formal IOT&E, provided eight remaining readiness requirements are met prior to the start of for-score events.
  - DOT&E verified readiness and approved the F-35 IOT&E Test Plan on December 3, 2018.
  - The Joint Strike Fighter (JSF) Operational Test Team (JOTT) began formal IOT&E open-air testing in accordance with the plan on December 5, 2018.
- Continuous Capability Development and Delivery (C2D2)
  - The JSF Program Office (JPO) and Lockheed Martin began to transition the development effort from delivering Block 3F capabilities in the SDD contract to a more rapid development, testing, and fielding cycle for additional capabilities in Block 4, and to address deficiencies carried over from SDD.
  - DOT&E considers the current C2D2 schedule to be high risk due to the large amount of planned capabilities to be delivered in 6-month increments.

Operational Effectiveness

- Operational Testing
  - The JOTT began conducting pre-IOT&E early test events for score in January 2018 with cold weather testing, followed by additional testing starting in April, including two-ship scenarios, deployments, and weapons testing.
- Mission Data Load (MDL) Development and Testing
  - The U.S. Reprogramming Laboratory (USRL) demonstrated the capability to create functioning MDLs for Block 3F and earlier blocks during SDD; however, it still lacks adequate equipment to be able to fully test and optimize MDLs under stressing conditions to ensure adequate performance against current and future threats.
  - Significant additional investments, well beyond the current upgrades to the signal generator channels and reprogramming tools, are required now for the USRL to support F-35 Block 4 C2D2 MDL development.

Operational Suitability

- Autonomic Logistics Information System (ALIS)
  - The program completed fielding of ALIS 2.0.2.4 in early CY18 and focused on testing the next iteration of the software, version 3.0.1.
  - Two additional versions of ALIS 3.0.1 software were developed and tested – versions 3.0.1.1 and 3.0.1.2 – to address deficiencies before delivery to fielded units.
- Cybersecurity Operational Testing
  - During CY18, the JOTT assessed ALIS version 3.0, F-35 training systems, and the ALIS-to-shipboard network interface onboard a nuclear powered aircraft carrier.
  - Cybersecurity testing in 2018 showed that some of the vulnerabilities identified during earlier testing periods still had not been remedied.
  - Limited cybersecurity testing of the air vehicle is planned during IOT&E; more testing will be needed.
- Availability, Reliability, and Maintainability
  - There was no improving trend in fleet aircraft availability
  - Fleet-wide average availability is below program target value of 60 percent and well below planned 80 percent needed for efficient conduct of IOT&E.
  - The trend in fleet availability has been flat over the past 3 years; the program's reliability improvement initiatives are still not translating into improved availability.
  - Reliability and maintainability metrics defined in the JSF Operational Requirements Document are not meeting interim goals needed to reach requirements at maturity.

Live Fire Test and Evaluation (LFT&E)

- In FY18, Lockheed Martin completed the Vulnerability Assessment Report and the Consolidated LFT&E Report. These reports do not include results from Electromagnetic Pulse (EMP) or gun lethality testing, which were not completed by the end of FY18.

- DOT&E is reviewing the F-35 vulnerability reports and completing its own evaluation, which will be documented in the combined IOT&E and LFT&E report to be published prior to the Full-Rate Production decision, anticipated in FY20.
- The JPO evaluated the chemical and biological agent protection and decontamination systems during dedicated full-up system-level testing. However, the test plan to assess the chemical and biological decontamination of pilot protective equipment is not adequate because the JPO does not plan to test the decontamination process for either the Generation (Gen) III or Gen III Lite Helmet-Mounted Display System (HMDS).
- Air-to-ground flight lethality tests of three 25-mm round variants against armored and technical vehicles, small boats, and plywood mannequins were conducted at the Naval Air Warfare Center Weapons Division (NAWCWD) at NAWS China Lake, California, from August through December 2017. The rounds tested were the Projectile Gun Unit (PGU)-32/U Semi-Armor-Piercing High-Explosive Incendiary round, PGU-47/U Armor-Piercing High-Explosive Incendiary with Tracer round, and PGU-48/B Frangible Armor-Piercing round. The target damage results are classified.

System

- The F-35 JSF program is a tri-Service, multinational, single-seat, single-engine family of strike aircraft consisting of three variants:
  - F-35A Conventional Take-Off and Landing
  - F-35B Short Take-Off/Vertical-Landing
  - F-35C Aircraft Carrier Variant
- The F-35 is designed to survive in an advanced threat environment (year 2015 and beyond). It is also designed to have improved lethality in this environment compared to legacy multi-role aircraft.
- Using an active electronically scanned array radar and other sensors, the F-35 with Block 3F or later software is intended to employ precision-guided weapons (e.g., GBU-12 Laser-Guided Bomb, GBU-31/32 JDAM, GBU-39 Small Diameter Bomb, Navy Joint Stand-Off Weapon version C1) and air-to-air missiles (e.g., AIM-120C Advanced Medium-Range Air-to-Air Missile (AMRAAM), AIM-9X infrared-guided, air-to-air missile) and a 25 mm Gun Automatic Unit (GAU)-22/A cannon.
- The SDD program was designed to provide mission capability in three increments:
  - Block 1 (initial training; two increments were fielded: Block 1A and Block 1B)
  - Block 2 (advanced training in Block 2A and limited combat capability with Block 2B)
  - Block 3 (limited combat capability in Block 3i and full SDD warfighting capability in Block 3F)
- The F-35 is under development by a partnership of countries: the United States, United Kingdom (UK), Italy, the Netherlands, Turkey, Canada, Australia, Denmark, and Norway.

Mission

- The Combatant Commander will employ units equipped with F-35 aircraft in joint operations to conduct a variety of missions during day or night, in all weather conditions, and in heavily defended areas.
- The F-35 will be used to attack fixed and mobile land targets, surface units at sea, and air threats, including advanced aircraft and cruise missiles.

Major Contractor

Lockheed Martin, Aeronautics Company – Fort Worth, Texas

Programmatics

Block 3F Developmental Testing

- **Activity**
  - The program completed SDD developmental flight testing on April 11, 2018, after nearly 10 years of flight testing.
  - At the completion of Block 3F developmental flight testing in April, the program had 941 open deficiencies – either in work or under investigation. These included 102 Category 1 deficiencies and 839 Category 2 deficiencies.
  - The Integrated Test Force (ITF) published their report on Block 3F testing in March 2018. The report documented numerous open deficiencies across the air system in the final version of Block 3F software, 18 of which were designated Category 1. The ITF recommended that the deficiencies be corrected, although the system could proceed into IOT&E.
  - As of October 17, 2018, the JPO had collected data and verified performance to close out 475 of 536 (89 percent) contract specifications paragraphs. Additionally, 3,363 of 3,452 (97 percent) success criteria derived from the contract specifications had been completed.
  - The program continued to address documented deficiencies in the Block 3F software by developing and flight testing additional software versions, under the nomenclature of Block 30RXX, as part of planned modernization. Throughout CY18, the program developed and tested numerous iterations, including versions 30R00, 30R01, and 30R02, and associated "Quick Reaction Cycle" versions (e.g., 30R01.02) to correct deficiencies and improve performance.

- The test centers at Edwards AFB, California, and Naval Air Station (NAS) Patuxent River, Maryland, made plans to transition test aircraft from Block 3F SDD to follow-on modernization. The status and configuration of the 18 developmental test aircraft used for SDD testing as of the end of September 2018 are as follows: 3 were retired, 2 were in storage, 5 were available for flight sciences testing, 5 were continuing missions systems testing, and 3 were returned to the Marine Corps and Navy as operational test aircraft.
- The program and stakeholders reviewed open deficiency reports between May and July, re-categorizing many of the 102 Category 1 deficiencies (as of May 2018) to Category 2, leaving 13 open Category 1 deficiencies for entry into IOT&E, which later became 15.

• **Assessment**
- Although the program completed SDD flight testing in April, the test centers continued to work on Block 3F technical debt by addressing known deficiencies. The extent that the open deficiencies will affect combat capability will be assessed during IOT&E.

Static Structural and Durability Testing

• **Activity**
- The F-35A full scale durability test article (AJ-1) completed the third lifetime of testing (one lifetime is 8,000 equivalent flight hours (EFH) on October 17, 2017. The test article was delivered to an inspection facility in June 2018, and is currently undergoing disassembly, inspections, and analysis.
- The program suspended testing of the F-35B ground test article (BH-1) after completing the second lifetime of testing in February 2017. Due to the significant amount of modifications and repairs to bulkheads and other structures, the program declared the F-35B ground test article no longer representative of the wing-carry-through structure in production aircraft, deemed it inadequate for further testing, and canceled the testing of the third lifetime with BH-1. The program secured funding to procure another ground test article, which will be production-representative of Lot 9 and later F-35B aircraft built with a re-designed wing-carry-through structure, but to date does not have the procurement of the test article on contract. The program has not completed durability testing of the aircraft with the new wing-carry-through structure to date.
- The F-35C durability test article (CJ-1) began third lifetime testing on April 4, 2017, and reached 18,792 EFH on April 12, 2018. Testing was stopped at that time following the discovery of more cracking in the Fuselage Station (FS) 518 Fairing Support Frame (cracking had been discovered at the end of the second lifetime), requiring repair before additional testing could proceed. After making an estimate for the cost and time to repair or replace the FS 518 Fairing Support Frame, coupled with the need to manage other structural parts that had existing damage (fuel floor segment, FS 450 bulkhead, FS 496 bulkhead, FS 556 bulkhead, and front spar repair) via scheduled inspections, the program determined that the third lifetime testing should be discontinued. The test article was removed from the test fixture in August 2018 and prepped for shipment to the tear down and inspection facility in September. Although the program planned for a third lifetime of testing to accumulate data for life extension, if needed, the program currently has no plans to procure another F-35C ground test article.

• **Assessment**
- For all variants, this testing has led to discoveries requiring repairs and modifications to production designs, some as late as Lot 12 aircraft, and retrofits to fielded aircraft.
- Based on durability testing, the service life of early-production F-35B aircraft is well under the expected service life of 8,000 flight hours, and may be as low as 2,100 flight hours. Fleet F-35B aircraft are expected to start reaching their service life limit in CY26, based on design usage. The JPO will continue to use Individual Aircraft Tracking (IAT) of actual usage to help the Services project changes in timing for required repairs and modifications, and aid in Fleet Life Management.
- For the F-35C, expected service life will be determined from the durability and damage tolerance analysis following tear down.

IOT&E Readiness

• **Activity**
- The JPO, Lockheed Martin, and JOTT continued to make preparations for entry into formal IOT&E.
- On August 24, 2018, DOT&E provided guidance in a memorandum to the test agencies on detailed requirements for formal entry into IOT&E. Specifically, to add clarity to the formal entrance criteria, the following items were listed as requirements for formal start:
  - F-35 software version Block 30R02 with Level 4 (fully validated and verified) mission data files (MDF)
  - ALIS software version 3.0
  - Air-to-Air Range Infrastructure (AARI) system with corrections planned for Block 30R02 software.
- On October 2, 2018, the Defense Acquisition Executive certified the program as ready for entry into formal IOT&E provided eight remaining readiness requirements are met prior to the start of for-score events:
  - A fully validated and verified mission data file for the Block 30R02.03 software
  - U.S. Services airworthiness authorities provide flight clearances for each variant with the Block 30R02.03 software
  - The program provides flight series data and joint technical data updated for the Block 30R02.03 software
  - Full partner participation is authorized for the applicable portions of the IOT&E mission sets
  - The last OT aircraft undergoing depot modifications – BF-18 – is delivered to Edwards AFB

  - Accreditation of necessary models for use in IOT&E are completed or on track for use
  - All unit-level modifications to the OT aircraft are complete, except those specifically waived or deferred by DOT&E
  - AARI has been installed on aircraft BF-17, BF-18, and CF-8 (the last three U.S. OT aircraft to complete depot modifications).
- DOT&E approved the IOT&E test plan on December 3, 2018, after verifying that the remaining readiness actions listed above had been met.

• **Assessment**
- Two additional factors caused readiness for the formal start of IOT&E to slip into early December. A Category 1 deficiency associated with blanking of the cockpit displays was discovered in Block 30R02.03 software, causing an additional software patch called 30R02.04 to be developed and tested prior to start of formal IOT&E. Additionally, a fleet-wide grounding in October 2018 to inspect and replace fuel pump tubes in a number of the OT aircraft added to the delay in readiness to start.

Continuous Capability Development and Delivery (C2D2)

• **Activity**
- The JPO and Lockheed Martin began to transition the development effort from delivering Block 3F capabilities in the SDD contract to a more rapid development, testing, and fielding cycle for additional capabilities in Block 4 and to address deficiencies carried over from SDD.
- The program's plans for the Block 4 modernization are included in an updated F-35 acquisition strategy that was approved on October 16, 2018.
  - These plans include lean test designs and agile development tenets.
  - The developmental test effort will be government-led compared to the contractor-led approach used for SDD.
  - The program plans to leverage a greater dependence on modeling and simulation than was used during SDD.
- The program developed and began staffing a draft Test and Evaluation Master Plan (TEMP) to support Block 4 development activities.

• **Assessment**
- The current C2D2 schedule is high risk with the planned content of capabilities to be made available for delivery in 6-month increments.
- Many of the lessons learned from SDD involving the amount of testing that can be done in laboratories and simulations, vice flight testing, could be applied to C2D2 planning.
- The program needs to ensure adequate funding is available to support a robust laboratory and simulation environment and develop adequate verification, validation, and accreditation plans.
- Sustaining multiple configurations of fielded aircraft (i.e., Block 2B, Block 3F, and the new electronic warfare (EW) system in Lot 11 and later aircraft) while managing a developmental test fleet with updated hardware to support the production of new lot aircraft will be a challenge for the JPO.
- The cost of software sustainment for multiple configurations of aircraft needs to be adequately assessed.
- The planned 6-month software release cycle does not align with the timelines of other increments of capability needed to support the entire JSF system (i.e., ALIS, mission data, training simulators, aircraft modifications). Other modern fighters (e.g., F/A-18, F-22) have historically taken much longer than 6 months – 2 and 3 years, respectively – to field new increments of capability. A more realistic C2D2 schedule with achievable content releases that includes adequate test infrastructure (labs, aircraft, and time) and modifications while aligning the other fielding requirements is necessary.
- F-35 modernization is on OT&E oversight. DOT&E will review the content of each Block 4 increment and, if the increment contains significant new capabilities or new hardware, it will require a tailored formal OT&E. DOT&E routinely conducts "agile" OT for other programs, so each F-35 OT&E will be tailored to be as efficient as possible while maintaining test adequacy by leveraging integrated testing with developmental testing (DT) and focusing on evaluating the new capabilities and affected mission areas.

Operational Effectiveness

Operational Testing

• **Activity**
- DOT&E, in coordination with the JPO and the JOTT, approved execution of select for-score pre-IOT&E test activities, prior to satisfying all 47 TEMP readiness criteria for IOT&E, when the applicable readiness criteria were met and the testing could be adequately completed.
  - Pre-IOT&E Increment 1: On January 18, 2018, DOT&E approved the JOTT to conduct planned cold weather testing that occurred from January 18 to February 2, 2018, at Eielson AFB, Alaska. The operational test squadrons deployed six F-35 aircraft, two of each variant, from Edwards AFB, California. The purpose of this for-score testing was to evaluate the suitability of the F-35 air system and evaluate alert launch timelines in the extreme cold weather environment. The deployment was one of six required by the F-35 IOT&E test design.
  - Pre-IOT&E Increment 2: Following approval from DOT&E on March 30, 2018, the JOTT began for-score testing of limited two-ship mission scenarios with Block 3F (30R00) software and Level 2 MDFs. The scenarios included Close Air Support, Reconnaissance, Forward Air Controller-Airborne, Strike Coordination and Armed Reconnaissance, and Combat Search and Rescue, along with ship deployments and weapons delivery events. Some missions were re-flown by the

A-10 as part of the planned F-35A and A-10 comparison testing.
  - The JOTT and the F-35A operational test squadrons deployed four F-35A OT aircraft from June 4 – 29, 2018, to Eglin AFB, Florida, to conduct Pre-IOT&E air-to-air missile Weapons Demonstration Events over the Gulf Coast test ranges. During the deployment, the test team completed six AIM-120 and six AIM-9X missile events, some with multiple shots, and all in accordance with the approved plan. In limited cases, DOT&E approved modifications to the mission profile when warranted.
  - The JOTT, in coordination with VFA-125, the Navy's west coast F-35C Fleet Replacement Squadron, deployed six aircraft aboard the USS *Abraham Lincoln* from August 18 – 31, 2018, to conduct shipboard operations and evaluate F-35C sortie generation rate (SGR) capabilities, per the IOT&E test plan.
  - The test included participation of aircraft from Carrier Air Wing Seven, which provided an operationally representative flight deck environment. This was the first time the F-35C was integrated with the rest of a carrier air wing as it would during an operational deployment.
  - The Navy approved the use of the F-35 Integrated Power Package (IPP) in the hangar bay for maintenance purposes, on an interim basis, just prior to the SGR testing onboard CVN 72. This approval will enable more efficient maintenance during deployments, increasing the options for providing electrical power and cooling air to aircraft undergoing maintenance. Squadrons will use temperature sensing devices to ensure that the IPP exhaust, which vents upwards on the F-35C, does not damage hangar bay overhead equipment, cabling, and structure while in use.
  - The Navy finalized a design for the Closed Bay Fire Fighting Tool (CBFFT), and produced several examples to provision CVN 72's crash and fire personnel prior to the SGR testing. The CBFFT will allow emergency responders to cut through the exterior of an F-35 aircraft carrying live internal ordnance and plug a water hose into the hole to provide ordnance cooling during a fire on the flight deck.
  - The JOTT and the F-35A operational test squadron deployed four F-35A OT aircraft to Volk Field Air National Guard Base, Wisconsin, to evaluate sortie generation rate surge operations from September 10 – 16, 2018. Although the test plan called for six aircraft to deploy, two remained at Edwards AFB due to maintenance problems.

- **Assessment**
  - DOT&E will report the results of the pre-IOT&E test events following IOT&E.

Gun Testing

- **Activity**
  - All three F-35 variants have the GAU-22/A cannon. The F-35A gun is internal; the F-35B and F-35C each use an external gun pod. Differences in the outer mold-line fairing mounting make the gun pods unique to a specific variant (i.e., an F-35B gun pod cannot be mounted on an F-35C aircraft).
  - Through July 2018, 19 air-to-ground strafing missions had been completed to assess gun accuracy on the F-35A. Eighteen missions were flown with AF-31 and one mission with AF-80. Over 3,400 rounds were fired using a cross section of rounds, including PGU-23, PGU-47, and PGU-48.
  - Through July 2018, 13 air-to-ground strafing missions had been completed using the missionized gun pod; one on BF-15, one on BF-16, six on BF-17, and five on CF-08. Overall, 2,695 rounds were fired using PGU-23 and PGU-32 rounds, including some for assessing accuracy compliance.
  - Operational test pilots conducted live firings of the gun against airborne targets, including drones and towed banners, throughout CY18. These firings were often in combination with other weapon demonstration events, such as air-to-air missile employment events.
- **Assessment**
  - Based on F-35A gun testing through September 2018, DOT&E currently considers the accuracy of the gun, as installed in the F-35A, to be unacceptable.
  - F-35A gun accuracy during SDD failed to meet the contract specification. Although software corrections were made to the F-35 mission systems software to improve the stability of gun aiming cues, no software or hardware corrections have yet been implemented to correct the gun accuracy errors.
  - Investigations into the gun mounts of the F-35A revealed misalignments that result in muzzle alignment errors. As a result, the true alignment of each F-35A gun is not known, so the program is considering options for re-boresighting and correcting gun alignments.
  - During air-to-air gun testing, F-35A operational test pilots received intermittent "unsafe gun" cockpit alerts while attempting gun attacks. These alerts occurred with two different aircraft; the root cause is under investigation.
  - F-35B and F-35C air-to-ground accuracy results to date with the gun pod have been consistent and meet the contract specifications. They do not show the accuracy errors of the internal gun on the F-35A.

Mission Data Load (MDL) Development and Testing

- **Activity**
  - F-35 effectiveness relies on the MDL, which is a compilation of the mission data files (MDF) needed for

operation of the sensors and other mission systems. The MDL works in conjunction with the avionics software and hardware to drive sensor search behaviors to provide target identification parameters. This enables the F-35 avionics to identify, correlate, and respond to sensor detections, such as threat and friendly radar signals.
  - The contractor produces an initial set of MDLs for each software version to support DT during SDD.
  - The USRL at Eglin AFB, Florida, creates, tests, and verifies operational MDLs – one for OT and training, plus one for each potential major geographic area of operation, called an area of responsibility (AOR). OT aircraft and fielded aircraft use the applicable USRL-generated MDLs for each AOR.
- The testing of the USRL MDLs is an operational test activity, as arranged by the JPO after the program restructure that occurred in 2010, and consists of laboratory and flight testing on OT aircraft.

- **Assessment**
  - Because MDLs are software components essential to F-35 mission capability, the Department must have a reprogramming lab that is capable of rapidly creating, testing, and optimizing MDLs, as well as verifying their functionality under stressing conditions representative of real-world scenarios.
    - The USRL demonstrated the capability to create functioning MDLs for Block 3F and earlier blocks during SDD. However, it still lacks adequate equipment to be able to test and optimize MDLs under conditions stressing enough to ensure adequate performance against current and future threats in combat.
    - The lab lacks a sufficient number of high-fidelity radio frequency signal generator channels, which are used to stimulate the F-35 EW system and functions of the radar, with simulated threat radar signals. This situation is improving as of the writing of this report, but additional improvements, above and beyond those currently planned, will be required.
    - By late 2019, both USRL mission data test lines will have been upgraded from three to eight high-fidelity channels. Eight high-fidelity channels per line represents a substantial improvement, but is still far short of the 16-20 recommended in the JPO's own 2014 gap analysis.
    - Even when this upgrade is complete, the USRL will still not have enough signal generators to simulate a realistic, dense threat laydown with multiple modern surface-to-air missile threats and the supporting air defense system radars that make up the signal background in the laydown.
  - The reprogramming lab must also be able to rapidly modify existing MDLs when intelligence data changes.
    - The mission data reprogramming hardware and software tools used by the USRL during SDD were cumbersome, requiring several months for the USRL to create, test, optimize, and verify a new MDL for each AOR. For this reason, effective rapid reprogramming capability was not demonstrated during SDD.
    - This situation recently improved with the delivery of a new Mission Data File Generation (MDFG) tool set from the contractor. How much improvement these tools will bring to MDL development timelines is yet to be determined, but initial indications are that the improvements will be significant.
  - Significant additional investments, well beyond the current upgrades to the signal generator channels and MDFG tools, are required now for the USRL to support F-35 Block 4 C2D2 MDL development.
    - The C2D2 plan includes new avionics hardware. Concurrency in development and production during SDD resulted in multiple fielded F-35 configurations that will continue to need to be supported indefinitely (i.e., until a specific configuration is modified or retired), after the development program enters the C2D2 phase. During C2D2, the program will require the USRL, or an additional reprogramming lab, to have the capability to simultaneously create and test MDLs for different avionics hardware and software configurations. These different configurations include the fielded Technical Refresh 2 processors for Block 3F, new EW equipment in Lot 11 and later aircraft, an improved display processor, new Technical Refresh 3 open-architecture processors, and other avionics for later increments in C2D2.
    - In order to be on a timeline that is fully aligned with the planned C2D2 capability development timeline, the C2D2 hardware upgrades for the USRL should have already been on contract. However, the requirements for the C2D2 software integration lab have yet to be fully defined. The JPO must expeditiously complete the development of these requirements while ensuring adequate lab infrastructure to meet the aggressive development timelines of C2D2 and the operational requirements of the Block 4 F-35.
  - As part of IOT&E, the USRL will complete an Urgent Reprogramming Exercise (URE). This test event will evaluate the ability of the USRL, with its hardware and software tools, to respond to an urgent request to modify the mission data in response to a new threat or a change to an existing threat.
    - During a URE at the USRL in 2016, the total hours recorded were double the Air Force standard for rapidly reprogramming a mature system. The JOTT identified several key process problems, including the lack of necessary hardware, analysis tools that were not built for operational use, and missing capabilities, such as the ability to quickly determine ambiguities in the mission data.
    - The JPO is working to correct these problems in order to bring the ability of the USRL to react to new threats up to the identified standards routinely achieved on legacy aircraft. A new Ambiguity Analysis Tool (AAT),

originally developed to meet requirements set forth for the Australia-Canada-UK Reprogramming Lab (ACURL), was delivered to both the ACURL and the USRL. The initial version of the AAT has provided improvements in identifying and correcting mission data ambiguities. Enhancements to the AAT now in work promise to significantly speed up the mission data development process.

- In addition to resolving the laboratory deficiencies above, the program will need to properly sustain the USRL to ensure a high state of readiness, particularly if the Services have an urgent reprogramming requirement, which could happen at any time for the fielded aircraft. To meet these tasks, the USRL will also need to maintain all necessary equipment in a functioning status with a high rate of availability, which will require a sufficient number of prime contractor Field Service Engineers to assist in maintenance and operation of the lab equipment, and adequate training for laboratory personnel. In addition, the USRL requires adequate technical data for lab equipment and enough spare parts and/or supply priority to quickly repair key components.

Joint Simulation Environment (JSE)

- **Activity**
  - The JSE is a man-in-the-loop, F-35 software-in-the-loop mission simulator intended to conduct IOT&E scenarios with modern threat types and densities that are not able to be replicated in open air. Originally slated to be operational by the end of 2017, first use of a fully functional simulator is now planned for the beginning of 2019 with accreditation later in 2019, near the end of planned IOT&E trials.
  - The JSE's physical facilities (cockpits, visuals, and buildings) and synthetic environment (terrain, threat, and target models) are nearing completion and security accreditation. Integration of the F-35 and its weapons is planned for 1QFY19. The JSE verification and validation process has made progress, but the bulk of validation testing still remains for the first half of FY19.
- **Assessment**
  - The government-led JSE team made good progress this year in getting the hardware developed and installed, which will likely meet requirements for IOT&E.
  - The planned schedules for JSE software development and accreditation support IOT&E, but there is some risk to software development (particularly F-35 model integration), which also affects verification and validation. Without the JSE, the IOT&E will be unable to adequately assess the F-35 against dense and modern threats that are not available for open-air testing, resulting in operational risk. Once the JSE completes development and accreditation, it should be an invaluable resource for follow-on F-35 testing and possibly for testing of other platforms.

Radar Signal Emulators (RSE)

- **Activity**
  - The Nevada Test and Training Range (NTTR) began accepting Radar Signal Emulators in late CY16 to support the DOT&E-initiated Electronic Warfare Infrastructure Improvement Program (EWIIP). As of October 10, 2018, 9 of 16 emulators had been accepted on the NTTR and had been used to conduct integration testing with the F-35 and other range test assets.
  - The RSEs will be used to provide operationally realistic threat laydowns for use in F-35 IOT&E.
- **Assessment**
  - All 16 RSEs should complete acceptance testing and integration by the end of CY18 and will be used to emulate threats during IOT&E.
  - More detail on the background, development, and fielding of EWIIP can be found in the T&E Resources section of this report.

Operational Suitability

Autonomic Logistics Information System (ALIS)

- **Activity**
  - The program completed fielding of ALIS 2.0.2.4 in early 2018. Feedback from operational users included:
    - The Deployment Planning Tool did not work well or significantly improve the ease of deploying F-35 units.
    - Life Limited Parts Management, which includes propulsion data integration and Production Aircraft Inspection Requirements (PAIRs), requires a great deal of time with manual workarounds by maintenance personnel.
  - The program rolled the capabilities planned for release in ALIS 2.0.2.5 into the next block of software – ALIS 3.0.1. ALIS 2.0.2.5 was intended to address deficiencies and usability problems, upgrade the browser to Internet Explorer 11, and include a filtering function to decrease false alarms in the Prognostic Health Management (PHM) System, referred to as Advanced Filter and Correlate (AFC).
  - The program focused on testing in preparation for fielding ALIS software version 3.0.1 throughout CY18. This version of ALIS software includes the following new major capabilities:
    - Support for lightning protection.
    - Low Observable Health Assessment System (LOHAS) improvements.
    - Security enhancements.
    - The first increment of the new Training Management System for tracking maintainer qualifications.
    - Improvements to address technical debt and corrections to existing deficiencies.

- The program conducted initial testing of ALIS 3.0.1 with field data between November 28, 2017, and January 7, 2018.
  - Testing with developmental test aircraft occurred at the Air Force Test Center at Edwards AFB and NAS Patuxent River.
  - The Operationally Representative Environment (ORE) at Edwards AFB was also used, which consists of production-representative ALIS hardware in a closed network and is designed for testing ALIS software using data downloaded from OT aircraft. The ORE also allows testing of ALIS propulsion capabilities as ALIS cannot support SDD propulsion systems.
  - Because of limitations associated with the hardware versions of the ALIS equipment used to support the SDD aircraft and the ORE, the program could not conduct fully operationally representative testing of new ALIS software versions in either venue.
- The initial report issued jointly by the test centers at Edwards AFB and NAS Patuxent River recommended that ALIS 3.0.1 continue development and testing before fielding.
- After making several fixes, the program completed testing of ALIS 3.0.1.1 with field data at the same venues between April 3 and May 31, 2018, and recommended fielding of this release. Findings included:
  - Updated software corrected the erroneous recording of air vehicle flight hours to components installed on a different air vehicle, a deficiency identified during ALIS 3.0.1 testing.
  - Problems with existing ALIS 2.0.2.4 capabilities noted in ALIS 3.0.1 testing were largely resolved.
  - PHM performance improved as ALIS 3.0.1.1 eliminated intermittent failures of PHM to auto-populate and display data during debrief.
  - AFC reduced non-actionable Health Reporting Codes (HRC) and maintainer workload.
  - Supply chain management data processing, data accessibility of Electronic Equipment Logbooks (EELs), which contain a virtual record of data for a specific part, and Anomaly Fault Resolution System reliability improved.
  - Significant deficiencies in supporting aircraft parts records remained, including long-standing enterprise-wide problems with data quality.
  - Documenting maintenance tasks in ALIS frequently takes more time than completing the maintenance action.
  - The lack of accurate and complete data in ALIS continued to drive many workarounds.
  - Deficiencies in the Deployment Planning Tool and in air vehicle data transfer functionality were not resolved in ALIS 3.0.1.1. Both require a high level of contractor support with frequent work stoppages, creating a heavy burden on support personnel time.
- The program completed verification testing of ALIS 3.0.1.1 at Nellis AFB, Nevada, to evaluate some capabilities, including LOHAS enhancements and lightning protection, which the program could not fully evaluate during prior testing. Following completion of this verification period, the program approved the release of ALIS 3.0.1.1 to operational test at Edwards AFB, which took place in August 2018. Concurrently, the program continued implementing fixes to ALIS 3.0.1.1 for the next software release, ALIS 3.0.1.2. The program conducted initial testing of ALIS 3.0.1.2 on SDD aircraft and at the ORE between June 9 and September 20, 2018, using five engineering releases. Initial testing was followed by verification testing at Nellis AFB beginning September 15, 2018. ALIS 3.0.1.2 does not deliver any new capabilities, focusing instead on delivering fixes to existing deficiencies. These fixes include:
  - Improvements within ALIS reporting of the inert gas state of the aircraft fuel system for lightning protection.
  - A propulsion data processing anomaly introduced in ALIS 3.0.1.1 was corrected.
  - A deficiency introduced in ALIS 3.0.1.1 that caused some damage tracings to not translate properly into LOHAS, resulting in significant inaccuracies in LOHAS status beyond the scope of actual damage, was corrected.
- The program installed ALIS 3.0.1.2 at the operational test sites at Edwards AFB beginning on September 25, 2018; it is expected to be the fielded version of ALIS that is currently being used during formal IOT&E.

- **Assessment**
  - ALIS is designed to bring efficiency to maintenance and flight operations, but it does not yet perform as intended. User feedback on ALIS deficiencies, some of which can have a significant effect on aircraft availability and sortie generation, fall into three major categories:
    - Users must employ numerous workarounds due to data and functionality deficiencies. Most capabilities function as intended only with a high level of manual effort by ALIS administrators and maintenance personnel. Manual workarounds are often needed to complete tasks designed to be automated. Configuration management of ALIS software and data products remains complex and time-consuming.
    - Users must deal with pervasive problems with data integrity and completeness on a daily basis. Maintainers frequently have to manually enter missing or incorrect EEL data, which accompany spare parts, so they can be accepted and tracked by an ALIS Standard Operating Unit (SOU) at the squadron and installed on an aircraft. Fixing data in complex EELs, which represent an assembly such as ejection seats, requires a great deal of time from ALIS administrators. EELs problems have many sources, including vendors who have not complied with guidance on creating EELs; a lack of standardization among suppliers, contractors, and field locations for updating EELs; and a lack of automation in the EEL process. Problems with EELs are a top-5

Not Mission Capable (NMC) maintenance driver and a top-10 propulsion degrader for the U.S. Air Force.
  - Users lack confidence in some ALIS functionality. For example, the problems noted above have resulted in users maintaining separate databases to track life usage in case PAIRs erroneously generates incorrect data. Users reference the external database created to determine the correct values.
- The timeline for correcting ALIS deficiencies is typically excessive, causing workarounds to remain in place for extended periods. For example, ALIS incorrectly reports the status of aircraft as NMC in the Squadron Health Management application based on HRCs (faults). Meanwhile, a separate application – Customer Maintenance Management System, which relies on the Mission Essential Function List (MEFL) – reports the same aircraft as mission capable. A logistics test and evaluation report for ALIS version 1.0.3A3 in December 2012 first noted this problem, yet it remains today in ALIS 3.0.1.2.
  - Many open deficiencies were not resolved during SDD and will continue to negatively affect aircraft availability and SGR.
  - During SDD, the program repeatedly demonstrated that attempting major software releases with large increments of ALIS capability resulted in delays and deferring capability. The program also did not allocate sufficient resources to simultaneously develop new required capabilities and reduce technical debt. Smaller, more frequent releases would allow the program to field new capabilities and fixes and receive frequent user feedback to plan for future improvements, which the program plans to do in C2D2.
- The program has completed several deployments to established bases and to austere locations and ships. In each location, the complexities of ALIS have caused a variety of information technology problems that delay the unit's ability to start generating sorties. Often, the timeframe to start flight operation is longer than that with legacy aircraft.
- The program plans to release an updated version of ALIS software (ALIS 3.1) to the international partners and foreign military sales customers that includes country-unique data (a.k.a. sovereign data) management within ALIS beginning in January 2019 .
- The program plans an additional major release of ALIS software, version 3.5, scheduled for fielding in mid-2019, during IOT&E. ALIS 3.5 will be a stabilization release, since it is intended to address a large amount of technical debt, meet cybersecurity threshold requirements – including the use of internet protocols, improving LOHAS, and providing an initial centralized capability for ALIS administration. The program plans to complete ALIS 3.5 with SDD funds.
- The program currently plans two additional releases, ALIS 3.6 and 3.7, to provide additional stabilization and improved sortie generation capabilities.
  - ALIS 3.6, scheduled for release in mid-2020, is planned to include Windows 10, additional cybersecurity enhancements, improved air vehicle data transfers between SOUs, and a decentralized maintenance capability, which would allow deployments without a full suite of ALIS hardware. The program also plans to replace obsolescent hardware with the rollout and fielding of the ALIS 3.6 software.
  - The goal of ALIS 3.7, planned for release in mid-2021, is improved mission support by adding capability to the Training Management System, improved spare parts support for deployments, support for partial squadron deployments, corrosion management, and ALIS support for helmets and other pilot flight equipment.
  - Because EELs is a top degrader, the program is working on high-priority corrective actions. However, per the JPO, the software capabilities planned for ALIS 3.7 will not address the root causes of the enterprise issues. This is an excessive delay for needed fixes.
- The release plan for ALIS 3.5 through 3.7 shows the program is moving toward a pace of one major software release per year with fielding of service packs between major releases. The program has demonstrated that it has difficulty fielding large increments in ALIS capability. While this movement toward more agile software development is positive, the JPO will need to provide sufficient resources for this effort.
- The use of ALIS across the F-35 enterprise would improve data integrity as contractors and vendors would be required to adhere to EELs requirements earlier in production and sustainment.
  - Lockheed Martin did not use ALIS in its production facilities until recently, adding an SOU to the factory floor in March 2018, shortly before propulsion system installation, to improve data quality.
  - Because data problems are frequently found when new aircraft arrive at operational locations, Lockheed Martin plans to begin using an SOU on the Fort Worth flight line in early 2019 to support aircraft before delivery.
  - While the addition of SOUs to the production line is a positive step in addressing data problems, the program will not extract maximum benefit from this effort unless ALIS is fully integrated into production facilities.
  - Vetting the data accompanying spare parts provided by suppliers in an SOU before allowing delivery to field units will reduce EELs deficiencies.
- Assessment of the testing regimen for ALIS.
  - The program still relies heavily on the results of laboratory testing of ALIS software, which does not resemble operational conditions in several ways, including the limited amount of data processed and external connections.
  - After the problems found during ALIS 2.0.2.4 testing and fielding, the program moved toward heavier use of ALIS testing facilities at Edwards AFB. However, these test venues do not permit testing of the full range

of ALIS capabilities. A single ALIS test venue would increase test efficiency and support more timely fielding of ALIS software to operational units. In the meantime, the program uses an operational assessment process at Nellis AFB to evaluate ALIS software releases before deployment to the rest of the fleet.
  - The current, non-operationally representative method of testing ALIS releases leads to delays in finding and fixing deficiencies, often after the new software is fielded.
  - Differences in laboratory testing and fleet personnel procedures show that fleet personnel use ALIS differently than the laboratory testers. Developmental testing, particularly laboratory-based testing, should include a variety of personnel from different Services and experience levels to increase the chances of finding problems early.
  - ALIS testing, architecture, operations, and fielding each absorb a disproportionate amount of time, manpower, and funding. The program is developing automated testing capabilities that are being accelerated in an attempt to improve lab testing speed and quality.

Cybersecurity Operational Testing

- Activity
  - The JOTT continued to accomplish testing based on the cybersecurity strategy approved by DOT&E in February 2015. The JOTT assessed F-35 training systems, the ALIS-to-shipboard network interface onboard a nuclear-powered aircraft carrier (CVN) with ALIS 2.0.2, and ALIS version 3.0.
  - The JOTT tested ALIS 3.0 at all three levels of operation:
    - Autonomic Logistics Operating Unit (ALOU)
    - Central Point of Entry (CPE)
    - Squadron Kit (SQK), composed of the SOU, the Mission Planning and Support Boundary, and the Low Observable Maintenance Boundary
  - In September 2018, the JOTT conducted Cooperative Vulnerability and Penetration Assessments (CVPAs) of ALIS 3.0.1.1 using National Security Agency-certified cybersecurity test organizations and personnel:
    - The Air Force's 346 Test Squadron assessed the sole ALOU at Lockheed Martin, Fort Worth, Texas.
    - The Air Force's 47 Cyber Test Squadron (CTS) assessed the sole U.S. CPE at Eglin AFB, Florida, and the SQK at Edwards AFB, California.
  - In October 2018, the JOTT conducted Adversarial Assessments (AAs) of the next iteration of ALIS 3.0 software – version 3.0.1.2 – with the assistance of National Security Agency-certified Red Teams.
    - The Marine Corps Red Team (MCRT) assessed the ALOU.
    - The Air Force's 57 Information Assurance Squadron (IAS) assessed the CPE.
    - The Air Force's 177 IAS assessed the SQK at Edwards AFB, California.
  - The ALIS 3.0 AA also included a limited Enterprise Assessment of the boundaries and interfaces between the ALOU, CPE, and SOU; Lockheed Martin Red Team testing of the Lockheed Martin Internal network, with observation by U.S. Government cyber test personnel; and a preliminary investigation into the cybersecurity posture of the supply chain for components of the SQK.
  - The JOTT tested the three different network environments present at the Academic Training Center at Eglin AFB, Florida:
    - The Unclassified Operating Environment (UOE), consisting of unclassified classroom and training resources.
    - The Classified Operating Environment (COE), consisting of classified classroom and training resources.
    - The Full Mission Simulator (FMS), consisting of pilot training stations for rehearsing mission tasks in a simulated cockpit.
  - In February through April 2018, the JOTT conducted CVPAs of the UOE, COE, and FMS respectively in partnership with the 47 CTS.
  - In April 2018, the JOTT conducted AAs of the UOE and COE utilizing the 57 IAS.
  - In July 2018, the JOTT conducted an AA of the FMS with the assistance of the 177 IAS.
  - In August 2018, the JOTT conducted an AA onboard the USS *Abraham Lincoln* of the network interface between a deployed SQK in the ALIS 2.0.2 configuration and the ship's Consolidated Afloat Networks and Enterprise Services internal network. The MCRT also facilitated the test.
  - All JSF cyber tests in 2018 were completed in accordance with their individual, DOT&E-approved test plans.
  - Throughout 2018, the JOTT continued to work with stakeholders across the DOD to identify relevant scenarios, qualified test personnel, and adequate resources for conducting cyber testing on air vehicle components and systems.
  - The JOTT expects to conduct a CVPA and AA of the USRL in early 2019, as well as several cyber demonstrations involving air vehicle components and sub-systems.
- **Assessment**
  - Cybersecurity testing in 2018 showed that some of the vulnerabilities identified during earlier testing periods still had not been remedied.
  - More testing is needed to assess the cybersecurity of the air vehicle. Actual on-aircraft or appropriate hardware- and software-in-the-loop facilities are necessary to enable operationally representative air vehicle cyber testing.
  - Testing of the JSF supply chain to date has not been adequate. Additional testing is needed to ensure the

integrity of hardware components for initial production of air vehicles and ALIS components, plus resupply of replacement parts.
- Testing to date has identified vulnerabilities that must be addressed to ensure secure ALIS operations.
- According to the JPO, the air vehicle is capable of operating for up to 30 days without connectivity to ALIS. In light of current cybersecurity threats and vulnerabilities, along with peer and near-peer threats to bases and communications, the F-35 program and Services should conduct testing of aircraft operations without access to ALIS for extended periods of time.

Availability, Reliability, and Maintainability

- **Activity**
  - The program continued to deliver aircraft to the U.S. Services, international partners, and foreign military sales throughout CY18 in production Lot 10. As of the end of September, 323 operational aircraft had been produced for the U.S. Services, international partners, and foreign military sales. These aircraft are in addition to the 13 aircraft dedicated to developmental testing.
  - As of the end of June, the U.S. fleet of F-35s had accumulated 126,136 flight hours
  - The following assessment of fleet availability, reliability, and maintainability is based on sets of data collected from the operational and test units and provided by the JPO. The assessment of aircraft availability is based on data provided through the end of August 2018. Reliability and maintainability assessments in this report are based on data covering the 12-month period ending June 30, 2018. Data for reliability and maintainability include the records of all maintenance activity and undergo an adjudication process by the government and contractor teams, a process which creates a lag in publishing those data. The variety of data sources and processes are the reasons the data have different dates and appear to be delayed.
- **Assessment**
  - The operational suitability of the F-35 fleet remains at a level below Service expectations. Similar to the 2017 DOT&E report, most suitability metrics remained nearly the same throughout 2018 or moved only within narrow bands.
  - Aircraft availability is determined by measuring the percentage of time individual aircraft are in an "available" status, aggregated monthly over a reporting period.
    - The program-set availability goal is modest at 60 percent, and the fleet-wide availability discussion uses data from the 12-month period ending August 2018.
    - For this report, DOT&E is reporting availability rates only for the U.S. fleet, vice including international partner and foreign military sales aircraft, as was done in previous reports.
  - The fleet-wide monthly availability rate for only the U.S. aircraft, for the 12 months ending August 2018, is below the target value of 60 percent. The DOT&E assessment of the trend shows no evidence of improvement in U.S. fleet wide availability during 2018 .
  - Aircraft that are not available are designated in one of three status categories: Not Mission Capable for Maintenance (NMC-M), Depot (in the depot for modifications or repairs beyond the capability of unit-level squadrons), and Not Mission Capable for Supply (NMC-S).
    - The average monthly NMC-M and Depot rates were relatively stable, with little variability, and near program targets.
    - The average monthly NMC-S rate was more variable, and was higher (i.e., worse) than program targets .
    - The average monthly utilization rate measures flight hours per aircraft per month. The average utilization rate of flight hours per tail per month increased slightly over previous years, but remains below original Service bed down plans.
    - The low utilization rates continue to prevent the Services from achieving their programmed fly rates, which are the basis of flying hour projections and sustainment cost models. As of June 30, 2018, the fleet had flown 126,136 hours. This amounted to 83 percent of an early 2017 "modeled achievable" projection of 152,445 flight hours by the end of June, 2018. Similarly, for the 12 months ending April 2018, the U.S. Services had contracted for 42,836 flight hours, but the U.S. F-35 fleet logged only 33,365 hours, or 78 percent of the contracted amount over this period.
  - A separate analysis of availability of the OT-instrumented fleet, using data from the 12-month period ending August 2018, is important to consider now that formal IOT&E is underway. The numbers below account for the full complement of 23 U.S. and international partner aircraft assigned to the OT fleet at the end of August 2018 (8 F-35A, 9 F-35B, and 6 F-35C).
    - The average monthly availability rate for F-35 OT aircraft was below the planned 80 percent needed for efficient conduct of IOT&E. The low availability during this period is partly explained by the fact that the aircraft of the OT fleet spent over a quarter of the time in depot modifications to bring them up to the Lot 9 production-representative standard configuration, as required prior to the start of IOT&E, with some DOT&E-approved modification deferrals.
    - Availability of the OT fleet will remain a challenge for the efficient conduct and timely completion of IOT&E. Although the necessary modifications have been completed on the OT aircraft and formal testing has started, mission capable aircraft will need to be available at a high rate to complete the open-air test trials as scheduled.

F-35 Fleet Reliability

- Aircraft reliability assessments include a variety of metrics, each characterizing a unique aspect of overall weapon system reliability.
  - 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.
  - 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. 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.
  - Mean Flight Hours Between Maintenance Event 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 Operational Requirements Document (ORD) requirement.
  - 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.
- The F-35 program developed reliability growth projection curves for each variant throughout the development period as a function of accumulated flight hours. These projections compare observed reliability with target numbers to meet the threshold requirement at maturity (200,000 total F-35 fleet flight hours, made up of 75,000 flight hours each for the F-35A and F-35B, and 50,000 flight hours for the F-35C). As of June 30, 2018, the date of the most recent set of reliability data available, the fleet and each variant accumulated the following flight hours, with the percentage of the associated hour count at maturity indicated as well:
  - The complete F-35 fleet accumulated 126,136 flight hours, or 61 percent of its maturity value.
  - The F-35A accumulated 74,758 hours, or over 99 percent of its maturity value.
  - The F-35B accumulated 35,076 hours, or 47 percent of its maturity value.
  - The F-35C accumulated 16,302 hours, or 33 percent of its maturity value.
- The program reports reliability and maintainability metrics for the 3 most recent months of data. This rolling 3-month window dampens month-to-month variability while providing a short enough period to distinguish current trends.
- Table 1 shows the trend in each reliability metric by comparing values from May 2017 to those of June 2018 and whether the current value is on track to meet the requirement at maturity.

TABLE 1. F-35 RELIABILITY METRICS (UP ARROW REPRESENTS IMPROVING TREND)

Variant	Flight Hours for ORD for JCS Threshold	Assessment as of June 30, 2018												
		Cumulative Flight Hours	MRHBCF (Hours)			MFHBR (Hours)			MFHBME (Hours)			MFHBF_DC (Hours)		
			ORD Threshold	Change: May 2017 to June 2018	Meeting Interim Goal for ORD Threshold	ORD Threshold	Change: May 2017 to June 2018	Meeting Interim Goal for ORD Threshold	ORD Threshold	Change: May 2017 to June 2018	Meeting Interim Goal for ORD Threshold	JCS Requirement	Change: May 2017 to June 2018	Meeting Interim Goal for ORD Threshold
F-35A	75,000	74,758	20	↑	No	6.5	↑	No	2.0	No Change	No	6.0	↑	Yes
F-35B	75,000	35,076	12	↑	No	6.0	↑	No	1.5	↑	No	4.0	↑	Yes
F-35C	50,000	16,302	14	↓	No	6.0	↓	No	1.5	↑	No	4.0	↑	Yes

- Between May 2017 and June 2018, six of the nine ORD metrics increased in value, often marginally, two decreased marginally, and one remained the same. Consistent with previous reports, the three JSF Contract Specification (JCS) metrics continued to show the strongest growth and, in all cases, were above their specifications for the 3 months ending June 2018. This strong MFHBF_DC growth has still not translated into equally strong growth for the ORD reliability metrics, all of which fall short of their interim goals.
- More in-depth reliability growth analyses conducted by DOT&E show that the ORD reliability metrics are growing, albeit slowly, especially for F-35B and F-35C MFHBCF. Also, for the majority of the metrics, reliability grew markedly more slowly after the release of the Block 2B flight envelope than before. Based on these

analyses, none of the ORD metrics are predicted to meet their requirements by their individual variant maturity milestones.
- In addition to reporting the MFHBCF values above, the JPO adopted a second, alternative approach for reporting MFHBCF in 2017 that only counts critical failures that take 8 hours or more to remedy. This approach presumably supports modeling of SGR, a Key Performance Parameter in the ORD.
  - DOT&E continues to disagree with this approach because failures that take less than 8 hours to remedy will likely still affect SGR, especially during a combat sortie surge. Also, it is not consistent with the widely accepted definition of the MFHBCF measure.

Maintainability
- The amount of time needed to repair aircraft and return them to flying status has changed little over the past year, and remains higher than the requirement for the system at maturity. The program assesses this time with several measures, including Mean Corrective Maintenance Time for Critical Failures (MCMTCF) and Mean Time To Repair (MTTR) for all unscheduled maintenance. Both measures include "active touch" labor time and cure times for coatings, sealants, paints, etc., but do not include logistics delay times, such as how long it takes to receive shipment of a replacement part.
  - 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 NMC to MC status.
  - MTTR measures the average active maintenance time for all unscheduled maintenance actions. It is a general indicator of the ease and timeliness of repair.
- The program reports maintainability metrics for the 3 most recent months of data. Table 2 shows the nominal change in each maintainability metric by comparing values from May 2017 to those of June 2018, and whether the current value is on track to meet the requirement at maturity.
  - All mean repair times are longer, some up to more than twice as long, as their ORD threshold values for maturity, reflecting a heavy maintenance burden on fielded units.
- The JPO, after analyzing MTTR projections to maturity, acknowledged that the program would not meet the MTTR requirements defined in the ORD. The JPO is seeking relief from the original MTTR requirements and has proposed new values of 5.0 hours for both the F-35A and F-35C, and 6.4 hours for the F-35B. This will affect the ability to meet the ORD requirement for SGR, a Key Performance Parameter.

TABLE 2. F-35 MAINTAINABILITY METRICS (DOWN ARROW REPRESENTS IMPROVING TREND)

Variant	Flight Hours for ORD Threshold	Assessment as of June 30, 2018						
		Cumulative Flight Hours	MCMTCF (Hours)			MTTR (Hours)		
			ORD Threshold	Change: May 2017 to June 2018	Meeting Interim Goal for ORD Threshold	ORD Threshold	Change: May 2017 to June 2018	Meeting Interim Goal for ORD Threshold
F-35A	75,000	74,758	4.0	↓	No	2.5	↓	No
F-35B	75,000	35,076	4.5	↑	No	3.0	↑	No
F-35C	50,000	16,302	4.0	↓	No	2.5	↓	No

Live Fire Test and Evaluation

F-35 Vulnerability to Kinetic Threats
- **Activity**
  - In April 2018, Lockheed Martin delivered the F-35 Vulnerability Assessment Report summarizing the force protection and vulnerabilities of all three F-35 variants, and the F-35 Consolidated LFT&E Report, which summarizes the live fire test and analysis efforts supporting the vulnerability assessments.
- **Assessment**
  - The assessments conclude the following:
    - For three of the four specification threats, the F-35 variants meet JSF contract specification requirements to enable safe ejection of the pilot in the event of an engagement.
    - For two of the four specification threats, the F-35A and F-35C variants meet JSF contract specification requirements to return safely to the Forward Line of Troops (FLOT) following an engagement. The F-35B met the requirements for only one of the four threats.
    - All three F-35 variants are less vulnerable to three of the four specification threats than the legacy F-16C aircraft, both for safe ejection and for return to FLOT.
  - DOT&E will publish an independent evaluation of the vulnerabilities of the F-35 aircraft variants to expected

and emerging threats in the report to support the Full-Rate Production decision scheduled for FY20.

F-35 Vulnerability to Unconventional Threats

- **Activity**
  - As of FY17, the Naval Air Warfare Center Aircraft Division at NAS Patuxent River, Maryland, completed full-up system-level testing of F-35A and C variants, and limited testing of the F-35B, to evaluate tolerance to electromagnetic pulse threats.
  - The program completed full-up, system-level, chemical-biological decontamination testing on BF-40 (a low-rate initial production F-35B aircraft) in February 2017.
- **Assessment**
  - Testing was done to the threat level defined in Military Standard 2169B. Follow-on, full-up, system-level tests of the F-35B, including a test series to evaluate Block 3F hardware and software changes, are ongoing.
  - In the event of a chemical or biological attack, the equipment is capable of decontaminating the F-35. Additional work would be needed to develop an operational decontamination capability.
    - To assess the protection capability of the Generation (Gen) II Helmet-Mounted Display System (HMDS) against chemical-biological agents, the JPO completed a comparison analysis of HMDS materials with those in an extensive DOD aerospace materials database. Compatibility testing of legacy protective ensembles and masks showed that the materials used in the protective equipment can survive exposure to chemical agents and decontamination materials and processes. The program plans similar analyses for the Gen III and Gen III Lite HMDS designs. While this assessment of material compatibilities provides some understanding of the force protection capability against chemical and biological agents, it does not demonstrate the process required to decontaminate either HMDS.

F-35 Gun Lethality

- **Activity**
  - From August through December 2017, during DT Weapons Delivery Accuracy testing, the Naval Air Warfare Center Weapons Division at Naval Air Weapons Station China Lake completed air-to-ground flight lethality tests of three different 25 mm ammunitions including the PGU-32/U Semi-Armor-Piercing High-Explosive Incendiary round, PGU-47/U Armor-Piercing High-Explosive Incendiary with Tracer round, and PGU-48/B Frangible Armor-Piercing round. Flight lethality tests included gun firings from all three F-35 variants against armored and technical vehicles, small boats, and plywood manikins. Tests revealed deficiencies with the Armor-Piercing High-Explosive round's fuze reliability for impacts into the ground. Nammo, the Norwegian manufacturer, is conducting testing to further modify the fuze design and increase reliability.
- **Assessment**
  - The weapon-target-pairing lethal effects are currently being analyzed by DOT&E.

Recommendations:

- The program should:
  1. Continue to work with the Services to prioritize and correct the remaining Category 1 and 2 deficiencies discovered during SDD.
  2. Apply lessons learned from SDD and other programs for scoping the amount of C2D2 testing that can be done in laboratories and simulations, compared with the need for flight testing.
  3. Reassess the C2D2 plan to ensure adequate test infrastructure (labs, aircraft, and time) is provided and modifications are aligned with other fielding requirements.
  4. Assess the annual cost of software sustainment.
  5. Determine the cause of the accuracy problems with the F-35A gun firing and implement a solution for increasing gun accuracy for the fielded aircraft.
  6. Develop a consolidated and adequate ALIS test venue to ensure ALIS capabilities are fully tested prior to fielding to operational units
  7. Conduct a study to determine the optimum balance of additional spare parts procurement versus adding depot capacity to repair spare parts, in order to decrease the percentage of NMC aircraft waiting for spare parts.
  8. Continue implementing measures to improve fleet availability.
  9. Make actual aircraft or appropriate hardware- and software-in-the-loop facilities available to enable operationally representative air vehicle cyber testing.
  10. Continue conducting periodic rounds of cybersecurity testing and correcting open cyber deficiencies.
  11. Continue testing the integrity and security of the JSF supply chain, expanding on initial testing conducted in 2018.
- The JPO should:
  1. Complete contracting actions to procure a second F-35B ground test article in order to complete at least two lifetimes of structural durability testing to validate the wing-carry-through structure.
  2. Fund and contract for the 16-20 recommended signal generators called for in the JPO's own 2014 gap analysis study.
  3. Fund and contract for the necessary hardware upgrades to the USRL to support Block 4 development and testing.

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

Executive Summary

- In FY18, the Defense Information Systems Agency (DISA) development of Global Command and Control System – Joint (GCCS-J) focused on the major components of GCCS-J: GCCS-J Global and the Joint Operation Planning and Execution System (JOPES).

Global

- The Program Office used incremental Maintenance Releases (MRs) to develop Global v6.0, completing four Global v6.0 MRs in FY18, which added intelligence, targeting, and chemical/biological/radiological/nuclear defense capabilities to the system. The Joint Interoperability Test Command (JITC) observed and reported on the Global v6.0 MR Level I operational tests. Operational testing in FY18 confirmed that the Program Office implemented the majority of new capabilities and defect fixes successfully. In cases where testers found defects, the Program Office removed the defective capability or component prior to deploying the MR to users.

JOPES

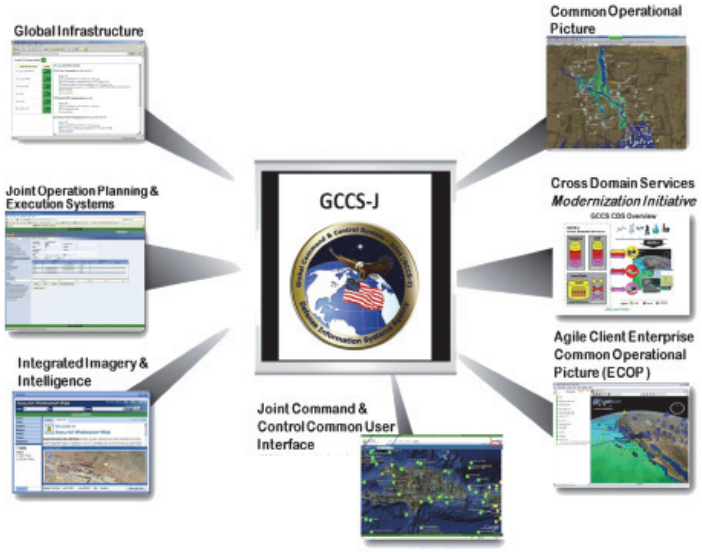
- The Program Office added U.S. Cyber Command (USCYBERCOM) and supporting command Joint Deployment Training Center (JDTC) to the currently fielded JOPES v4.3 using MRs. JITC operationally tested JOPES v4.3.0.1 MR and JOPES v4.3.0.2 MR in FY18, and found them operationally effective and operationally suitable.
- JITC and the DISA Red Team conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) and Adversarial Assessment (AA) of v4.2.0.3 MR4 from January through March 2018. The cybersecurity testing was not adequate for DOT&E to determine JOPES v4.2.0.3 MR4 survivability in a cyber-contested environment. DISA agreed to plan and execute additional cybersecurity testing on JOPES to fully characterize the cyber survivability of the system.

System

GCCS-J consists of hardware, software (both commercial off-the-shelf and government off-the-shelf), 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. Its client/server architecture uses open systems standards and government-developed military planning software. Global and JOPES are the two baseline systems that comprise GCCS-J.

Global (Force Protection, Situational Awareness, and Intelligence applications)

- Global v4.3.0.13 is currently fielded worldwide.
- Global v6.0.0.9 and Agile Client v5.2.0.2 are currently fielded at a limited number of sites. DISA is developing Global v6.0.1.0 to replace Global v4.3.0.13.



- Global v6.0.1.0 is intended to provide back-end services, databases, and system administration functions. Agile Client v5.2.0.2 is intended to provide visualization and presentation of GCCS-J mission applications and functionality to the user. The Program Office is using agile development to evolve Global v6.0.1.0, releasing incremental MR packages to expand capabilities available to the warfighter.
- DISA is developing GCCS-Joint Enterprise (JE) to replace Global v4.3.0.14, Global v6.0.1.0, and Agile Client Release v5.2.0.2. GCCS-JE is intended to provide situational awareness using a data subscription service, ending the current dependence on a local software instantiation of GCCS-J Global. The Services and Combatant Commands will need to modify their command and control systems to interface with the new GCCS-JE data service.

JOPES (Force Employment, Projection, Planning, and Deployment/Redeployment applications)

- JOPES v4.3.0.2 is the currently fielded version.
- DISA is developing Joint Planning and Execution System (JPES) to replace the JOPES v4.3 baseline. JPES provides all of the functionality of the current JOPES in a modernized architecture.

Mission

Joint Commanders utilize the GCCS-J to accomplish command and control.

Global

- Commanders use Global to:

- Link the National Command Authority to the Joint Task Force, Component Commanders, and Service-unique systems at lower levels of command
- Process, correlate, and display geographic track information integrated with available intelligence and environmental information to provide the user a fused battlespace picture
- Provide integrated imagery and intelligence capabilities (e.g., battlespace views and other relevant intelligence) into the common operational picture and allow commanders to manage and produce target data using the joint tactical terminal
- Provide a missile warning and tracking capability

• Air Operations Centers use Global to:
- Build the air picture portion of the common operational picture and maintain its accuracy
- Correlate or merge raw track data from multiple sources
- Associate raw electronics intelligence data with track data
- Perform targeting operations

JOPES

• Commanders use JOPES to:
- Translate policy decisions into operations plans that meet U.S. requirements to employ military forces
- Support force deployment
- Conduct contingency and crisis action planning

Major Contractors

• Government Integrator: DISA – Fort Meade, Maryland
• Software Developers:
- Northrop Grumman – Arlington, Virginia
- Leidos – Arlington, Virginia
- InterImage – Arlington, Virginia
- CSRA – Falls Church, Virginia

Activity

Global

• The Program Office conducted and JITC observed and reported on the following:
- Level I operational test of Global v6.0.0.6 MR at the DISA laboratory from November 21 to December 2017
- Level I operational test of Global v6.0.0.8 MR at the DISA laboratory from March 7 – 12, 2018
- Level I operational test of Global v4.3.0.12 at the DISA laboratory December 12 – 13, 2017

• The Program Office approved the following releases in FY18:
- Global v6.0.0.6 MR for release on March 5, 2018
- Global v6.0.0.7 MR for release on March 12, 2018
- Global v6.0.0.8 MR for release on April 4, 2018
- Global v6.0.0.9 MR for release on June 20, 2018
- Global v4.3.0.13 MR for release on August 28, 2018
- GCCS-J v5.2.0.2 plug-in on September 10, 2018

• JITC conducted the GCCS-J v6.0.1.0 level II operational test at U.S. Central Command and U.S. Indo-Pacific Command September 17 – 28, 2018, in accordance with a DOT&E-approved test plan.

JOPES

• JITC and the DISA Red Team conducted cybersecurity testing on v4.2.0.3 MR4 remotely from Fort Huachuca, Arizona, and Chambersburg, Pennsylvania. The DISA Red Team failed to conduct the test in accordance with the DOT&E-approved test plan, resulting in an inadequate test. JITC and the DISA Red Team conducted the CVPA, from January 22 through February 1, 2018, and the AA, from February 19 through March 1, 2018, against the primary JOPES server located in the Pentagon, Washington, D.C.

• JITC and the Program Office conducted the following:
- An operational test of JOPES v4.3.0.1 at the Fort George G. Meade (FGGM) Lab, Maryland, from April 16 through May 2, 2018
- An operational test of JOPES v4.3.0.2 at the FGGM Lab from August 7 – 10, 2018

Assessment

Global

• The Program Office added functionality to address operational needs in the intelligence, targeting capabilities, and chemical, biological, radiological, and nuclear defense mission areas and corrected 56 defects in Global v6.0.0.6 MR. The release met all but one of the Key Performance Parameters. A new capability, designed to allow the web-based Joint Warning and Reporting Network (JWARN) application to be displayed using Agile Client, failed during testing. Users can still complete their mission using the standard JWARN web display.

• The Program Office added Java Runtime Environment (JRE) 8 to Global v4.3.0.12, replacing non-supported JRE versions in the GCCS-J v4.3 baseline. Testers successfully completed validation of JRE 8 and regression testing of capability areas that could be affected by this upgrade.

• GCCS-J v6.0.1.0 level II operational test results are pending the analysis of collected data.

• JITC is planning to conduct a CVPA and AA of the operational Global v6.0.1.0 at a Combatant Command site in 4QFY19, following system deployment.

JOPES

• JOPES cybersecurity testing in FY18 was not adequate for DOT&E to determine v4.2.0.3 MR4 survivability in a cyber-contested environment. During the AA, the DISA Red Team completed only two of seven planned attacks and did not conduct any advanced attacks. DISA agreed to plan and execute advanced adversarial attacks against JOPES to fully characterize the survivability of the system.

• JOPES v4.3.0.1 is operationally effective and operationally suitable. The Program Office corrected six defects in this

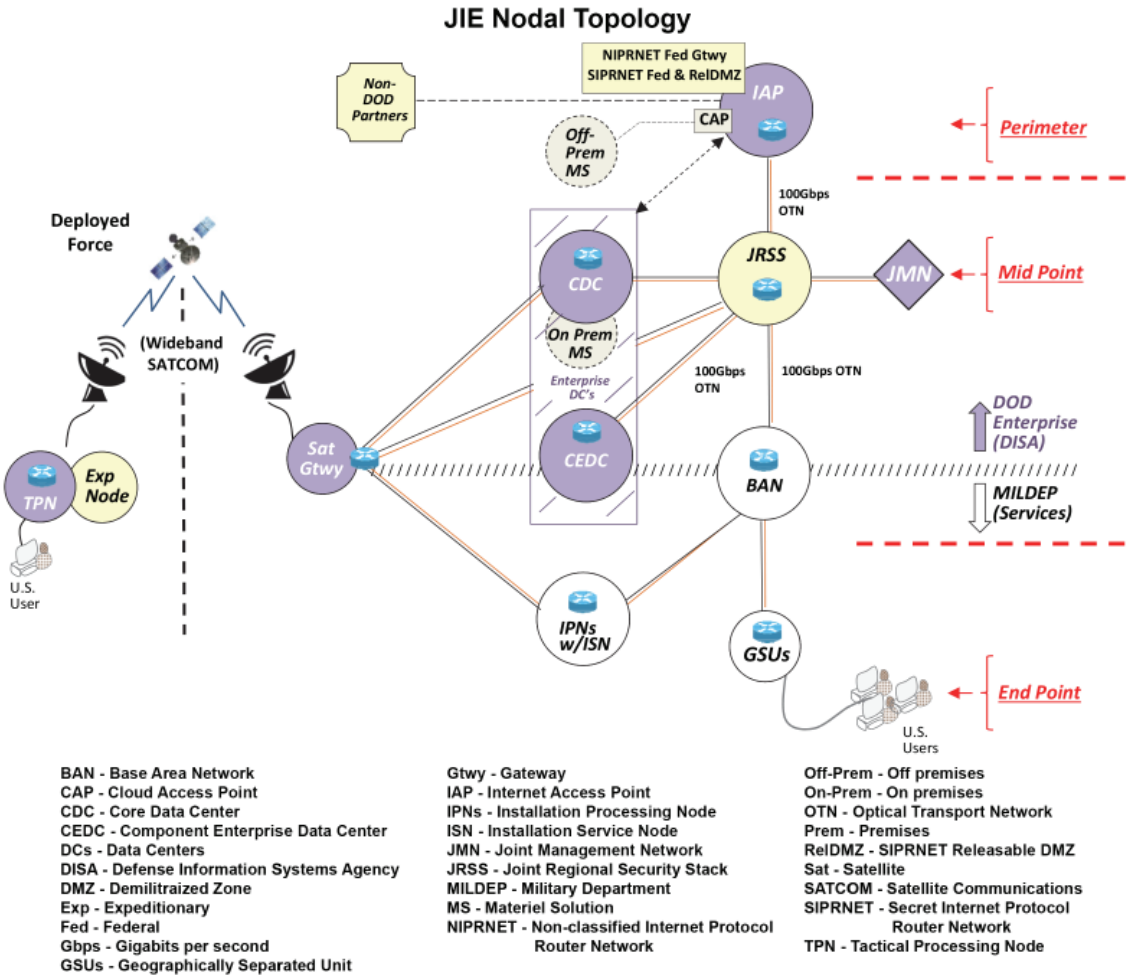
release. Testers discovered one low priority defect with the JOPES v4.3.0.1 software. Users identified an operational workaround for the new defect.

- JOPES v4.3.0.2 is operationally effective and operationally suitable. The Program Office added the USCYBERCOM and supporting command JDTC to the JOPES system, each with its own operation plan series. Operational testing showed that USCYBERCOM and JDTC could create operation plans and force requirements; source, update, and validate force requirements; and schedule and move forces. JITC successfully completed regression testing for 13 of 17 available external interfaces.

Recommendation

1. DISA should conduct a CVPA and AA on the operational version of Global v6.0.1.0, in accordance with DOT&E-approved cybersecurity test guidelines.

Joint Information Environment (JIE)



Executive Summary

- The Joint Information Environment (JIE) Executive Committee (EXCOM) continued to provide guidance and direct the implementation of the funded initiatives supporting the 10 JIE capability objectives and integration efforts for the DOD.
- The cybersecurity effectiveness of the Joint Regional Security Stack (JRSS), a component of JIE, calls into question the current JIE cybersecurity approach. For reporting on the JRSS, see the separate article on page 45.
- The USD(A&S) approved the Defense Enterprise Office Solution (DEOS) acquisition strategy in June 2018.
- The Deputy SECDEF intends to designate the Secretary of the Air Force as the DOD Executive Agent for Mission Partner Environment (MPE) capabilities in FY19.
- The Air Force is conducting a programmatic and technical assessment of the MPE portfolio and will assume responsibility in FY19.

Capability and Attributes

- In August 2012, the Joint Chiefs of Staff (JCS) approved the JIE concept as a secure environment, comprising a single security architecture, shared information technology (IT) infrastructure, and enterprise services.
- JIE consists of multiple subordinate programs, projects, and initiatives managed and implemented by the Defense Information Systems Agency (DISA) and the Military Services.
- In January 2017, the JIE EXCOM approved the following 10 JIE capability objectives:
  - Modernize Network Infrastructure, to include optical carrier upgrades, multi-protocol label switching, satellite communication gateway modernization, and Internet Protocol (IP) version 6 implementation
  - Enable Enterprise Network Operations, to include establishing global and regional operations centers, a JIE

out-of-band management network, and converging IT service management solutions
- Implement Regional Security, to include the JRSS, and the Joint Management System for JRSS
- Provide MPE-Information System (IS) for coalition/ partner information sharing, to include virtual data centers, services, and Mission Partner Gateways
- Optimize Data Center Infrastructure
- Implement Consistent Cybersecurity Architecture/ Protections, to include DOD enterprise perimeter protection, endpoint security, mobile endpoint security, data center security, cybersecurity situational awareness analytic capabilities, and identity and access management (previously referred to as the Single Security Architecture in older JIE documentation)
- Enhance Mobility for unclassified and classified capabilities
- Standardized IT Commodity Management, to include enterprise software agreements, license agreements, hardware agreements, and IT asset management
- Establish End-User Enterprise Services, to include the Enterprise Collaboration and Productivity Services (ECAPS) and converged voice and video services over IP
- Provide Hybrid Cloud Computing Environments, to include Commercial Cloud, Cloud Access Points, and milCloud

- The JCS envisions JIE as a shared information technology construct for DOD to reduce costs, improve and standardize physical infrastructure, increase the use of enterprise services, improve IT effectiveness, and centralize the management of network defense. The Joint Staff specifies the following enabling characteristics for JIE capability objectives:
  - Transition to centralized data storage
  - Rapid delivery of integrated enterprise services (such as email and collaboration)
  - Real-time cybersecurity awareness
  - Scalability and flexibility to provide new services
  - Use of common standards and operational techniques
  - Transition to the JIE Cybersecurity Architecture
- JIE is not a program of record and does not have a traditional milestone decision authority, program executive organization, and project management structure that would normally be responsible for the cost, schedule, and performance of a program.
- The DOD Chief Information Officer (CIO) is the overall lead for JIE efforts with support from the JIE EXCOM – chaired by the DOD CIO, U.S. Cyber Command, and Joint Staff J6. The EXCOM provides JIE direction and objectives. DISA is the principal integrator for JIE capabilities and testing.

Activity

JIE
- For reporting on the JRSS, see the separate article on page 45.
- The JIE EXCOM continued to provide guidance and direct the implementation of the funded initiatives supporting the 10 JIE capability objectives and integration efforts for the DOD.
- The DOD CIO, Joint Staff, Combatant Commands, Services, and DOD Agencies continued efforts to collaboratively develop and build the JIE Cybersecurity Architecture.

ECAPS
- In 2018, the DEOS (ECAPS capability set 1) Program Management Office (PMO) and the Joint Interoperability Test Command began efforts to draft a DEOS Test and Evaluation Master Plan (TEMP).
- The USD(A&S) approved the DEOS acquisition strategy in June 2018, and, in coordination with the DOD CIO, is refining the ECAPS capability sets 2 and 3 requirements evaluation through 1QFY19.

MPE
- The Deputy SECDEF intends to designate the Secretary of the Air Force as the DOD Executive Agent for MPE and the DOD CIO as the Principal Staff Assistant for MPE in FY19.
- The intent is to rationalize and modernize the overall MPE portfolio of command and control, and intelligence information sharing capabilities.
- The MPE-IS initiative is intended to consolidate and recapitalize 28 physical Combined Enterprise Regional Information Exchange Systems (CENTRIXS) across the DOD, providing virtualized enduring and episodic MPE-IS services tailored to meet mission partner information sharing needs.
- The Air Force is conducting a programmatic and technical assessment of the MPE portfolio and will assume responsibility in FY19.

Assessment
- The DOD CIO, DISA, and Services intend to achieve the JIE goals through implementation of initiatives aligned under the JIE EXCOM-approved capability objectives.
- The JIE EXCOM has started efforts to monitor JIE capability performance factors; however, the EXCOM does not place high enough priority on developmental and operational test results to inform decisions.
- The cybersecurity effectiveness of the JRSS, a component of JIE, calls into question the current JIE cybersecurity approach.

Recommendations

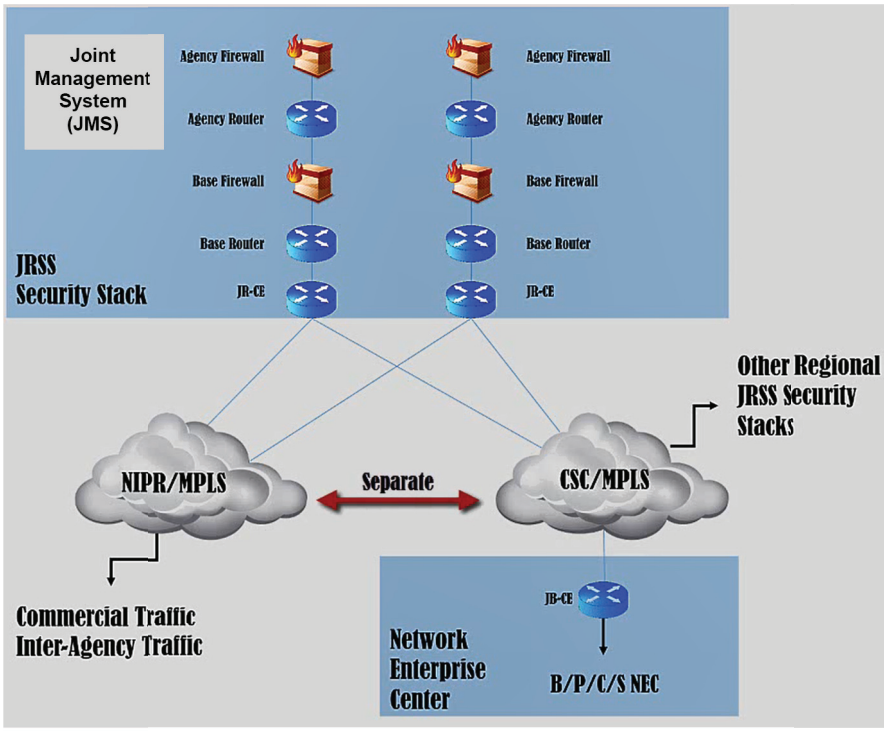
The DOD CIO, JIE EXCOM, Services, and Director of DISA should:

1. Use operational test information, such as that from the recent JRSS operational assessments, to inform JIE decisions.
2. Update the MPE-IS Test and Evaluation Strategy upon completion of the Air Force programmatic and technical assessment.
3. Update the DEOS TEMP for approval once the PMO awards a contract and updates the master schedule.
4. Develop a Test and Evaluation Strategy for ECAPS and more generally for each JIE capability objective with funded initiatives.
5. Conduct thorough cybersecurity operational testing of all JIE capabilities, employing current cybersecurity testing guidance and policy.

Joint Regional Security Stack (JRSS)

Executive Summary

- In March 2018, the Joint Interoperability Test Command (JITC) conducted an operational assessment (OA) that demonstrated that the Joint Regional Security Stack (JRSS) Version 1.5, as utilized by the Air Force, is unable to help network defenders protect the network against operationally realistic cyber-attacks. The JRSS showed little improvement from the OA conducted in July 2017.
- The following factors affected the OA results: 1) the difficulty inherent in integrating disparate, complex commercial technologies into a functional system of systems; 2) although improving, training remains insufficient, and; 3) standard operating procedures (SOPs) remain immature.
- Since the OA, JRSS has continued to experience operational and technical problems, including high latency that adversely impacted the Joint Service Provider, Army Materiel Command (AMC) and U.S. Southern Command (SOUTHCOM) and delayed migration of additional users associated with those components.
- Over the last 2 years, the JRSS Program Manager has continued to address persistent problems with JRSS; however, it remains unclear whether the very high volume of data designed to traverse each JRSS can be managed effectively.
- Due to the poor JRSS performance, the JRSS Senior Advisory Group (SAG) and Executive Committee for Joint Information Environment (JIE EXCOM) delayed the JRSS migration for U.S. Central Command, Southwest Asia (Army), and the Marine Corps, and deferred JRSS deployments for SIPRNET until FY19.
- On May 10, 2018, the JIE EXCOM conducted a Strategic Review of JRSS. The JIE EXCOM approved an adjustment to migration schedules and redirected resources to mitigate JRSS performance, training, and operational process issues based on testing results and operational lessons learned. Operational assessments are scheduled for January and July 2019, and every 6 months until the IOT&E, tentatively scheduled for FY20
- On June 28, 2018, the JIE EXCOM approved the proposed timeline to implement actions across these lines of effort: training, migration, capability, JRSS deployments for SIPRNET, and operational governance. Efforts are ongoing by the JRSS Program Manager and stakeholders to correct findings from previous test events, with status reports provided monthly to the JIE EXCOM.



B/P/C/S - Base, Post, Camp, Station
CSC - Carrier Supporting Carrier
JB-CE - Joint Base - Customer Edge
JR-CE - Joint Router- Customer Edge
JRSS - Joint Regional Security Stack
MPLS - Multi-Protocol Label Switching
NEC - Network Enterprise Center
NIPR - Non-classified Internet Protocol Router Network

- Defense Information Systems Agency (DISA) Global Operations Command reported that they require 17 additional government positions (e.g., engineers, administrators, development operations manager, and project managers) at DISA, Global Operations Command East (DGOC-E) to cover manning shortfalls with plans to be properly manned by July 2019.
- The Army (Regional Cyber Center-Continental United States) could not certify that they had sufficient manning to assume the JRSS mission.
- Fourteen JRSSs are currently deployed on the NIPRNET, (23 are planned). No JRSSs are currently deployed on SIPRNET (25 are planned).

Capabilities and Attributes

- As a component of the JIE, JRSS is a suite of equipment intended to perform firewall functions, intrusion detection and prevention, enterprise management, and virtual routing and forwarding, as well as provide a host of network security capabilities. Neither JIE nor JRSS is a program of record.

- The JRSS is intended to centralize and standardize network security into regional architectures instead of locally distributed, non-standardized architectures at different levels of maturity and different stages in their lifecycle at each military base, post, camp, or station.
- Each JRSS includes many racks of equipment, which allow DOD components to intake, process, and analyze very large network data flows.
- The Services and DISA intended to deploy JRSS on both the NIPRNET (N-JRSS) and SIPRNET (S-JRSS).
- DISA is the designated approving and certification authority for both JRSS equipment and multiprotocol label switching (MPLS) equipment.
- MPLS is part of a modernization effort to upgrade the bandwidth capacity of the Defense Information Systems Network (DISN). DISA will implement MPLS/JRSS-enabling technology to increase network speed and manage the larger traffic flows.
- A key component of JRSS is the Joint Management System (JMS) that provides centralized management of cybersecurity services required for DOD Information Network (DODIN) operations and defensive cyber operations.

Mission

DISA and the Services intend to use JRSS to enable DOD cyber defenders to continuously monitor and analyze the DODIN for increased situational awareness to minimize the effects of cyber threats while ensuring the integrity, availability, confidentiality, and non-repudiation of data.

Vendors

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

OEM	OEM Location
A10	San Jose, California
Argus	Houston, Texas
Axway	Phoenix, Arizona
Bivio	Pleasanton, California
BMC	Houston, Texas
Bro	Berkeley, California
Cisco	San Jose, California
Citrix	Fort Lauderdale, Florida
CSG International	Alexandria, Virginia
Dell	Round Rock, Texas
EMC	Santa Clara, California
F5	Seattle, Washington
Fidelis	Bethesda, Maryland
Gigamon	Santa Clara, California
HP	Palo Alto, California
IBM	Armonk, New York
InfoVista	Ashburn, Virginia
InQuest	Arlington, Virginia
Juniper	Sunnyvale, California

OEM	OEM Location
Micro Focus	Rockville, Maryland
Microsoft	Redmond, Washington
Niksun	Princeton, New Jersey
OPSWAT	San Francisco, California
Palo Alto	Santa Clara, California
Quest	Aliso Viejo, California
Raritan	Somerset, New Jersey
Red Hat	Raleigh, North Carolina
Red Seal	Sunnyvale, California
Riverbed	San Francisco, California
Safenet	Belcamp, Maryland
Splunk	San Francisco, California
Symantec	Mountain View, California
Trend Micro	Irving, Texas
Van Dyke	Albuquerque, New Mexico
Veeam	Columbus, Ohio
Veritas	Mountain View, California
VMWare	Palo Alto, California

Activity

- JITC conducted an OA of the JRSS Version 1.5 in March 2018.
- On May 10, 2018, the JIE EXCOM approved an adjustment to migration schedules and redirected resources to mitigate JRSS performance, training, and operational process issues based on testing results and operational lessons learned.
- On June 28, 2018, the JIE EXCOM approved the JRSS Strategic Review, which delayed N-JRSS migrations and deferred S-JRSS migrations until FY19. The program manager and stakeholders have undertaken efforts to correct findings from previous test events and make improvements along five lines of effort: training, migration, capability, S-JRSS, and governance.
- In August 2018, JITC hosted a 5-day JRSS Lab-based Exercise (LBE) to prepare the Army, Air Force, and Navy for the planned 2019 operational testing, to facilitate hands-on learning for other Services prior to their migration behind JRSS, and to provide an opportunity for DOD components to

exercise their SOPs. Thirteen components participated in the LBE and several others observed.

Assessment

- The March 2018 OA demonstrated that the JRSS, as the Joint Regional Security Stack (JRSS) Version 1.5, as utilized by the Air Force, is unable to help network defenders protect the network against operationally realistic cyber-attacks. JRSS performed poorly, and showed little improvement from the July 2017 OA. JRSS operators did not detect the Air Force 177th Information Aggressor Squadron as it portrayed a cyber adversary attacking the Enclave Control Node logically situated behind JRSS defenses. The following shortfalls contributed to poor JRSS cybersecurity performance:
  - It is inherently difficult to effectively manage the very large amount of data designed to traverse each JRSS.
  - Although the JRSS uses commercial off-the-shelf technologies, JRSS operator training still lags behind JRSS deployment, and is not sufficient to prepare operators to effectively integrate and configure the complex suite of JRSS hardware and associated software.
  - The Services, DISA, and U.S. Cyber Command have not codified JRSS joint tactics, techniques, and procedures to ensure unity of defensive effort and enhance defensive operations.
  - DISA Global and the Army have insufficient manning to properly operate JRSS.

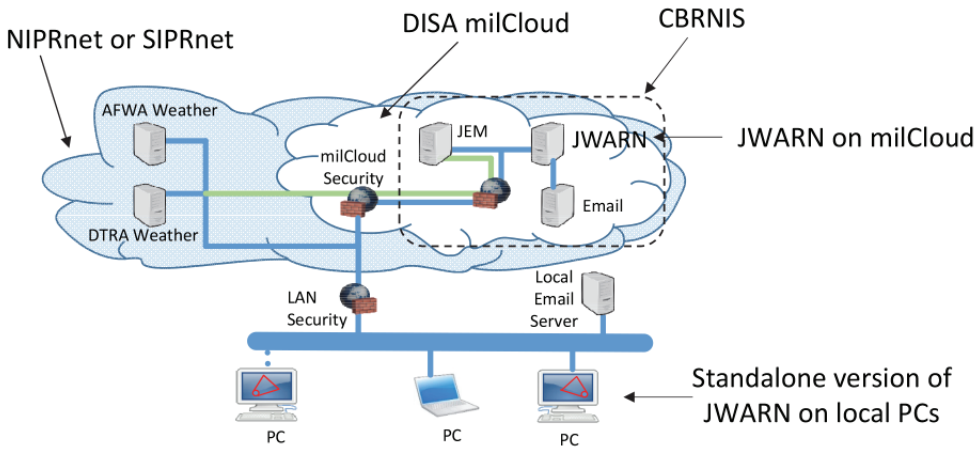
Recommendations

1. The DOD Chief Information Officer (CIO) and the Services should discontinue deploying JRSSs until the system demonstrates that it is capable of helping network defenders to detect and respond to operationally realistic cyber-attacks.
2. The JRSS Program Manager, DISA Global, and the Services should:
   - Use operationally realistic test results to improve current JRSS configurations, training, and procedures, and to inform future N-JRSS and S-JRSS migration decisions
   - Address problems discovered during the most recent OA and from previous testing before proceeding to other tests
   - Include the Army, Navy, and Marine Corps JRSS configurations in future operational tests
3. The DOD CIO and the Services should consider the possibility that the data flow designed to traverse each JRSS may be too large to enable secure data management, and if that is the case, refine the JRSS deployment plans to reduce the required data flow through each JRSS.
4. DISA and the Services should ensure sufficient trained personnel are available to support JRSS migration schedules.
5. DISA and the Services should conduct routine cyber assessments of deployed JRSSs, using a threat representative Persistent Cyber Opposing Force, to discover and address critical cyber vulnerabilities.

Joint Warning and Reporting Network (JWARN)

Executive Summary

- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted operational testing of the Joint Warning and Reporting Network (JWARN) Increment 2 hosted on the Defense Information Systems Agency (DISA) Military Cloud (milCloud) between January 22, 2018, and February 3, 2018, at Eglin AFB, Florida.
- JWARN Increment 2 hosted on milCloud and standalone computers is operationally effective to support chemical, biological, radiological, and nuclear (CBRN) situational awareness and planning. Operators employing JWARN are able to provide information to support time critical operational decisions.
- JWARN Increment 2 is operationally suitable when employed in conjunction with a standalone version of JWARN for continuity of operations, and survivable in a cyber-contested environment.



AFWA - Air Force Weather Agency
CBRN - Chemical, Biological, Radiological, Nuclear
CBRNIS - CBRN Information System
DISA - Defense Intelligence Systems Agency
DTRA - Defense Threat Reduction Agency
JEM - Joint Effects Model
JWARN - Joint Warning and Reporting Network
LAN - local area network
NIPRNET - Non-classified Internet Protocol (IP) Router Network
PC - personal computer
SIPRNET - Secret Internet Protocol Router Network

System

- JWARN is a software application that integrates CBRN data into joint and Service command and control systems for battlespace situational awareness. It incorporates and displays sensor alert information and CBRN observation reports on the Common Operational Picture, and generates a warning message to units.
- JWARN replaces the manual processes of incident reporting and hazard plot generation, and warning of affected operational forces. The application is based on the standards outlined in NATO Allied Technical Publication 45, "Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological, and Nuclear Incidents (Operators Manual)."

Mission

A unit equipped with JWARN provides analysis of potential or actual CBRN hazard areas based on operational scenarios or sensor and observer reports, identifies affected units and operating areas, and provides warning information to support commanders' force protection and operational decisions.

Major Contractor

Northrop Grumman Mission Systems – Orlando, Florida

Activity

- AFOTEC conducted initial operational testing of JWARN Increment 2 on the DISA milCloud and local computers from January 22, 2018, to February 3, 2018, at Eglin AFB, Florida. The Army Threat Systems Management Office conducted an Adversarial Assessment during the operational test.
- AFOTEC conducted the operational test in accordance with the DOT&E-approved test plan. The test was adequate to assess the operational effectiveness, operational suitability, and cybersecurity of JWARN hosted on milCloud and the continuity of operations plan associated with the use of JWARN Increment 2 operating on a local computer.
- The Joint Program Executive Office for Chemical, Biological, Radiological, and Nuclear Defense authorized full deployment of JWARN Increment 2 Requirements Definition Package-2 Capability Drop 2.1 on milCloud on August 17, 2018.

Assessment

- JWARN Increment 2 hosted on milCloud is operationally effective to support CBRN situational awareness to support operational decision-making and planning.
- JWARN Increment 2 met and in some cases exceeded the operational requirement for timely warning of downwind units at risk.
- JWARN Increment 2 is operationally suitable when employed in conjunction with a standalone version of JWARN for continuity of operations. JWARN demonstrated the required 96 percent probability of successful mission completion for warning and reporting missions.
- JWARN is survivable against cyber-attacks. Hostile cyber activity during testing had no significant effect on the unit equipped with JWARN ability to accomplish its mission.

Recommendations

None.

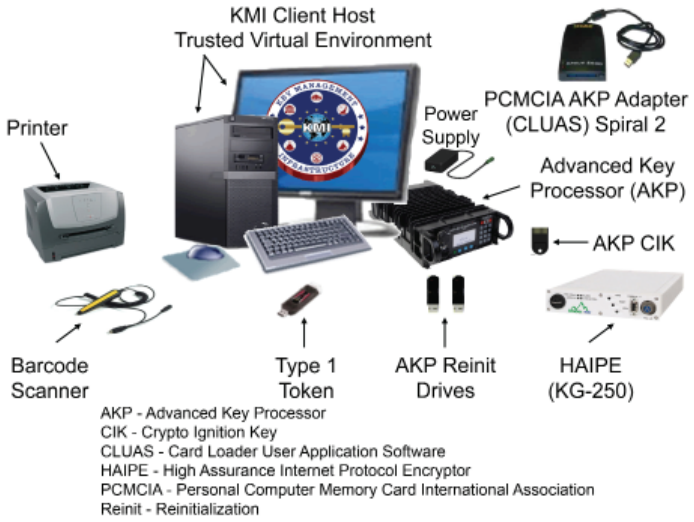
Key Management Infrastructure (KMI) Increment 2

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted an Operational Assessment (OA) of Key Management Infrastructure (KMI) Increment 2 Spiral 2, Spin 3 capabilities in October/November 2017.
- DOT&E published its KMI Spiral 2, Spin 3 OA Report in March 2018 that found system stability, usability, and maturity continue to improve. However, some high-priority defects remained in the KMI Spiral 2, Spin 3 software. Sustainment, KMI Operations staffing, KMI Test Infrastructure, and configuration management problems prevent KMI from being operationally suitable for long-term sustainment.
- The USD(A&S) delegated Milestone Decision Authority for the KMI Increment 2 program to the National Security Agency (NSA) Senior Acquisition Executive in March 2018.
- JITC conducted an FOT&E of KMI Increment 2 that included Spin 3 capabilities in April/June 2018. The FOT&E examined KMI regression capabilities, enhancements to existing functionality, the NATO infrastructure, asymmetric and symmetric key ordering, and sustainment processes.
- During the KMI Increment 2 FOT&E, the KMI Spin 3 capabilities did not perform successfully. JITC did not fully test the NATO capabilities due to a high-priority finding that halted the planned NATO account transition. Also, a large number of high-priority system findings led the KMI Program Management Office (PMO) to fix the problems and plan to re-test the FOT&E in January/February 2019. DOT&E will make operational effectiveness, suitability, and survivability/cybersecurity determinations after the FOT&E re-test.

System

- KMI will replace the legacy Electronic Key Management System (EKMS) to provide a means for securely ordering, generating, producing, distributing, managing, and auditing cryptographic products (e.g., encryption keys, cryptographic applications, and account management tools).
- KMI consists of core nodes that provide web operations at sites operated by the NSA, as well as individual client nodes distributed globally, to enable secure key and software provisioning services for the DOD, the Intelligence Community, and other Federal agencies.
- KMI combines substantial custom software and hardware development with commercial off-the-shelf (COTS) computer components. The custom hardware includes an Advanced Key Processor for autonomous cryptographic key generation and a Type 1 user token for role-based user authentication.



The COTS components include a client host computer with monitor and peripherals, printer, and barcode scanner.

- The NSA is delivering KMI Increment 2 in two spirals with Spiral 2 having three development spins. The NSA previously delivered KMI Increment 2, Spiral 1 and Spiral 2, Spin 1 and Spin 2. KMI Increment 2 Spiral 2, Spin 3 is the final capability delivery for the increment.

Mission

- Combatant Commands, Services, DOD agencies, other Federal agencies, coalition partners, and allies will use KMI to provide secure and interoperable cryptographic key generation, distribution, and management capabilities to support mission-critical systems, the DOD Information Network, and initiatives such as Cryptographic Modernization.
- Service members will use KMI cryptographic products and services to enable security services (confidentiality, non-repudiation, authentication, and source authentication) for diverse systems such as Identification Friend or Foe, GPS, and Advanced Extremely High Frequency Satellite System.

Major Contractors

- Leidos – Columbia, Maryland (Spiral 2 Prime)
- General Dynamics Information Technology – Dedham, Massachusetts
- SafeNet – Belcamp, Maryland
- L3 Communications – Camden, New Jersey

Activity

- JITC conducted an OA of KMI Increment 2 Spiral 2, Spin 3 capabilities in October/November 2017 in accordance with a JITC-approved test plan.
  - JITC approved the test plan in accordance with delegated authority in the DOT&E policy memorandum, "Guidelines for OT&E of Information and Business Systems," September 14, 2010.
  - To support agile acquisition and fielding approaches, DOT&E delegates test plan approval on an assessment of moderate or low overall risk to mission accomplishment of new software integration. DOT&E and JITC assessed the KMI Spiral 2, Spin 3 OA as low risk.
- The USD(AT&L) published the KMI Spiral 2, Spin 2 limited fielding Acquisition Decision Memorandum in November 2017 that directed the NSA and the Services to resolve the long-term sustainability problems to include staffing levels, training infrastructure availability, adequacy of spares, and help desk operations prior to the Increment 2 FOT&E.
- The USD(A&S) delegated Milestone Decision Authority for the KMI Increment 2 program to the NSA Senior Acquisition Executive in March 2018.
- JITC conducted a KMI Spiral 2, Spin 3 defect resolution verification test in January 2018.
- DOT&E published its KMI Spiral 2, Spin 3 OA Report in March 2018.
- JITC conducted an FOT&E of KMI Increment 2 capabilities in April/June 2018 in accordance with a DOT&E-approved test plan. Due to KMI Spin 3 capabilities performance and configuration management problems in FOT&E, the KMI PMO intends to re-test the Increment 2 FOT&E in January/February 2019.
- The KMI PMO changed the estimated Increment 2 Full Deployment Decision to late April 2019.

Assessment

- The KMI Spiral 2, Spin 3 OA indicated system stability, usability, and maturity continue to improve. However, some high-priority defects remained in the KMI Spiral 2, Spin 3 software. Sustainment, KMI Operations staffing, KMI Test Infrastructure, and configuration management problems prevent KMI from being operationally suitable for long-term sustainment.
- JITC evaluated all of the new Spin 3 capabilities during the OA, and all KMI capabilities in previous releases continued to function to support the operational missions. JITC discovered 15 high-priority defects during the OA.
- The Increment 2 FOT&E examined KMI regression capabilities, enhancements to existing functionality, the NATO infrastructure, asymmetric and symmetric key ordering, and sustainment processes.
- The KMI Spin 3 capabilities did not perform successfully in FOT&E. JITC did not fully test the NATO capabilities due to a high-priority finding that halted the planned NATO account transition. The large numbers of high-priority system findings led the KMI PMO to fix the problems and plan the future re-test for the Increment 2 FOT&E. DOT&E will make operational effectiveness, suitability, and survivability/cybersecurity determinations after the FOT&E re-test.
- The NSA KMI Operations continues to surge manning for operational test events and has reoccurring staffing shortages that affect long-term system sustainment.
- The KMI PMO now has an executable schedule to fix and operationally test/re-test the remaining Increment 2 capabilities, including system maintenance releases and Windows 10 client integration.

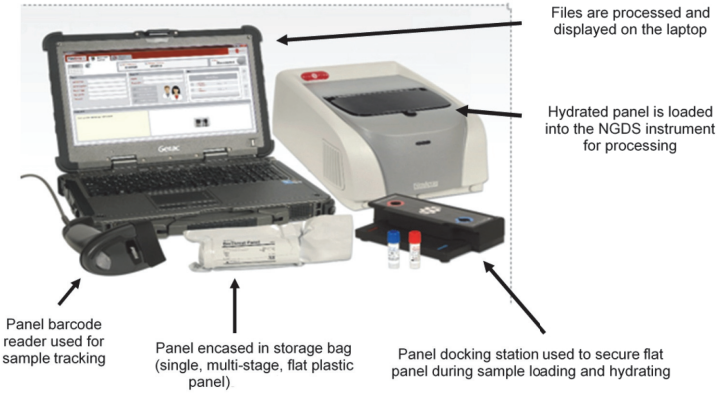
Recommendations

- The KMI PMO should:
  1. Continue to resolve all high-priority defects and verify acceptability on the integrated Windows 10 KMI client to users prior to Increment 2 FOT&E re-test and full deployment.
  2. Maintain the KMI Test Infrastructure to the same degree as the operational environment.
- The NSA KMI Operations should:
  1. Improve KMI configuration management and long-term sustainment.
  2. Reassess KMI Operations staffing to ensure that it can support all existing and planned new capabilities, networks, sites, and users.

Next Generation Diagnostic System (NGDS) Increment 1

Executive Summary
- The Next Generation Diagnostics System (NGDS) is a polymerase chain reaction analytical instrument to aid in the diagnosis of biological warfare agent (BWA)-related illnesses and environmental sample analysis to identify the presence of BWA in the operational environment.
- The NGDS is operationally effective for the analysis of environmental samples to confirm the presence of BWAs to support force protection and situational awareness.
- The NGDS is operationally effective for analysis of clinical samples to support the diagnosis and treatment of symptomatic patients.
- The NGDS is operationally suitable. The system exceeds reliability and availability requirements, is easy to use, and has a smaller logistics footprint than the system it replaces.
- The NGDS is survivable against cyber threats.

System
- The NGDS is a U.S. Food and Drug Administration (FDA) cleared commercial off-the shelf diagnostic device manufactured by BioFire Defense, LLC.
- Two consumable panels are available for use with the NGDS: the Warrior Panel to identify the presence of BWA in clinical samples and the Sentinel Panel to identify the presence of BWA in environmental samples.



Mission
Army, Navy, and Air Force units equipped with the NGDS analyze clinical and environmental samples to identify the presence of BWAs and infectious diseases to aid in medical diagnosis and provide situational awareness to support force protection decisions.

Major Contractor
BioFire Defense, LLC – Salt Lake City, Utah

Activity
- The U.S. Army Medical Research Institute of Infectious Disease at Fort Detrick, Maryland, and the Battelle Eastern Science and Technology Center, Aberdeen, Maryland, conducted combined developmental/operational testing of the Sentinel Panel and BioFire FilmArray device from April 2017 to February 2018.
- The combined developmental/operational testing was conducted in accordance with DOT&E-approved test plans.
- DOT&E submitted the NGDS Operational Test and Evaluation Report to Congress in May 2018.

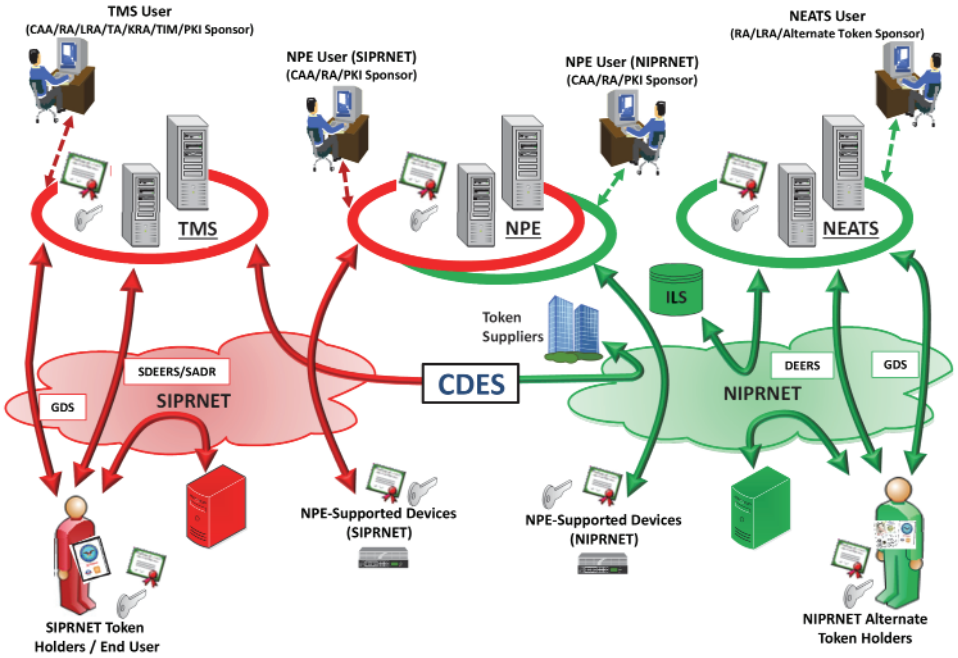
Assessment
- The NGDS is operationally effective for deployable medical units to analyze clinical samples to aid in the diagnosis of anthrax, plague, tularemia, Q fever, and the hemorrhagic fevers caused by Ebola and Marburg, in response to a suspected or confirmed bioterrorism events or outbreak.
- The NGDS is operationally effective for the analysis of environmental samples to confirm the presence of BWAs to provide timely and accurate information to improve situational awareness and support force protection decisions.
- The NGDS is operationally suitable. It exceeds mission reliability and operational availability requirements, requires less support equipment thus reducing the operational footprint from the system it replaces. The NGDS is easy to operate and requires minimal operator hands-on time.
- The NGDS is survivable against cyber threats.

Recommendations
None.

Public Key Infrastructure (PKI) Increment 2

Executive Summary

- DOT&E published the Public Key Infrastructure (PKI) Increment 2, Spiral 3 FOT&E Report in December 2017 based on the test that the Joint Interoperability Test Command (JITC) conducted in August/September 2017.
  - Spiral 3 is operationally effective and suitable for day-to-day operations, but not suitable for long-term sustainment.
  - The National Security Agency (NSA) Senior Acquisition Executive (SAE) approved DOD-wide fielding of Spiral 3 in October 2018.
- The USD(A&S) delegated Milestone Decision Authority for the DOD PKI Increment 2 program to the NSA in March 2018.
- JITC began assessments of PKI Increment 2, Spiral 4 in 2018. In late July 2018, the PKI Program Management Office (PMO) delayed the Operational Assessment (OA) of the PKI Increment 2, Spiral 4 capabilities until November/ December 2018 to resolve high-priority system defects and integration problems.



System

- DOD PKI provides for the generation, production, distribution, control, revocation, recovery, and tracking of public key certificates and their corresponding private keys. By controlling the distribution of encryption, identity, signing, and device certificates and keys, DOD PKI helps ensure only authorized individuals and devices have access to networks and data, which supports the secure flow of information across the DOD Information Network as well as secure local storage of information.
- The NSA deployed PKI Increment 1 on the NIPRNET with access control provided through Common Access Cards (CACs) issued to authorized personnel.
- The NSA is developing and deploying PKI Increment 2 in four spirals on SIPRNET and NIPRNET. The NSA delivered the SIPRNET Token Management System (TMS) in Spirals 1, 2, and 3. Spiral 4 is intended to deliver the NIPRNET Enterprise Alternate Token System (NEATS) and Non-Person Entity (NPE) capabilities.
  - NEATS is intended to provide confidentiality, integrity, authentication, and nonrepudiation services by providing a centralized system for the management of NIPRNET certificates on NEATS tokens for privileged users, which includes System Administrators, groups, roles, code signing, and individuals not eligible to receive CACs. NEATS will provide token registration, issuance, personnel identification number reset, revocation, and key recovery. The private keys are encoded on the token, which is a smartcard embedded with a microchip.
  - The NPE system issues certificates to large numbers of network devices (e.g., routers and web servers) using both manual and automated methods. These certificates help ensure only authorized devices are allowed to access DOD networks. NPE provides authorized System Administrators and Registered Sponsors with the capability to issue device certificates singularly or in bulk without the need for PKI registration authority approval.
  - The NSA manages the NEATS and NPE with operational support from the Defense Information Systems Agency (DISA), which hosts the infrastructure and provides PKI support for the DOD, and the Defense Manpower Data Center (DMDC). DMDC also manages the Defense Enrollment Eligibility Reporting System (DEERS) for the NIPRNET and Secure Defense Enrollment Eligibility Reporting System (SDEERS) for the SIPRNET, the authoritative sources for personnel data.

- NPE and NEATS use commercial and government off-the-shelf hardware and software hosted at respective DISA and DMDC sites.

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

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

Activity
- In February 2018, DOT&E approved the combined test plan for the PKI Increment 2 OA and future FOT&E.
- The USD(A&S) delegated Milestone Decision Authority for the DOD PKI Increment 2 program to the NSA in March 2018.

Spiral 3
- DOT&E published the PKI Increment 2, Spiral 3 FOT&E Report in December 2017 based on a test that JITC conducted in August/September 2017.
- JITC verified Spiral 3 deficiency fixes in June 2018 and began a SIPRNET token reliability assessment in July 2018.
- The NSA SAE approved DOD-wide fielding of Spiral 3 in October 2018.

Spiral 4
- JITC conducted three cybersecurity assessments of PKI Increment 2, Spiral 4 capabilities in FY18 (the results are classified):
  - NPE Cooperative Vulnerability and Penetration Assessment (CVPA), February 2018
  - NEATS CVPA, March 2018
  - NPE Adversarial Assessment, June 2018
- JITC conducted the NPE and NEATS CVPA re-tests in October 2018.
- In late July 2018, the PKI PMO delayed the OA of the PKI Increment 2, Spiral 4 capabilities until November/December 2018 to resolve high-priority system defects and integration problems.
- JITC plans to conduct an FOT&E of all Increment 2 capabilities, including the new Spiral 4 NPE and NEATS functionalities, from March/April 2019. The FOT&E will examine the NEATS on NIPRNET and the NPE enterprise certificate issuance and management system deployed on both the NIPRNET and the SIPRNET.
- The PKI PMO changed the estimated Increment 2 Full Deployment Decision to late July 2019.

Assessment
- PKI Increment 2, Spiral 3 is operationally effective and suitable for day-to-day operations, but not suitable for long-term sustainment.
  - Testing revealed PKI process problems with tiered help desk coordination, configuration management, and token certification.
- Problems associated with Spiral 4 NPE and NEATS capabilities found in developmental and integrated testing events are affecting preparations for operational testing.
- NPE and NEATS capability problems and the lack of operationally representative NPE devices caused several test event slips.
- The Service and Agency NIPRNET System Administrators must be equipped with NEATS tokens in order to adequately demonstrate auto-provisioning of NPE certificates. Because of the significance of NEATS developmental test findings and initial classified findings stemming from the NEATS CVPA, the PKI PMO delayed the OA to resolve high-priority system defects and integration problems.
- The NPE test effort is handicapped because vendors have not fully implemented protocols for device enrollment, so the Key System Attribute to auto-rekey devices is unlikely to be met.
  - The PKI PMO is still investigating and identifying devices that will support the NPE protocols.
- The proposed NPE integration efforts only provide limited, semi-automated protocol solutions that likely will not satisfy the greater NPE requirement needs of the DOD, which include an as yet unknown, and certainly much broader, range of devices.
- The NSA is responsible for certifying that tokens are secure in the operational environment. However, the NSA did not fully document or follow a formal assessment process for the Giesecke and Devrient tokens.
- The PKI PMO and DISA plan to migrate TMS from the DISA physical hosting to a virtualized, Next Generation environment after the planned Increment 2 FOT&E and currently do

not have plans to operationally test changes to the system architecture and any interfaces for the Services and Agencies.

Recommendations

- The DOD and Service Chief Information Officers should:
  1. Develop a DOD enterprise NPE policy and implementation guidance for automated device enrollment.
- The PKI PMO and DISA should:
  1. Continue to resolve all high-priority defects and verify acceptability to users prior to entering the PKI Increment 2, Spiral 4 OA and FOT&E.
  2. Establish a dedicated sustainability working-level integrated product team to address sustainability and logistics problems through transition to DISA and DMDC.
  3. Establish a more realistic, event-driven timeline for future PKI capability testing that better supports milestone decisions, while managing the expectations of those with PKI equities.
  4. Issue NPE procedures for implementation of auto-rekey protocols to assist Service and Agency System Administrators with device configurations.
  5. Coordinate with the DOD Chief Information Officer to issue NPE guidance for the Services and Agencies on the intended NPE approach for enterprise-wide Certificate Authorities and devices.
  6. Complete full security certification testing for existing Giesecke and Devrient tokens, and rigorously follow the certification process for all future token variants to ensure new tokens are secure prior to deploying them into the operational environment.
  7. Delay the PKI Increment 2 FOT&E until the system architecture, critical Spiral 4 functionality, and interfaces are ready for test.
  8. Plan for JITC to conduct a post-Increment 2 operational test to evaluate the TMS hosting and cybersecurity in the DISA Next Generation environment.

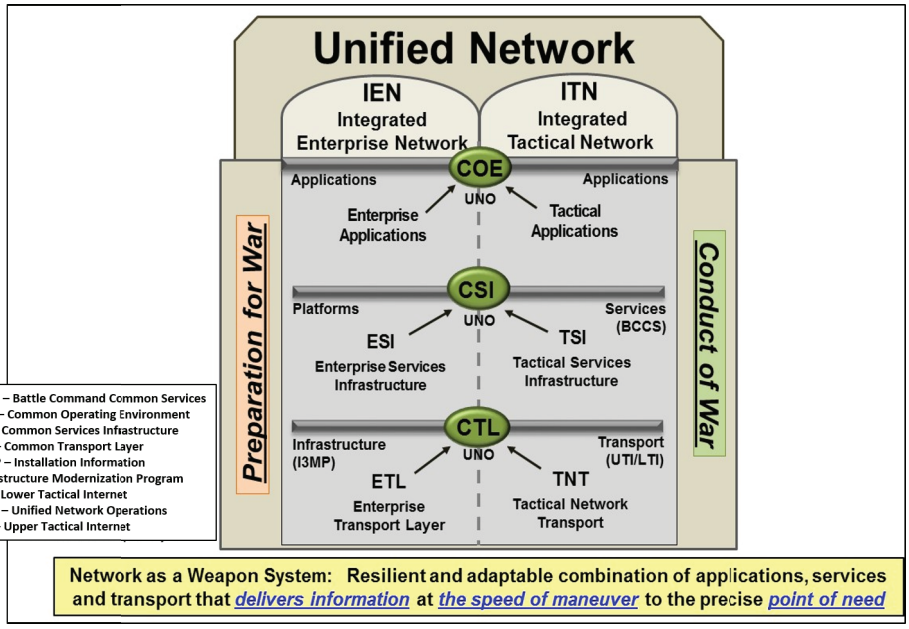
Army Programs

Army Programs

Army Network Modernization

Network Modernization

The 2018 National Defense Authorization Act directed the Army to submit to the congressional defense committees a report on the Army strategy for "modernizing air-land ad-hoc, mobile tactical communications and data networks." The Chief of Staff of the Army developed a strategy intended to enable the Army to "fight tonight" while seeking technical solutions in order to modernize the Army's communications. The Army's strategy recognized that its network had not evolved to enable decisive action against a peer threat in a highly mobile and contested environment. To correct this, the Army seeks to pivot away from traditional acquisition by including non-developmental items and commercial off-the-shelf technologies with programs of record to build its tactical network.



The Army's plan has four tenets: institute cohesive governance, halt select programs of record, fix existing critical programs, and pivot to a new acquisition approach. The Army strategy intends to create a new process by which it will experiment and learn about a broad array of technologies. The Army created the Network Cross Functional Team (N-CFT) to augment traditional acquisition through rapid prototyping and experimentation. The N-CFT is a subordinate organization to the Army Futures Command, a new four-star Army Command, combining people, responsibilities, and funding from the requirements, research and development, and systems analysis communities. The N-CFT will design and execute experimentation to inform requirements and design for future acquisition programs. The Army has identified four primary lines of effort to modernize its tactical network:

- **Unified Network** – This effort has three components: integrated tactical network, integrated enterprise network, and unified network enabling capabilities. It includes the development of a standards-based network architecture that unifies enterprise and deployed network capabilities and features a unified transport layer, network operations, and other enabling functions that allows integration of disparate networks. A unified network could provide resiliency through path diversity and dynamic routing to ensure tactical units can communicate in hostile environments. Allied partners have successfully implemented a similar approach.
- **Common Operating Environment (COE)** – When complete, the Army intends for the COE to include a set of computing technologies, integrated data and databases, common graphics, and a unified set of mission command applications. It will rely on data standards and virtualization to provide browser-based access to mission command capabilities for at-the-halt and on-the-move leaders.
- **Interoperability** – This effort includes joint interoperability and coalition accessibility through a network that enables appropriate collaboration with all unified action partners.
- **Command Posts** – The Army wants to improve the mobility and signature (visual, acoustic, thermal, and electromagnetic) of expeditionary command posts.

The Director, Cost Assessment and Program Evaluation (CAPE) and DOT&E reviewed the Army's strategy in response to the Explanatory Statement for the Department of Defense Appropriations Bill, 2018. CAPE and DOT&E concluded:

- The strategy was a work in progress and was premature to assess the suitability of programs and technologies that the Army was investigating.
- The Army strategy of using experimentation to inform requirements is suitable and the Army should continue to refine the process of how technologies were chosen for inclusion in the experimentation.
- Each experiment should be conducted against the appropriate threat scenario to include cybersecurity and electronic warfare capabilities.
- A standards-based network strategy is suitable and could allow for rapid insertion of new technology over time. The Army should prioritize completion of the standards and architectures for the COE and unified network in order to create a cohesive effort of building the Army's network.
- The success of this strategy is directly tied to adequately funding experimentation by the N-CFT.

Network Cross Functional Team (N-CFT)

The N-CFT is working on several lines of effort in order to continue the Army's network modernization strategy.

The N-CFT is in the middle of developing requirements and systems to create a unified network for the Army to use. This includes efforts to develop and implement an architecture that will unify the tactical network; finding, developing, and demonstrating technologies to create this network; and the creation of requirements. The N-CFT defined a working term, the Integrated Tactical Network (ITN). The ITN is the suite of communications and networking hardware and software that provides voice and data communication capabilities to tactical units. It is the infrastructure necessary to support the current and future voice and data needs (namely mission command software). The ITN is not rigidly defined and will continue to evolve over time as the Army identifies new technologies.

The ITN Information System Initial Capabilities is under development with a planned approval during 1QFY19. The N-CFT has lines of effort for the COE, interoperability, and command post mobility and survivability.

The N-CFT has conducted ITN-based experiments in FY18 to include major training events in the United States and Europe. The Army Test and Evaluation Command (ATEC) led a team that observed the experimentation and published a Capabilities and Limitations Report for the ITN in May 2018. This report recommended several possible ways to refine the configuration, evaluation, and deployment of the ITN in the future. This included recommendations to reduce or eliminate wired connections, create less resource intensive range extension, and use conformal wearable batteries. The report also recommended that future testing of the ITN should include cybersecurity, human factors, and waveform characterizations.

Directed Requirement to Experiment, Demonstrate, and Assess an Integrated Tactical Network (ITN)

In June 2018, the Vice Chief of Staff of the Army used the Army's Tactical Network Modernization Strategy and the ATEC Capabilities and Limitations Report for the ITN as references for the Directed Requirement to Experiment, Demonstrate, and Assess an ITN. This document created the requirement to procure equipment necessary to field the ITN to an Infantry Brigade Combat Team (IBCT), Stryker Brigade Combat Team (SBCT), Armored Brigade Combat Team (ABCT), and associated units. The document gave responsibility of the architecture of the network to the Army Capabilities Integration Center (now part of Army Futures Command) in coordination with the Chief Information Officer of the G6 and the Assistant Secretary of the Army for Acquisition Logistics and Technology's System of Systems Engineering and Integration.

The Directed Requirement included guidance to the N-CFT to conduct assessments and characterizations of the ITN with an IBCT, an SBCT battalion, and an ABCT battalion. The Vice Chief of Staff of the Army directed the N-CFT assessments of the ITN to focus on the networking capabilities of the ITN to include: alternate networks, advanced waveforms, network gateways, satellite terminals, mission command system integration, and range extension. The experimentation is expected to include scenarios and equipment that will help inform future requirements, capability sets, and procurement recommendations. DOT&E is concerned about the level of test rigor planned for these assessments. In the absence of a detailed experimentation and evaluation strategy, it is unlikely that the Army will be able to collect the data required to support development of requirements.

The Directed Requirement seems to have implemented the network modernization plan to use experimentation to develop requirements and define ITN equipment. The Vice Chief of Staff of the Army has included some of the ATEC suggestions for additional testing and made them a part of the requirements. The development of the evaluation strategy is undefined at this point. The Army intends to do the assessment with a unit during a combat training center rotation. The development of this assessment strategy is crucial to how the equipment fielded to the designated units will function in an operational setting, but also how future requirements will be written and implemented.

Network Integration Evaluation (NIE) 18.2

The NIE 18.2, scheduled for October and November of 2018, will serve as the final NIE. ATEC will conduct three operational tests as a part of the NIE 18.2: Command Post Computing Environment (CPCE) IOT&E, Distributed Common Ground System – Army (DCGS-A) Capability Drop 1 IOT&E, and the Mounted Computing Environment (Mounted CE) Customer Test. The NIE 18.2 will include risk reductions of the air-ground network integration and demonstrations of the ITN and various tactical radios.

The NIE events were a useful tool for the Army to conduct comprehensive evaluations of an integrated mission command network than was possible through evaluations of individual components. This benefit was predicated on aligning multiple operational tests with a single, annual, schedule-based event. This schedule alignment limited the flexibility of programs to adapt to schedule delays, and delays could be amplified when a program needed to wait for the next scheduled NIE.

The ITN is a capability comprised of many different systems. The N-CFT would benefit from conducting an integrated experiment, with a dedicated test unit, against an appropriately sized opposing force, in challenging terrain, which will be necessary to evaluate that overarching capability. This will necessarily align the systems being tested together and could prevent the schedule driven nature of the NIE. The Army should consider using the lessons learned from the execution of 8 years of NIEs to develop a plan for the assessment and evaluation of the ITN. Using test and evaluation best practices will enable the Army to gather objective, defensible data to inform future requirements.

Abrams M1A1 System Enhancement Program (SEP) Main Battle Tank (MBT)

Executive Summary
- The Army continues to characterize the survivability of the M1A2 System Enhancement Program (SEP) version 3 (v3) against IEDs, mines, and direct- and indirect-fire threats. In FY18, LFT&E examined the vulnerability of the tank to threat-induced impact to onboard ammunition, and full-up system-level (FUSL) testing. FUSL is scheduled to be completed in 3QFY19.
- DOT&E plans to complete a detailed survivability analysis in 4QFY19 to support the Full Materiel Release decision in 1QFY20.

System
- The Abrams M1A2 Main Battle Tank (MBT) is a tracked, land combat, assault weapon system equipped with a 120 mm main gun designed to possess significant survivability, shoot-on-the-move firepower, joint interoperability (for the exchange of tactical and support information), and a high degree of maneuverability and tactical agility.
- The M1A2 SEPv2 is currently fielded. It upgrades the M1A2 SEP by providing increased memory and processor speeds; full color tactical display; digital map capability; compatibility with the Army Technical Architecture; improved target detection, recognition, and identification through incorporation of second-generation Forward Looking Infrared technology and electronics; Common Remotely Operated Weapon Station (CROWS)-Low Profile (LP); and crew compartment cooling through the addition of a thermal management system.
- M1A2 SEPv3 fielding is planned for FY20. The M1A2 SEPv3 is an upgrade to the M1A2 SEPv2. The upgrades include:
  - Power generation and distribution to support the power demands of future technologies
  - Compatibility with joint battle command network
  - Survivability enhancements including Next Evolution Armor and reduction in vulnerability to IED threats

  - Reduction in vulnerability to Remote Controlled Improvised Explosive Devices (RCIEDs)
  - Lethality by providing the ability for the fire control system to digitally communicate with the new large caliber ammunition through use of an ammunition datalink
  - Energy efficiency (sustainment) due to the incorporation of an auxiliary power unit
  - Improved silent watch capability

Mission
- Commanders employ units equipped with the M1A2 SEP MBT to close with and destroy the enemy by fire and maneuver across the full range of military operations.
- The Army intends the M1A2 SEP MBT to defeat and/or suppress enemy tanks, reconnaissance vehicles, infantry fighting vehicles, armored personnel carriers, anti-tank guns, guided missile launchers (ground and vehicle-mounted), bunkers, dismounted infantry, and helicopters.

Major Contractor
General Dynamics Land Systems – Sterling Heights, Michigan

Activity
- The Army conducted all testing in accordance with a DOT&E-approved test plan.
- In FY18, the Army completed the system-level ammunition vulnerability test series intended to quantify the performance of bustle side armor and to assess the vulnerability of the vehicle to threat-induced impact to the onboard M829A4 ammunition.
- The Army started the execution of the FUSL test series in February 2018 to assess the survivability of a combat-ready tank against IEDs, mines, and direct and indirect fire. The FUSL test series includes a total of 21 tests on 3 fully functional tests tanks, and is expected to be completed in 3QFY19.

- The live fire events are coupled with modeling and simulation to support shot-line selection, pre-shot prediction, test damage, casualty assessment, and generalization of system vulnerabilities over a range of engagement conditions.

Assessment

- DOT&E continues to assess available live fire test data to characterize the protection provided by the M1A2 SEPv3 against expected operationally realistic threats. DOT&E will use modeling and simulation to support the final assessment.
- The program moved its Full Material Release from 3QFY20 to 1QFY20, potentially posing some challenges to complete planned testing, modeling and simulation activity, and reporting by the end of 3QFY19.
- The Abrams SEPv3 does not have a unique requirements document to specify expected survivability and force protection capabilities.

Recommendation

1. The Army should ensure that the SEPv4 and future Abrams tank upgrades are supported by a comprehensive set of requirements that accurately reflect the operational challenges.

Active Protection Systems (APS) Program

Executive Summary

- The Active Protection System (APS) program is intended to improve the survivability of ground combat vehicles against anti-tank guided missiles, rocket-propelled grenades, and recoilless rifle threats by using a kinetic "hard kill" mechanism to intercept and disrupt/defeat the incoming threat.
- In 2017, in support of the European Deterrence Initiative, the Army initiated an expedited installation and characterization of three Non-Developmental Item (NDI) "hard kill" APS: Rafael Trophy APS for the Army Abrams M1A2 and Marine Corps M1A1 tanks, the Artis Iron Curtain for the Stryker vehicles, and the IMI Systems Iron Fist APS for the Bradley vehicles.
- The Army divided APS testing into two major phases to assess technology maturity, performance, and integration, and to support the Urgent Material Release (UMR).

Trophy APS

- Trophy APS demonstrated the potential to provide improved protection to the Abrams tank when compared to the existing systems without APS.
- The test was designed to assess fundamental APS capability in basic range conditions and engagements. The test was not designed to enable detailed assessment of vehicle survivability and force protection after the engagement.
- The Army issued a directed requirement to procure and install Trophy APS systems on Abrams for a total of four Armored Brigade Combat Teams, by the end of FY20.

Iron Curtain APS

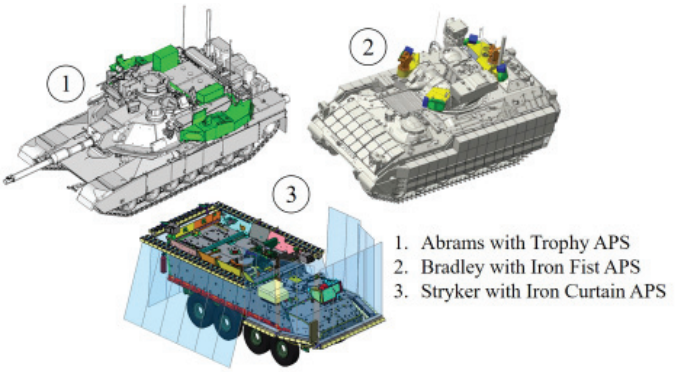
- Iron Curtain APS did not demonstrate sufficient threat intercept and Stryker/force protection capability. Consequently, the Army issued a request for information for other Stryker APS systems with the intent to test in late CY19.

Iron Fist APS

- Phase I Iron Fist APS testing on the Bradley is complete. This test supported the Army Requirements Oversight Council (AROC) decision meeting on November 30, 2018.

System

- The APS solutions are designed to enable the system to detect and declare a threat, deploy counter-munitions, and disrupt/defeat the threat. A successful APS intercept of a threat does not imply the absence of residual damage to the combat vehicle or its crew following an engagement. The Army selected the following to be installed and characterized:
  - Rafael Trophy APS on the Army Abrams M1A2 and Marine Corps M1A1 tanks
  - Artis Iron Curtain on the Stryker
  - IMI Systems Iron Fist on the Bradley.



Trophy APS

- The Trophy system is designed to engage incoming threats with a kinetic projectile intended to destroy the threat or cause early detonation. The Abrams base armor is expected to be able to absorb post engagement threat residuals (threat by-products generated after the collision). The Trophy APS adds approximately 7,200-pounds to the platform. In addition to the installation of the Trophy system onto the tank, the Army has incorporated limited integration of the Trophy system into the tank's situational awareness system.

Iron Curtain

- The Iron Curtain is designed to engage incoming threats with a kinetic projectile intended to prevent function of the warhead. The Iron Curtain adds approximately 5,700 pounds to the Stryker vehicle.

Iron Fist

- The Iron Fist is designed to engage incoming threats with an explosive projectile intended to destroy or divert the threat, and adds approximately 1,543-pounds to the platform. The fielded Bradley A3 does not generate sufficient power to operate the APS. Power components from the Bradley A4, currently under development, were integrated into the APS test asset.

Mission

- Army and Marine units intend to use Abrams main battle tanks equipped with the Trophy APS to disrupt/destroy certain classes of enemy fire while safely maneuvering across the full range of military operations.
- Army commanders intend to use Stryker vehicles equipped with the Iron Curtain APS to disrupt/destroy enemy military forces, to control land areas including populations and resources, and to conduct combat operations to protect U.S. national interests while increasing protection to the vehicle and its crew.

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

Major Contractors
- DRS – St. Louis, Missouri
- IMI Systems – Ramat HaSharon, Israel
- Artis, LLC – Reston, Virginia

Activity
- The Army used a two-phased approach to characterize the performance of the various APS solutions in support of the UMR:
  - Phase I consisted of limited characterization testing of threat interactions with the APS system. It was intended to determine fundamental performance and limitations of the APS and feasibility of installing APS systems on the host platforms.
  - Phase II is intended to test production-representative APS as installed on operationally representative systems under realistic combat condition. It is intended to adequately assess the capabilities and limitations of the systems prior to fielding in support of the UMR.
- Phase I live fire testing for each of the three APS solutions included up to 50 events. Approximately 70 percent of the tests were performance characterization events and the remaining tests were operationally relevant environment events. The Army conducted APS testing at the Redstone Test Center, Alabama.

Trophy APS
- The Army completed Phase I testing in September 2017. Phase I testing also included 10 Marine Corps Abrams tests with moving vehicle and inert threats.
- Phase II test planning is ongoing.

Iron Curtain APS
- The Army completed Phase I testing in March 2018 and is analyzing the results.
- The Army is reassessing the path forward for Stryker APS.

Iron Fist APS
- The Army completed Phase I testing in August 2018. The contractor (IMI Systems Iron Fist) conducted follow-on testing to implement and retest minor changes to the system design needed for the AROC decision to enter Phase II.

Assessment

Trophy APS
- Phase I live fire testing demonstrated the capability of the system to counter most of the threats tested under basic range conditions and simple threat scenarios. Phase I testing included several limitations that inhibit an assessment of the APS performance with confidence:
  - The Army performed the majority of the tests on a ballistic hull and turret asset that did not independently power the APS, nor have any internal operational features as they would in a fielded configuration.
  - The Army relied heavily on the contractors to set up the APS due to the limited knowledge of the foreign system.
  - The test was not designed to enable assessment of the vehicle vulnerability after an engagement: rolled homogeneous armor plates were used as witness material in lieu of the complex armors used by the Abrams.
  - Testing for Trophy and Iron Curtain has had limited scope pertaining to logistical considerations for installation, maintenance, counter-munition resupply, and transportation. This will limit the Army's understanding of the logistical burden Trophy and Iron Curtain place on units that receive the system
- Phase II testing will require more operationally realistic testing and evaluation (using adequate modeling and simulation tools) to support the UMR. Phase II testing is scheduled to start in November 2018. The modeling and simulation tools need to be updated to enable more comprehensive evaluation of systems equipped with APS.

Iron Curtain APS
- Phase I live fire testing demonstrated an improved ability of the Iron Curtain system to intercept incoming threats compared to prior DOT&E tests (held in 2011) and ground combat vehicle tests (held in 2014). However, damaging effects to the Stryker vehicle base armor occurred regularly even with successful intercepts. An upgrade to the baseline armor will be necessary if this APS is to be employed on a Stryker vehicle. The Army has also observed other limitations regarding performance in low light and simulated rainy conditions. Consequently, the Army is pursuing other systems for Stryker.

Iron Fist APS
- Phase I Iron Fist live fire and user testing was completed in 2018. Preliminary assessment by the Army was that the system demonstrated an inconsistent capability to intercept threats. Counter-munition dudding and power failures to the launcher were leading contributors to the low intercept rate. The Program Office has been working with the vendor on design improvements to address the system performance shortcomings. Some prospective solutions have been implemented and will be tested in Phase II.

Recommendations

The Army should:
1. Conduct live fire test of final APS solutions installed on combat-configured vehicles against operationally

representative threats to adequately evaluate force protection and survivability of the vehicle.
2. Ensure Phase II testing is designed to assess force protection and the survivability of the vehicle (residual mission capability and damage effects) post engagement, even given a successful APS intercept of the threat.
3. Minimize contractor involvement during Phase II testing to fully characterize the capabilities and limitations of the system.
4. Develop and advance the appropriate modeling and simulation tools needed to support the test planning and evaluation of systems equipped with APS.
5. Include logistical considerations for installation, maintenance, counter-munition resupply, and transportation in future user test design.

AH-64E Apache

Executive Summary

- The Army conducted 30 mm gun accuracy testing to characterize performance and isolate root causes of inaccuracy reported by units fielded with AH-64E aircraft.
- The Army conducted developmental flight testing of upgraded subsystems to the Version 6 AH-64E aircraft in preparation for FOT&E II in 2019.
- In March 2018, the Army informed Boeing that it would suspend acceptance of all AH-64E aircraft due to the unacceptable safety risks and increased Army burden (inspections, time, funding) the strap pack retention nut failure presents. Boeing met the conditions for production restart in August 2018 and the Army has begun accepting production AH-64E aircraft.
- The Army is continuing with live fire testing to assess the vulnerability of the aircraft to combat induced fires.

System

- The AH-64E is a modernized version of the AH-64D Attack Helicopter. The Army intends to sustain the Apache fleet through the year 2040. The Army uses the AH-64E in Attack/Reconnaissance Battalions assigned to Combat Aviation Brigades. Each battalion has 24 aircraft.
- The AH-64E advanced sensors, improved flight performance, and ability to integrate off-board sensor information provide increased standoff and situational awareness in support of the joint force.
- The Army fielded the AH-64E in two versions (1 and 4). Version 1 following IOT&E in 2012 and Version 4 following FOT&E I in 2014. Operational testing of Version 6 is planned for 2019.
- The major Version 1 AH-64E capability improvements included:
  - The ability of the aircrew to control the flight path and the payload of an Unmanned Aircraft System
  - Improved aircraft performance with 701D engines, composite main rotor blades, and an improved rotor drive system
  - Enhanced avionics, which includes satellite communication and an integrated navigation suite to meet global air traffic management requirements
- The Version 4 AH-64E retained Version 1 capabilities and added hardware and software to operate in the Link 16 network.
- The Army has developed AH-64E Version 4.5 with a pilot vehicle interface that enables employment of all Joint Air-to-Ground Missile (JAGM) modes to support JAGM flight testing.
- The Army will conduct FOT&E II with Version 6 AH-64E in 2019. The Army plans to add multiple enhancements in Version 6 to include:

  - Radar Frequency Interferometer (RFI) passive ranging
  - Fire Control Radar range extension and maritime targeting mode
  - Cognitive Decision Aiding System
  - Modernized Day Sensor Assembly with color and high definition displays
- The Army procurement objective is to procure 791 AH-64E aircraft. The Army's long term plan is to convert all AH-64E to Version 6. In the interim, the Army will convert fielded Version 1 aircraft to JAGM-capable Version 4.5. In time, all Version 4 AH-64E aircraft will be converted to Version 6.

Mission

The Joint Force Commander and Ground Maneuver Commander employ AH-64E-equipped units to shape the area of operations and defeat the enemy at a specified place and time. The Attack/Reconnaissance Battalions assigned to the Combat Aviation Brigade employ the AH-64E to conduct the following types of missions:

- Attack
- Movement to contact
- Reconnaissance
- Security

Major Contractors

- Aircraft: The Boeing Company Integrated Defense Systems – Mesa, Arizona
- Targeting Sensors and Unmanned Aircraft System datalink:
  - Longbow Limited Liability Company – Orlando, Florida, and Baltimore, Maryland
  - Lockheed Martin Corporation – Orlando, Florida, and Owego, New York
- L3 Communications Systems – Salt Lake City, Utah

Activity

- In December 2016, the failure of a Main Rotor Strap Pack resulted in the loss of an AH-64D and two crew members. The outboard retention nut failure was attributed to stress corrosion cracking. Boeing designed a larger strap pack retention nut that incorporates a stronger material with anti-corrosive properties. The Army has increased strap pack inspections and is retrofitting all AH-64 aircraft with the enhanced strap pack with priority going to coastal units that operate in more corrosive environments. The Apache Program Manager completed retrofit of coastal units in September 2018 and expects retrofit completion of U.S. and Foreign Military Sales aircraft by December 2019.
- Citing unacceptable safety risks and increased Army burden (inspections, time, funding) related to the strap pack nut failure, the Army informed Boeing in March 2018 that it would halt acceptance of all AH-64E aircraft. Boeing met the conditions for production restart in August 2018, and the Army has begun accepting production AH-64Es.
- Operational units have reported that the 30 mm gun is less accurate on the AH-64E than on the legacy AH-64D. The Apache Program Manager performed root cause analysis and identified three issues: early round inaccuracy (early round off target), dispersion (rounds not consistently on target), and changing bias (over time, shot group drifts from target). The Apache Program Manager and Boeing have systematically tested multiple subsystems and developed software fixes to be verified in October 2018 testing. The Program Manager expects to field solutions starting in early 2019.
- The Army conducted developmental flight testing of upgraded Version 6 AH-64E subsystems to include RFI passive ranging, the Fire Control Radar range extension and maritime targeting, the Cognitive Decision Aiding System, and the Modernized Day Sensor Assembly with color and high-definition displays.
- Apache aircraft supported integrated testing of 49 JAGM shots in FY17 and FY18.
- The Army selected AH-64E to be one of the five systems to complete an evaluation of cyber vulnerabilities to comply with section 1647 of the National Defense Authorization Act for FY16. The Army conducted a Cooperative Vulnerability and Penetration Assessment in September 2017 and plans to conduct an Adversarial Assessment of the Version 6 AH-64E in June 2019.
- In October 2017, the Army Research, Development, and Engineering Command (RDECOM)/Survivability/Lethality Directorate (SLAD) completed live fire testing of the fire detection and expansion system.
- In November 2017, RDECOM/SLAD conducted testing to determine the effectiveness of a new fire barrier and intumescent paint added to production AH-64s to minimize the effect of fires in the tail boom aft transition. In August 2018, these tests were followed by additional tests, funded by the Joint Live Fire program, to assess the fire-induced damage effects under flight loading.
- Testing of the onboard halon fire suppression system is currently expected to begin in 1QFY19.
- The Army completed all testing in accordance with a DOT&E-approved Test and Evaluation Master Plan and Live Fire Strategy.

Assessment

- Developmental testing of Version 6 AH-64E software and major subsystems in 2018 revealed multiple performance deficiencies. One or more deficiencies affected the Multi-Core Mission Processor, Modernized Radar Interferometer, the Fire Control Radar, the Target Acquisition Designation Sight, and Manned – Unmanned Teaming. The Program Office has since identified fixes for most of the problems. Regression testing on Apache subsystems has begun and early indications are that some of the problems have been resolved.
- The Fire detection and expansion system is largely effective in detecting tail boom fires providing aircrew with the awareness of the fire event before the condition becomes critical. Analysis of the fire barrier and intumescent paint testing is ongoing.

Recommendations

1. The Army should continue to investigate sources of AH-64E 30 mm gun error, implement fixes as appropriate, and demonstrate in side-by-side testing that the AH-64E gun is as accurate as the gun on legacy aircraft.
2. The Apache Program Office should verify in regression testing of Version 6 AH-64E subsystems that Boeing has corrected the previous deficiencies. Following verification of fixes, the Army should conduct FOT&E II to demonstrate Version 6 Apache capabilities.
3. The Army should continue to retrofit all U.S. Government and Foreign Military Sales aircraft with the enhanced strap pack.

Armored Multi-Purpose Vehicle (AMPV)

Executive Summary

- The Armored Multi-Purpose Vehicle (AMPV) program conducted a Limited User Test (LUT) in September 2018. Preliminary analysis indicates the AMPV meets or exceeds its goal of replacing the M113 Armored Brigade Combat Team (ABCT) Family of Vehicles (FoV) with a more capable platform.
- In FY17, the Army completed component (armor) live fire testing, and in FY18, the Army completed ballistic hull live fire testing of the AMPV General Purpose (GP) and Mortar Carrier (MC) variants to assess survivability and force protection specification requirements.
- Preliminary assessment identified minor vehicle design vulnerabilities that the program would have to mitigate to meet the survivability and force protection requirements.
- In FY18, the AMPV program started system-level live fire testing on GP and MC prototype vehicles. Testing will continue for all AMPV variants to assess survivability and force protection against underbody mines, and direct and indirect threats in support of the program of record Milestone C decision scheduled for 1QFY19, and the FY20 European Deterrence Initiative (EDI) fielding decision.

Mission Command (Mcmd)

Mortar Carrier (MC)

General Purpose (GP)

Medical Evacuation (ME)

Medical Treatment (MT)

System

- The AMPV will replace the ABCT M113 FoV program that the Army terminated in 2007. The AMPV is required to operate alongside the M1 Abrams Main Battle Tank and the M2 Bradley Infantry Fighting Vehicle.
- The Army intends for the AMPV variants to address the M113 shortcomings in survivability and force protection; size, weight, power, and cooling; and the ability to incorporate future technologies such as the Army Network.
- The Army is carrying over the Mission Equipment Packages from the existing M113 FoV into the AMPV variants.
- The AMPV has five variants:
  - GP vehicle from which the unit First Sergeant will conduct combat resupply escort, emergency resupply, and casualty evacuation; and provides security for medical evacuation.
  - Mission Command (MCmd) vehicle intended to integrate the communications equipment in accordance with the Network Systems Architecture.
  - Medical Treatment (MT) vehicle to provide an armored and mobile protected environment for the unit surgeon and medical staff to provide immediate medical care of casualties or life stabilization triage for casualties prior to their evacuation to more capable facilities.
  - Medical Evacuation (ME) (Ambulance) vehicle supports the ABCT integration of medical support providing

protected ambulance evacuation and immediate medical care to the mechanized and armored cavalry units.
- MC vehicle provides immediate, responsive, heavy mortar fire support to the ABCT in the conduct of fast-paced offensive operations by utilizing the M121 Mortar System and the M95 Mortar Fire Control System.

Mission
Commanders employ units equipped with the AMPV to provide a more survivable and highly mobile platform to accomplish required operational support missions across the range of military operations. ABCT units use AMPVs to conduct logistical resupply; casualty evacuation and treatment; command post operations; and heavy mortar fire support.

Major Contractor
BAE Systems – York, Pennsylvania

Activity
- The Army approved an Operational Needs Statement in FY17 directing the program manager to begin fielding two brigade sets of AMPV no later than December 2020.
- USD(AT&L) approved the EDI Acceleration acquisition strategy and funding in January 2016. Two hundred and fifty-eight vehicles are to be procured and fielded beginning in FY20.
- DOT&E approved the test plan and the Cooperative Vulnerability and Penetration Assessment (CVPA) in March 2018.
- The Army moved the Milestone C decision from 2QFY19 to 1QFY19 in order to align with the EDI production decision.
- The vendor experienced production challenges that delayed the delivery of vehicles to the Army Test and Evaluation Command (ATEC), which delayed the start of the Production Prove-Out Test (PPT) by 60 days. The First AMPV vehicle was delivered and started testing in June 2017; ATEC began PPT in September 2017 on all five variants.
- The Army conducted a LUT from September 6 – 24, 2018, at Fort Hood, Texas, in accordance with the DOT&E-approved test plan. The test unit was the 4-9 Cavalry Squadron out of the second Brigade First Cavalry Division. The opposing force was the 1-5 Mechanized Infantry Battalion out of the second Brigade First Cavalry Division.
- The Army completed armor coupon testing in November 2017 to evaluate armor performance and to assess any secondary damage effects of the armor debris.
- In June 2018, the Army completed ballistic hull testing of the AMPV GP and MC variants to evaluate vehicle survivability against underbody mines and direct and indirect threats.
- In September 2018, the Army started system-level live fire tests on prototype AMPV vehicles configured with operational systems and equipment to evaluate system and crew vulnerability to direct fire kinetic energy munitions, shape charged jet threats, artillery, explosively formed penetrators, and side and underbody mines.
- AMPV full-up system-level (FUSL) live fire test planning is ongoing. FUSL testing is scheduled to start in FY20 and is intended to support a survivability and crew casualty assessment of the production-representative AMPV variants against expected operational threats. DOT&E is working with the live fire integrated product team to incorporate the latest underbody LFT&E methods to increase test repeatability and crew surrogate biofidelity.
- The Army conducted Cooperative Vulnerability Identification (CVI) in FY16 and a CVI Verification of Fixes in FY17.
- The Army conducted a CVPA in April 2018 and an Adversarial Assessment in conjunction with the LUT at Fort Hood in September 2018.
- The program manager has updated the Milestone C Test and Evaluation Master Plan; it is currently being staffed through the Army.

Assessment
- During PPT testing, several deficiencies reduced the Mean Miles Between System Aborts (MMBSA).
  - The demonstrated MMBSA of 445 was below the expected entrance criteria of 850 MMBSA.
  - Several unintended Automatic Fire Extinguishing System (AFES) engine discharges occurred. Following each AFES discharge, the Program Office thoroughly investigated the vehicle to rule out a possible thermal incident.
  - There were several instances of the elevating support of the mortar carrier bipod becoming unlatched after firing, allowing the mortar to lift and/or fall.
- The vendor conducted corrective actions during PPT and reliability, availability, and maintainability testing to address the critical deficiencies identified prior to the LUT.
- Preliminary observations of the LUT indicate the AMPV meets or exceeds its goal of replacing the M113 FoV with a more capable platform.
  - The AMPV demonstrated superior power and mobility than the M113 FoV.
  - The AMPV was able to maintain its position in the formation.
  - The AMPV operational mission availability and reliability were far superior to the M113 FoV.
  - The AMPV demonstrated a point estimate of 665 MMBSA.
  - The platform provides potential for growth for power demand.
  - Having common parts amongst all the variants should improve overall availability.
  - The MCmd variant facilitates digital mission command.

  - The MT and ME variants provide improved patient care and treatment capability with a new capability of conducting treatment on the move.
- The following deficiencies, if uncorrected, could adversely affect IOT&E:
  - The driver's and vehicle commander's displays would frequently lock up and the reboots each took 10 minutes.
  - Due to the physical size and location, the commander's weapons station degraded situational awareness of the vehicle commander.
  - The Joint Battle Command – Platform and radios in the MCmd vehicle cannot be removed from their docking stations within the vehicle. This limits the ability of the command group to share a common operational picture when operating as a Tactical Operations Center.
  - The capability to support analog operations is degraded without the stowage for mapboards and plotting boards.
  - The ME vehicle seat stowage and litter lift are difficult to use. The program manager has identified a design change to correct this deficiency.
  - The MC ammunition storage is not optimized to support the mortar system.
  - There is water leakage from the hatch and the roof leaks affecting the electronics in all variants and patient care in the medical variants.
- Preliminary survivability assessment identified minor vehicle design vulnerabilities that the Program Office is addressing with the vendor in order to meet survivability and force protection requirements.
- Preliminary analysis of armor coupon testing demonstrated expected armor protection capabilities.
- DOT&E will summarize AMPV survivability findings in a classified LFT&E report to support the Full-Rate Production decision.
- The Adversarial Assessment built upon vulnerabilities identified during the CVPA and attempted to exploit those vulnerabilities using insider and near-sider attacks. The Army was not able to conduct outsider attacks during the LUT.

Recommendations

The Army should:

1. Mitigate the vulnerabilities identified in sub-system level testing to meet the survivability and force protection requirements.
2. Ensure AMPV FUSL testing is executed in accordance with the latest LFT&E guidance to include those related to employing buried underbody blast threats.
3. Correct critical deficiencies identified during the LUT prior to fielding the AMPV in support of EDI.

Army Tactical Missile System (ATACMS) Modification (MOD)

Executive Summary

- The Army converted the M39 and M39A1 Army Tactical Missile System (ATACMS) with anti-personnel and anti-materiel (APAM) bomblets to the M57 ATACMS 500-pound Unitary warhead using the same single warhead used in the Navy Harpoon missile.
- The Army integrated a proximity sensor into the M57 ATACMS Unitary to add an airburst mode and regain some area effects capability. The new missile is designated M57E1 ATACMS Modification (MOD).
- Seven of seven M57E1 ATACMS MOD missiles detonated with the required accuracy and height of burst. The Army conducted an operational test in March 2018. DOT&E published a classified report in September 2018.

System

- The ATACMS Service Life Extension Program converted the M39 and M39A1 ATACMS with APAM bomblets to the M57 ATACMS with a single 500-pound warhead. The M57E1 ATACMS MOD adds a proximity sensor.
- The Army re-grained the M39/M39A1 motor, updated obsolete navigation and guidance software and hardware, and replaced the M39/M39A1 APAM bomblets with the Navy Harpoon WDU-18/B warhead. The Army intends for the warhead change to meet the unexploded ordnance rate requirement defined in the 2017 DOD Policy on Cluster Munitions.
- The M57E1 ATACMS MOD missile uses Inertial Measurement Unit and GPS guidance to engage point and area targets out to a range of 300 kilometers.
- The M57E1 ATACMS MOD missile can be fired from the tracked M270A1 Multiple Launch Rocket System and the wheeled M142 High Mobility Artillery Rocket System.

Mission

Commanders use M57E1 ATACMS MOD missiles to engage long-range point or area-located targets including air defense, command posts, assembly areas, and high value targets without the hazard of unexploded submunitions.

Major Contractor

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

Activity

- In FY17, the Army conducted four system qualification tests of the M57E1 ATACMS MOD at White Sands Missile Range, New Mexico. Live fire testing consisted of two M57E1s fired against witness panels and two M57E1s fired against an array of three operationally representative targets.
- The Army conducted a soldier-executed user demonstration on September 14, 2017, in accordance with a DOT&E-approved test plan. During the test, a soldier crew fired one M57E1 against an array of six operationally representative targets.
- As part of the M57 ATACMS Unitary Stockpile Reliability Program, the Army fired a missile against the same array of targets as the M57E1 live fire tests. This allowed a comparison of effects with and without the airburst.
- In March 2018, the Army conducted an operational test of the M57E1 ATACMS MOD, in accordance with the DOT&E-approved test plan. The operational test consisted of two missiles fired against an array of targets with countermeasures, which are described in the DOT&E September 2018 classified report.

Assessment

- The M57E1 ATACMS MOD is operationally effective, operationally suitable, and survivable. The complete assessment can be found in the DOT&E September 2018 classified report.
- There were no reliability failures in the M57E1 ATACMS MOD testing. The M57E1 ATACMS MOD is the same design as the M57 ATACMS Unitary with the exception of the proximity sensor, thus it should have a similar reliability.
- The M57E1 ATACMS MOD met accuracy requirements.

Recommendation

1. The Army should address the recommendations found in the September 2018 classified report.

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

Executive Summary

- In 2018, the Army started live fire testing of the Bradley Engineering Change Proposal (ECP) to evaluate the survivability of the Bradley to threat-induced ballistic shock and underbody accelerative loads. The Army completed controlled damage experiments (CDE) and started with live fire system-level tests on prototype vehicles. Full-up system-level (FUSL) events using production-representative vehicles will be completed in FY20.
- Preliminary analysis of live fire testing did not reveal any unexpected vulnerabilities. DOT&E plans to complete detailed survivability analysis to support the ECP 2 Full Materiel Release decision in 4QFY20.
- The Army terminated the follow-on ECP 2b upgrade (designated as Bradley A5) in early June 2018 due to cost concerns. The Bradley A5 was intended to provide additional lethality and vehicle survivability improvements by FY25.

System

- The Bradley Family of Vehicles (BFoV) ECP program intends to integrate new technologies to mitigate the degradation of existing system performance. The ECPs are not intended to exceed the operational capability outlined in current system requirements documents.
- The initial ECP 1 phase was a suspension and track upgrade to restore ground clearance and suspension reliability because of increases in Bradley armor and weight. The follow-on ECP 2 phase will upgrade the electrical system and power train to restore lost mobility and integrate new technologies to improve situational awareness and vehicle survivability.
- Installation of ECP 1 and ECP 2 kits will result in the conversion of existing M2A3 and Operation Desert Storm – situational awareness (ODS-SA) versions of Bradley Fighting Vehicles into the M2A4 version and the M7A3 Bradley Fire Support Team vehicle into the M7A4 version.
- The current plan is to convert five brigades to the A4 variant and supply the European Deterrence Initiative with one brigade set of A4 vehicles. The A3/ODS-SA baseline configurations include the additional Bradley Urban Survivability Kits, Bradley Reactive Armor Tiles, and Add-on Armor Kit that the Army developed and fielded in response to Operational Needs Statements during Operation Iraqi Freedom. The A3 also includes the Commander's Independent Viewer.

Mission

Combatant Commanders employ Armor Brigade Combat Teams equipped with Bradley Fighting Vehicles to provide protected transport of soldiers, provide direct fires to support dismounted infantry, to disrupt or destroy enemy military forces, and to control land areas.

Major Contractor

BAE Systems Land and Armaments – Sterling Heights, Michigan

Activity

- In September 2016, DOT&E approved an updated Test and Evaluation Master Plan to support the production contract award for ECP 2 for June 2017. Government changes in desired quantity, late delivery of the contractor proposal, and increased contractor cost per vehicle estimates resulted in a slip in the production contract award to 3QFY18.
- In 2018, the Army completed CDE in support of the LFT&E program. The LFT&E program largely consists of two phases: Phase I or system-level tests on prototype vehicles, and Phase II or FUSL events on production vehicles. The Army will complete Phase I in FY18 and Phase II in FY20 to

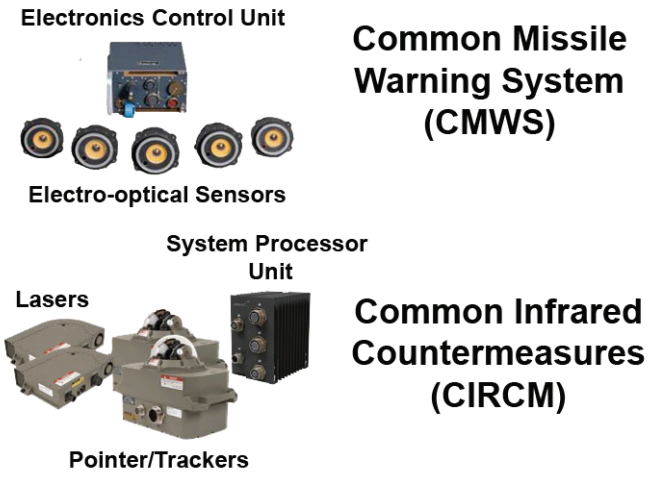
evaluate system vulnerability to threat-induced ballistic shock and underbody accelerative loads.
- The Army continued efforts in 2018 to test and improve M2A4 ECP reliability through developmental testing.
- In June 2018, the Program Office canceled the follow-on ECP 2b upgrade (designated as Bradley A5), which was intended to provide additional lethality and vehicle survivability improvements by FY25.

Assessment
- Preliminary analysis of live fire testing did not reveal any unexpected vulnerabilities. DOT&E intends to complete a detailed survivability assessment in FY20. The survivability assessment will include results from Bradley reactive armor tile tests completed in FY16, CDEs, automatic fire extinguishing system tests, system-level tests, FUSL, and modeling and simulation. This analysis will support the ECP 2 Full Materiel Release decision in 4QFY20.
- The hydro-mechanical power transmission (HMPT) 800B series was the original transmission selected for the M2A4 and M7A4 ECP. Problems identified with the HMPT 800B series during developmental testing resulted in the Army deciding to replace the HMPT 800B series with the existing HMPT 800 series.

Recommendations
None.

Common Infrared Countermeasures (CIRCM)

Executive Summary
- The Army accomplished laboratory tests, free flight live missile tests, and flight tests as part of an operational assessment that concluded in August 2018. DOT&E provided the Army a classified operational assessment of the Common Infrared Countermeasure (CIRCM) system to inform the Army September 2018 Milestone C decision.
- In general, the CIRCM system performed as intended. The pointer/trackers slewed to the missile locations designated by the missile warning system and the lasers provided effective jamming.
- Operational flight tests did not provide enough hours to assess the CIRCM system reliability requirement; however, system reliability to date indicates CIRCM is on track to meet the requirement at the conclusion of IOT&E.



System
- The CIRCM system is a defensive system for aircraft, which is designed to defend against surface-to-air infrared missile threats.
- The system combines the Army's legacy Common Missile Warning System (CMWS) consisting of ultraviolet missile warning sensors and electronics control unit (ECU) with the CIRCM system consisting of two lasers, two pointer/trackers, and a system processor unit. If CMWS detects a probable threat to the aircraft, it passes the tracking information for that possible threat to the CIRCM processor, which directs the pointer/trackers to slew to and jam the threat with laser energy. Simultaneously, the CMWS processor continues to evaluate the possible threat to determine if it is a real threat or a false alarm. If CMWS declares the detection to be an actual threat, it notifies the aircrew through audio alerts and a visual display on the aircraft Multi-function Display (MFD) in the cockpit, while also releasing flares as a secondary countermeasure.

Mission
- Commanders employ Army rotorcraft equipped with the CIRCM system to conduct medium and heavy lift logistical support, medical evacuation, search-and-rescue, armed escort, and attack operations. Commanders employ Army fixed-wing aircraft equipped with the CIRCM system to conduct personnel transport, electronic warfare, and logistic support.
- During Army missions, the CIRCM system is intended to provide automatic protection for fixed- and rotary-wing aircraft against shoulder-fired, vehicle-launched, and other infrared missiles.

Major Contractor
Northrop Grumman, Electronic Systems, Defensive Systems Division – Rolling Meadows, Illinois

Activity
- The Army accomplished the following testing to support an operational assessment of the CIRCM system:
  - Operational-mode testing of CMWS and CIRCM to determine system performance timelines at the Integrated Threat Warning Laboratory (ITWL), Wright Patterson AFB, Ohio, from October 18, 2017, through April 17, 2018.
  - Closed-loop hardware-in-the-loop (HWIL) simulations to show the effects of the CIRCM system on actual threat missile system hardware at the Guided Weapons Effects Facility (GWEF), Eglin AFB, Florida, from November 6, 2017, through August 13, 2018.
  - CIRCM laser and jam code performance evaluations at various missile engagements for selected missile threats with and without flare interaction at the Threat Signal Processor in the Loop (T-SPIL), Naval Air Station China Lake, California, from January 18, 2018, through May 13, 2018.
  - Flight tests against missile simulators and in ultraviolet and infrared environmental clutter at Redstone Arsenal, Alabama; U.S. Army White Sands Missile Range, New Mexico; and Houston, Texas, from May 9 through July 31, 2018.

  - Free flight missiles fired at CIRCM system hardware (not installed in aircraft) at U.S. Army Dugway Proving Ground, Utah, from June 22 through July 28, 2018.
- The Army conducted most testing in accordance with the DOT&E-approved test plan but requested deferring littoral and snow clutter environmental testing until IOT&E. DOT&E approved the request.
- DOT&E provided the Army a classified operational assessment of the CIRCM system testing to inform the Army September 2018 Milestone C decision.

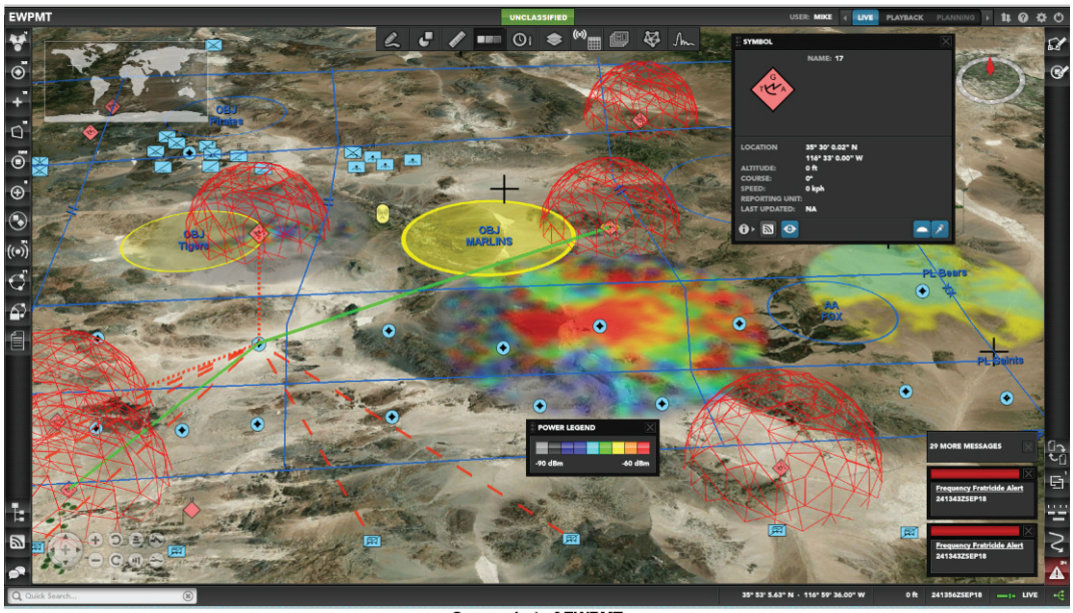
Assessment

- In general, the CIRCM system performed as intended. The pointer/trackers slewed to the missile locations designated by the missile warning system and the lasers provided effective jamming.
- The CIRCM system reliability requirement is 214 hours mean time between operational failures, which allows for a 95 percent chance of completing a typical 11-hour mission. The operational flight tests did not include enough hours to assess the 214-hour requirement. However, flight test data to date indicates CIRCM is on track to meet the requirement at the conclusion of IOT&E with a current measured reliability of 115 hours.

Recommendation

1. The Army should continue to collect reliability flight hours and make system improvements as necessary to ensure the system meets its reliability requirement.

Electronic Warfare Planning and Management Tool (EWPMT)



Screenshot of EWPMT

Executive Summary

- In response to a U.S. Army Europe (USAREUR) Operational Needs Statement (ONS), the Program Executive Office Intelligence Electronic Warfare and Sensors (PEO IEW&S) deployed an early version of the Electronic Warfare Planning and Management Tool (EWPMT) to conduct command and control of direct connect, non-networked sensors. The Army deployed this early capability, Raven Claw, in conjunction with Versatile Radio Observation and Direction Finding Modular Adaptive Transmitter (VMAX) and Sabre Fury. Collectively, this capability is referred to as USAREUR ONS Phase I.
- DOT&E observed the employment of USAREUR ONS Phase I capabilities by the 173rd Airborne Brigade and 2nd Brigade/1st Infantry Division (2/1 ID) during Joint Warfighting Assessment (JWA) 18.1 at Hohenfels, Germany. JWA 18.1 provided an opportunity to observe initial employment of USAREUR ONS Phase I systems and collect operator feedback.
- The Army is in the process of restoring its tactical EW capabilities and personnel, and will need to continue to refine doctrine and systems.

System

- In response to a USAREUR ONS, the Army Rapid Capabilities Office selected EW capabilities for accelerated development and deployment under a proof of concept called "USAREUR ONS Phase I." This collection of capabilities includes Raven Claw, VMAX, and Sabre Fury. Raven Claw is a hardened laptop with an early version of EWPMT software from Capability Drop 1 and other software applications that physically connect to VMAX and Sabre Fury sensors. Dismounted soldiers use VMAX systems to direction find and jam. Sabre Fury is a vehicle-mounted system for direction finding and jamming. EW teams employ Raven Claw to capture sensor feeds, conduct analysis, and pass refined data back to the EW officer at the command post.
- EWPMT provides the EW officer, the electromagnetic spectrum manager, and the cyber electromagnetic activities cell, from battalion to theater level, with an EW battle management capability to plan, coordinate, and synchronize EW in support of the commander's tactical plan.
- EWPMT is a software application that will reside in the Command Post Computing Environment as a server-client web-based application and/or a server-client laptop configuration.
- EWPMT will provide the ability to conduct remote control and management of networked EW assets to conduct offensive and defensive electronic attack, EW targeting, and synchronization of EW and spectrum management operations.
- Increment 1 consists of four capability drops with each successive drop building on the previous baseline.
  - Capability Drop 1: EW planning and targeting
  - Capability Drop 2: Spectrum management
  - Capability Drop 3: Disconnected, intermittent, and latent integration of USAREUR ONS Phase I sensors
  - Capability Drop 4: EW effectiveness, remote control and management, and enhanced targeting
- USAREUR ONS Phase II will provide additional sensor capabilities to the field in FY19.

Mission

- A unit equipped with EWPMT plans, coordinates, and synchronizes EW throughout the operations process. Staff from battalion through theater employ EWPMT to manage EW capabilities and integrate battlefield information and management systems into mission command systems.

- The Army intends a brigade equipped with USAREUR ONS Phase I systems to be capable of conducting spectrum situational awareness, EW planning, dismounted and vehicle-based direction finding and electronic attack.

Major Contractor
Raytheon Space and Airborne Systems – Fort Wayne, Indiana

Activity
- The PEO IEW&S deployed USAREUR ONS Phase I to three active duty brigades in Europe: 173rd Airborne Brigade, 2/1 ID, and 2nd Armored Cavalry Regiment.
- The 173rd Airborne Brigade and 2/1 ID employed USAREUR ONS Phase I systems during the JWA 18.1 in April through May 2018 at Hohenfels, Germany. Joint Modernization Command conducted JWA at the Joint Multinational Readiness Center. JWA 18.1 was a coalition-level force-on-force training exercise.
- JWA 18.1 provided an opportunity to observe employment and collect operator feedback on USAREUR ONS Phase I systems. Since JWA 18.1 was a training exercise, the Army did not develop an operational test plan for DOT&E approval.

Assessment
- DOT&E used JWA as an opportunity to gain early insights into initial employment and capabilities of USAREUR ONS Phase I systems and collect operator feedback.
- The EW operators collected spectrum emissions with VMAX and Sabre Fury, and determined lines of bearing with the Raven Claw Laptop. As a proof-of-concept, the EW teams notionally demonstrated the ability to pass data from VMAX and Sabre Fury through Raven Claw to the brigade headquarters. Given the nature of the event, DOT&E could not verify the capability to move data accurately and consistently.
- The Army is in the initial stage of rebuilding EW capabilities lost after the end of the Cold War. During JWA 18.1, the 173rd and 2/1 ID employed their USAREUR ONS Phase I equipment and personnel differently. The 173rd organized the EW equipment and personnel underneath the brigade's Military Intelligence Company. 2/1 ID created a section of EW crews underneath the brigade EW officer in the S-3 section. The current Army publications do not have the fidelity to assist units with refining their tactics, techniques, and procedures and organizing and employing tactical EW.
- The procedures for coordination between intelligence and EW are evolving. As the Army refines doctrine, it will need to place emphasis on coordination between EW and intelligence to provide EW crews with the essential information required to discern between friendly and enemy signals.
- As fielded at JWA 18.1, the 2/1 ID EW teams deployed in High Mobility Multipurpose Wheeled Vehicles (HMMWVs) with shelters limited to two crew members. Two soldiers are not sufficient to conduct 24-hour operations. EW teams in HMMWVs could not keep up with scout security elements. Soldiers were concerned that the HMMWV with shelter posed a rollover hazard in rough terrain.
- The 173rd EW Crews operating in Mine Resistant Ambush Protected (MRAP) – All Terrain Vehicle (M-ATVs) did not have the appropriate equipment (computers, cables, etc.) installed to network with VMAX systems. The effect was no depiction of dismounted direction finding information displayed in the Raven Claw. While M-ATVs provided improved mobility and protection, they do not have the deployability necessary for an airborne unit.
- Due to the lack of detailed terrain elevation map data, EW teams were not able to provide accurate planning models to the commander.
- Soldiers commented that the startup process for Raven Claw was too long and required multiple passwords.
- To date, the Army has not conducted cybersecurity testing on USAREUR ONS Phase I systems.

Recommendations
The Army should:
1. Conduct a Cooperative Vulnerability and Penetration Assessment and Adversarial Assessment as soon as practicable.
2. Consider integrating USAREUR ONS Phase I capabilities in vehicles appropriate for the brigade's mission.
3. Continue to refine doctrine to support tactical EW employment.

Javelin Close Combat Missile System – Medium

Executive Summary
- In FY18, the Army continued development of the Spiral 3 missile and a new Light Weight Command Launch Unit (CLU). The Army intends these efforts to reduce unit cost and weight while maintaining or improving system performance.
- In FY18, the Army conducted 22 Spiral 3 static penetration tests. Two additional static tests remain. Early indications from Spiral 3 static penetration testing showed no differences between the Spiral 3 and Spiral 2 warhead (behind seeker) performance.
- DOT&E and the Army continue to plan and execute the testing required for the Spiral 3 missile and Light Weight CLU developments. The Test and Evaluation Master Plan (TEMP) and Live Fire Strategy are under development and expected to be submitted for approval in FY19.

System
- The Javelin Close Combat Missile System – Medium is a man-portable, fire-and-forget, anti-tank guided missile.
- The Javelin system consists of a missile in a disposable launch tube assembly and a reusable CLU. The CLU mechanically engages the launch tube assembly 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. An operationally ready Javelin system weighs 48.3 to 48.8 pounds, depending on the variant.
- The Javelin missile employs a tandem shaped-charged warhead to defeat vehicle armor and can be fired in direct-attack or top-attack modes.
- The Army initiated four Javelin system improvements to reduce unit cost and weight and improve lethality against non-armored targets. These improvements are referred to as Spiral 1, 2, 3, and Light Weight CLU.
  - The Spiral 1 effort replaced electronic components in the control actuator section of the missile for cost and weight savings. Production missiles are designated FGM-148E.
  - The Spiral 2 effort utilizes the legacy Precursor Warhead (PCWH), and a newly developed Multipurpose Warhead (MPWH) that uses enhanced fragmentation to improve lethality against non-armored targets and personnel in the open while maintaining lethality against armored threats. Production missiles are designated FGM-148F.
  - The Spiral 3 effort develops a new launch tube assembly and battery unit, and will replace the current gas-cooled seeker with an uncooled seeker in the guidance section of the missile. Production missiles will be designated FGM-148G.
  - The Light Weight CLU effort develops a new CLU that is smaller and lighter while maintaining or improving system performance.

Mission
- Commanders use Army and Marine Corps ground maneuver units equipped with the Javelin to destroy or repel enemy assault through maneuver and firepower.
- Service members use the Javelin to destroy threat armor targets and light-skinned vehicles, and to incapacitate or kill threat personnel within fortified positions. In recent conflicts, Javelin was used against enemy bunkers, caves, urban structures, mortar positions, snipers, and personnel emplacing IEDs.

Major Contractors
- Raytheon – Tucson, Arizona
- Lockheed Martin – Orlando, Florida

Activity
- In FY18, the Army conducted 22 Spiral 3 static penetration tests: 18 of the static tests were Penetration Versus Standoff tests and 4 were warhead through seeker comparison tests. Two additional static tests remain.
- The Army conducted all testing in accordance with the draft LFT&E Strategy. To prevent delaying the test program, DOT&E approved the execution of the static penetration test series in accordance with the draft LFT&E Strategy.

- In FY18, DOT&E, the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation, and the Army continued test planning for the Spiral 3 missile and Light Weight CLU. A Live Fire Strategy and a combined OT&E/ LFT&E Concept were developed for the Spiral 3 missile. The Javelin Program Office began a comprehensive update to the TEMP. The TEMP and Live Fire Strategy are expected to be staffed and approved in FY19.

Assessment

Early indications from Spiral 3 static penetration testing showed no differences between the Spiral 3 and Spiral 2 warhead (behind seeker) performance. Additional flight and static tests against realistic targets are planned to confirm performance for additional operational conditions.

Recommendations

None.

Joint Air-to-Ground Missile (JAGM)

Executive Summary

- In pre-Milestone C testing, the Joint Air-to-Ground Missile (JAGM) met the Key Performance Parameter (KPP) for probability of hit and met the inflight reliability requirement.
- The pilot vehicle interface for launching JAGM from legacy Apache aircraft was adequate for testing but not suitable for combat, training, or fielding.
- The Army discovered minor vulnerabilities during cybersecurity and electromagnetic environmental effects (E3) testing. The cybersecurity Adversarial Assessment (AA) confirmed that a missile vulnerability discovered during the Cooperative Vulnerability and Penetration Assessment (CVPA) had been eliminated. The vulnerability discovered during E3 testing was eliminated. The AA highlighted a new vulnerability to the missile when mounted on the Apache.
- JAGM maintains the lethality of the legacy HELLFIRE Romeo against target-representative light and heavy armored ground combat vehicles, trucks, and boats. The Army is working on adjusting the fuse delay timing to improve JAGM lethality against bunkers, adobe walls, and personnel in the open to either meet or exceed legacy lethality against these targets.

System

- JAGM is an air-to-ground, precision-guided missile with two new seekers that replicate and combine capabilities of the existing laser-guided HELLFIRE Romeo and radar-guided Longbow HELLFIRE missiles.
- Attack helicopter aircrews using JAGM will have added flexibility to engage targets with dual-seeker engagement modes to optimize missile performance while minimizing aircraft exposure to enemy observation and fire.
- JAGM dual-seeker modes enable aircrews to destroy targets obscured by countermeasures or obscurants, provide target location updates to an inflight missile, avoid alerting enemy vehicles of imminent attack, avoid unwanted collateral damage, and engage multiple targets quickly.
- The JAGM design combines two sensor technologies – semi active laser and millimeter wave (MMW) radar – into a single seeker and guidance system and mated it to the HELLFIRE Romeo warhead, motor, and flight control systems.
- The HELLFIRE Romeo warhead Integrated Blast and Fragmentation Sleeve (IBFS) detonates with a programmable delay fuse and a Height-of-Burst (HOB) feature. This updated warhead blast provides a capability to engage armored vehicles while the IBFS and HOB feature is designed to engage personnel in the open. The programmable delay allows time for the warhead to penetrate deep into a building, bunker or lightly armored vehicle before detonating to incapacitate the personnel and destroy the equipment inside.

Mission

Army and Marine Corps commanders intend to employ JAGM from rotary-wing and unmanned aircraft to engage enemy combatants in stationary and moving armored and unarmored vehicles, within complex building and bunker structures, in small boats, and in the open.

Major Contractor

Lockheed Martin Corporation, Missiles and Fire Control Division – Grand Prairie, Texas

Activity

- The Army conducted environmental testing in 2016 and 2017 by exposing JAGM missiles to extreme but realistic temperatures and repeated handling and transportation stresses. The Army fired seven of these missiles during missile flight testing without failure.
- The Army completed E3 testing, a logistics demonstration, and chemical agent testing. The Navy conducted shipboard compatibility testing. Soldiers loaded and unloaded JAGM from an AH-64D Apache helicopter while wearing chemical protection gloves and clothing during the logistics demonstration. Army laboratories tested the resilience of the JAGM dome to chemical agents and to chemical decontamination. The Navy tested the suitability of shipboard equipment for storing JAGM and arming aircraft.

- The JAGM Program Office developed a high-fidelity, all-digital simulation model to complement the test program and estimate hit performance throughout the engagement envelope. The Integrated Flight Simulation (IFS) includes a six degree-of-freedom missile model, tactical flight software, scene generation models for laser and MMW scenes, target models, clutter models, aircraft models, atmospheric models, and countermeasure models.
- Cybersecurity testing included a CVPA and an AA; both conducted at Redstone Arsenal, Alabama. The Army Research Laboratory Survivability/Lethality Analysis Directorate conducted the CVPA in a laboratory using a JAGM guidance section attached to a missile launcher. The Threat Systems Management Office conducted an AA in an aircraft hangar with a JAGM and missile launcher attached to an AH-64D aircraft.
- The JAGM Program Office conducted integrated developmental/operational test shots of 49 missiles before Milestone C. The missile shots spanned the engagement envelope for target type, target speed, aircraft maneuvers, and range to target.
- The Army Test and Evaluation Command conducted a Limited User Test in January 2018 at Yuma Proving Ground, Arizona. Experienced pilots fired 10 missiles in all 4 JAGM engagement modes against stationary and moving targets in daytime conditions.
- During all phases of the Engineering and Manufacturing Development (EMD) live missile testing, 13 of the armored targets were obscured or covered by threat countermeasures (smoke, dust, radar reflectors, camouflage netting).
- Live fire testing in FY18 included flight tests against light and heavy armored ground combat vehicles, trucks, boats, and personnel in the open, in bunkers and behind adobe walls. These tests were adequate to characterize any performance effects of the newly integrated seeker on the existing, HELLFIRE Romeo-based warhead, as well as to demonstrate JAGM lethality against the intended targets.
- The Army conducted all pre-Milestone C operational and live fire testing in accordance with DOT&E-approved TEMP and test plans.

Assessment

- In pre-Milestone C testing, JAGM met hit performance and reliability requirements. JAGM demonstrated performance requirements for probability of hit, even though many of the targets were obscured by countermeasures or dust. The IFS provided valid hit-point estimates for 23 shots; information that was used to confirm that JAGM maintains lethality of the HELLFIRE Romeo missile. JAGM demonstrated its inflight and overall reliability requirements with the live missile shots.
- JAGM maintains the lethality of the HELLFIRE Romeo missile against light and heavy armored vehicles, trucks, and boat targets. JAGM met its lethality requirements against bunkers, adobe walls, and personnel in the open. The Army is working on optimizing the fuse delay timing to improve lethality against these targets to either match or exceed HELLFIRE Romeo performance.
- The pilot vehicle interface for launching JAGM from legacy Apache aircraft enabled operational testing but is not suitable for combat, training, or fielding. Programming the aircraft and missile to fire a single missile requires approximately 40 steps and 5 minutes of dedicated operator attention. The Apache program has developed software to recognize JAGM and enable pilots to efficiently employ all JAGM operational modes. The new Apache interface will support integrated and operational testing of JAGMs in 2019.
- Minor vulnerabilities were discovered during cybersecurity and E3 testing. The cybersecurity AA confirmed that a missile vulnerability discovered during the CVPA had been eliminated. The vulnerability discovered during E3 testing was eliminated. The AA demonstrated a new vulnerability to the missile when mounted on the Apache.

Recommendations

The Army should:

1. Complete development and testing of an efficient pilot vehicle interface for employment of JAGM from the AH-64E aircraft.
2. Complete development and validation of the IFS to estimate JAGM performance and lethality across the employment envelope and in expected operational terrain and conditions.
3. Investigate JAGM performance in flight testing against targets in realistic expected operational terrain and conditions.
4. Optimize and demonstrate adjusted JAGM fuse timing to further improve JAGM lethality against personnel in the open, personnel behind adobe walls, and personnel in bunkers.
5. Coordinate between the JAGM and AH-64E Program Managers to address the vulnerability found during the AA.

Joint Assault Bridge (JAB)

Executive Summary
- In FY18, the Army completed the LFT&E program to assess platform survivability against a spectrum of operationally realistic threats. The LFT&E program included Automatic Fire Extinguishing System (AFES) tests, armor tests, ballistic components tests, controlled damage experiments (CDEs), system-level tests, and full-up system-level (FUSL) tests. Preliminary assessments demonstrate that the current vehicle design requires some material fixes to achieve the Key Performance Parameter requirements.
- DOT&E plans to complete a detailed classified Joint Assault Bridge (JAB) LFT&E report to support the Full-Rate Production (FRP) decision in 4QFY19.

System
- The JAB replaces the Wolverine and M48/M60 chassis-based Armored Vehicle Launched Bridge systems in the Armored Brigade Combat Team (ABCT) Brigade Engineer Battalions (BEB) and in Mobility Augmentation Companies (MAC) supporting ABCT operations.
- The JAB was also designed to support M1 Abrams-equipped units in Marine Air Ground Task Forces (MAGTF). The Army assumed the lead for the JAB program in 2010 after the Marine Corps canceled the program due to cost and performance concerns. The Marine Corps remains involved and is seeking to procure 28 JAB systems in collaboration with the Army.
- The design concept includes an overhauled M1A1 Abrams chassis with M1A2 heavy suspension, and a contractor designed and integrated hydraulics system to launch the Bridge.
- Program goals for JAB include adequate survivability, improved mobility ensuring freedom of maneuver, improved supportability, and enabling use of common battlefield communication suites.
- In 2015, the Army increased the JAB Acquisition Objective from 168 to 337 assets to support the Army force structure changes that affected the BEB and MAC. The increase in vehicle quantity changed the JAB to an Acquisition Category (ACAT) II program.
- The JAB program awarded the production procurement contract to DRS Technologies, Inc. after full and open competition in 3QFY16.

Mission
Commanders employ JAB to enable the ABCT and MAGTF to close with and destroy the enemy by maneuvering over natural and man-made obstacles that would otherwise prevent the BCTs freedom of maneuver.

Major Contractor
DRS Technologies, Inc. – St. Louis, Missouri

Activity
- In March 2018, the Army completed the LFT&E program in accordance with the DOT&E-approved Test and Evaluation Master Plan (TEMP) and test plan.
- LFT&E events included AFES, armor, ballistic components, CDEs, system-level, and FUSL tests against underbody blast mine threats and direct and indirect fire threats. LFT&E will support the 4QFY19 FRP decision.
- The Program Office is working on potential design changes to the vehicle to address vulnerabilities found during exploitation and FUSL testing. Follow-on testing will be conducted and is tentatively scheduled for 3QFY19 to determine if the vehicle design changes adequately mitigated the known vulnerabilities.

Assessment
- Preliminary survivability analysis identified vehicle design vulnerabilities that the Program Office is addressing with the vendor to consider design improvements.
- DOT&E plans to complete a detailed survivability analysis on the performance of the JAB against operationally relevant threats. This analysis will support the DOT&E classified JAB LFT&E report in FY19.

Recommendation

1. The Army should correct design deficiencies and vehicle vulnerabilities found in testing and validate those fixes and mitigation techniques in test.

Joint Light Tactical Vehicle (JLTV) Family of Vehicles (FoV)

General Purpose

Heavy Guns Carrier

Utility/Shelter Carrier

Close Combat Weapons Carrier

Executive Summary

- The Army Systems Acquisition Review Council (ASARC) Full-Rate Production (FRP) decision for the Joint Light Tactical Vehicles (JLTV) program is planned for December 2018.
- DOT&E submitted the JLTV Multi-Service Operational Test and Evaluation (MOT&E) report and classified LFT&E annex to Congress in October 2018.
- The JLTV General Purpose (GP), Heavy Guns Carrier (HGC), and Utility (UTL) variants are operationally effective for employment in combat and tactical missions.
- The JLTV Close Combat Weapons Carrier (CCWC) is not operationally effective for use in combat and tactical missions. The CCWC provides less capability to engage threats with the Tube-launched, Optically tracked, Wire-guided (TOW) missiles over the fielded High Mobility Multipurpose Wheeled Vehicle (HMMWV). The missile reload process is slow and difficult for crews.
- All JLTVs are not operationally suitable because of deficiencies in reliability, maintainability, training, manuals, crew situational awareness, and safety.
- JLTVs are survivable providing crew survivability against threshold and some objective threats required by the Capabilities Production Document and other limited threats that U.S. forces would likely encounter during future conflicts.

System

- The JLTV Family of Vehicles (FoV) is the partial replacement for the HMMWV fleet for the Marine Corps and Army. The Services intend JLTV to provide increased crew protection against IEDs and underbody attacks, improved mobility, and higher reliability than the HMMWV.
- The JLTV FoV consists of two mission categories: the JLTV Combat Tactical Vehicle, designed to seat four passengers, and the JLTV Combat Support Vehicle, designed to seat two passengers.
- The JLTV Combat Tactical Vehicle has a 3,500-pound payload and three mission package configurations:
  - General Purpose (GP) Variant
  - Heavy Guns Carrier (HGC) Variant
  - Close Combat Weapon Carrier (CCWC) Variant
- The JLTV Combat Support Vehicle has a 5,100-pound payload and one mission package configuration:
  - Utility (UTL) Prime Mover Variant that can accept a shelter
- As a result of General Motor's decision to discontinue the JLTV engine used during Engineering and Manufacturing Development, the JLTV program plans to field two vehicle versions: the JLTV A0 and A1. The JLTV A1 has a new Duramax engine that replaces the A0 engine.
- The program plans to procure approximately 49,099 vehicles for the Army, 9,091 vehicles for the Marines, and 80 vehicles for the Air Force.
- JLTVs are equipped with two armor levels: the A-structure, or base vehicle, which the Services intend to employ in low-threat environments, and the B-kit, an add-on armor kit,

for additional force protection against enhanced small arms, fragmentation, and underbody threats.

Mission
- Commanders employ military units equipped with JLTV as a light, tactical-wheeled vehicle to support all types of military operations. Airborne, air assault, amphibious, light, Stryker, and heavy forces use JLTVs as reconnaissance, maneuver, and maneuver sustainment platforms. Air Force units intend to employ JLTVs for security and special operations.
- Small ground combat units will employ JLTV in combat patrols, raids, long-range reconnaissance, and convoy escort.

Major Contractor
Oshkosh Corporation – Oshkosh, Wisconsin

Activity
- The Army Test and Evaluation Command (ATEC) completed the majority of Production Qualification Testing (PQT) and Reliability Qualification Testing (RQT) on the JLTV A1 by March 2018. The purpose of PQT was to ensure that the JLTV performance, reliability, weapons integration, and transportability met the requirements outlined in the JLTV Capabilities Production Document.
- RQT at Aberdeen Proving Ground (APG), Maryland, and Yuma Proving Ground (YPG), Arizona, accumulated over 32,000 combined miles to assess the A1 vehicle reliability.
- Transportability certification testing is ongoing at APG and Airborne Operational Test Directorate, Fort Bragg, North Carolina. The testing consists of strategic, internal and external air, and rail transport for transportability certification. ATEC completed the rail transportability testing in October 2018.
- In December 2017, the program conducted the JLTV Maritime Prepositioned Force Shipboard Evaluation at Charleston, South Carolina. This assessment provided the program with information regarding the capability to embark, stow, maneuver, and disembark from decks on Maritime Sealift Command vessels.
- Low Velocity Air Drop Testing is ongoing at Fort Bragg, North Carolina. The testing is planned to be completed by April 2019.
- ATEC and the Marine Corps Operational Test and Evaluation Activity (MCOTEA) conducted the JLTV MOT&E at 29 Palms and Camp Pendleton, California, from February through April 2018 in accordance with the DOT&E-approved test plan. The Marine test unit completed two 96-hour major combat scenarios and the Army test unit completed one 96-hour major combat scenario and one 168-hour wide area security scenario.
- In December 2017, ATEC and MCOTEA completed the LFT&E program at APG in accordance with the DOT&E-approved test plan:
  - Full-up system-level live fire testing evaluated crew survivability and vehicle performance against mine and IED threats, overhead artillery, rocket-propelled grenades, and homemade explosives.
  - Ballistic cab testing characterized the explosively formed penetrator armor kit.
  - Exploitation testing evaluated the survivability of the JLTV against small arms and fragment simulating projectiles.
  - Fire survivability testing was performed to determine if the Automatic Fire Extinguisher System (AFES) could detect and extinguish fires without injuring the crew with toxic gases or excess extinguishing agent.
- In October 2018, DOT&E submitted the JLTV MOT&E Report and classified LFT&E annex to Congress to support the ASARC JLTV FRP decision.
- The JLTV Program Office completed the JLTV FRP Test and Evaluation Master Plan (TEMP) Annex in October 2019 to support Engineering Change Proposals and correction of vehicle deficiencies based on performance demonstrated in the MOT&E and developmental testing. The Army did not submit the JLTV TEMP Annex for OSD approval prior to FRP.
- The JLTV FRP decision is planned for December 2018.
- MCOTEA plans to observe and collect data on the JLTVs integrated into Marine Expeditionary Unit operations during pre-deployment training with the first JLTV-equipped unit in the fourth quarter of 2019 and first quarter 2020.
- The program plans to implement corrective actions to the CCWC field of fire to meet user TOW fire threshold requirements and investigate solutions to improve missile reload prior to fielding to Army and Marine units.
- The program intends to increase the duration of training, revise maintenance course content and documentation, and augment unit maintainers with on-site field service representatives as part of JLTV fielding.

Assessment
- Based on the MOT&E and the DOT&E 2014 Operational Assessment, the JLTV GP, HGC, and UTL variants are operationally effective for their employment in combat and tactical missions. The Army and Marine Corps units equipped with the JLTVs accomplished 17 of 24 major combat and wide-area security missions successfully employing the JLTVs. The majority of unsuccessful missions were attributed to combat losses. The single non-successful mission attributed to the JLTV was due to reliability failures.
- All JLTVs provide sufficient protected tactical mobility, are capable of negotiating complex terrain, and have the agility to react to changing tactical situations. The vehicles have the necessary command, control, and communications capabilities to support tactical decision-making. The HGC can deliver lethal and suppressive fires against the enemy.

- The JLTV towing the fielded M1102H trailer is not operationally effective for combat missions. The trailer has less mobility than the JLTV, which slowed the operational tempo of the test units. The Army has made no decision to procure the JLTV companion trailer.
- A unit equipped with JLTVs can sustain itself for 24 hours.
- The JLTV has large visual and loud aural signature increasing detectability.
- The CCWC is not operationally effective for employment in combat and tactical missions. The CCWC provides less capability to engage threats with the TOW missiles over the fielded HMMWV. The missile reload process is slow and difficult for crews. The CCWC has less storage space than other JLTV variants and accessing mission-essential equipment from the cargo area is a challenge.
- Marine Corps units can accomplish shore-to-shore amphibious operations on a non-contested beach.
- Marine Corps units can accomplish air assault missions with JLTVs with B-kit armor providing protected maneuver capability to counter threat activities at the landing zone.
- Army units equipped with JLTV can accomplish air assault missions with B-kit armor removed. JLTVs with B-kit armor installed exceed the vehicle gross weight limit of the external lift capability of the CH-47F helicopter.
- All JLTVs are not operationally suitable because of deficiencies in reliability, maintainability, training, manuals, crew situational awareness, and safety. JLTVs demonstrated less reliability than its requirement. The primary drivers of operational mission failures were engine wiring problems, flat and damaged tires, and break system faults.
- Units cannot maintain the JLTV without support from the contractor field service representatives due to vehicle complexity, ineffective training, poor manuals, and challenges with troubleshooting the vehicle. The JLTV will require more maintenance that the HMMWV based on the maintenance ratio demonstrated in the MOT&E.
- The health monitoring system is not accurate and reduces crew and maintainer confidence in the system.
- The maintainer training was not effective and required additional familiarization and hands-on time to increase the competency of military maintainers to troubleshoot the vehicle.
- Technical manuals were not useful because instructions were not detailed, incorrect, and lacked steps to troubleshoot problems.
- Crew has poor visibility due to blind spots around the vehicle.
- Crews had slow egress from JLTVs and numerous reliability failures of doors not opening impeded the ability of the soldiers and marines to safely ingress and egress the JLTV.
- Fewer JLTVs can fit on Maritime Prepositioned Force ships than HMMWVs. Ship load planners will need to reconfigure loads to store required amount of JLTVs.
- The JLTV provides force protection against threshold and some objective threats required by the Capabilities Production Document that U.S. forces would likely encounter during future conflicts.
- The AFES extinguished all fires without causing any toxic-gas induced crew injuries.

Recommendation

1. The program should develop a plan to address the recommendations identified in the DOT&E MOT&E Report and LFT&E classified annex.

M109A7 Family of Vehicles (FoV) Paladin Integrated Management (PIM)

Executive Summary

- The Army began the second M109 Family of Vehicles (FoV) Paladin Integrated Management (PIM) IOT&E on February 26, 2018, at Fort Riley, Kansas.
- The results from the second IOT&E indicate that the system is operationally effective. The Self-Propelled Howitzer (SPH) demonstrated accurate artillery fires, and both the SPH and the Carrier Ammunition Tracked (CAT) conducted movement and maneuver sufficient to keep pace with an Armored Brigade Combat Team.
- The SPH is operationally suitable in environments that require the SPH to fire Modular Artillery Charges 1-4. The SPH is not operationally suitable in environments that require the highest propelling charge, Modular Artillery Charge 5H.
- The CAT resupply vehicle is operationally suitable. The CAT exceeded its reliability and availability requirement.
- The M109A7 SPH met operational availability and maintainability requirements. The Army may need to stockpile spare breech- and cannon-related parts to support operations in a high-intensity environment.
- In the second IOT&E, the Army updated technical manuals to address methods to mitigate toxic fumes, to amplify system maintenance requirements, and to prescribe recurring breech subcomponent preventive and corrective maintenance tasks.
- In July 2018, DOT&E submitted a report to Congress for the second IOT&E.
- The Army plans to continue developmental testing of the M109A7 FoV PIM weapons firing to address planned improvements to the breech and increased reliability. The Army will conduct missions with soldier crews as part of the breech reliability testing to address those missions not completed during the IOT&E.

System

- The M109 FoV PIM program consists of two vehicles: the SPH and CAT resupply vehicle.
  - The M109A7 SPH is a tracked, self-propelled 155 mm howitzer designed to improve sustainability over the legacy M109A6 howitzer. The Army is updating the breech based on results from testing in the second IOT&E.
  - The M992A3 CAT supplies the SPH with ammunition. The ammunition carriers have a chassis similar to the SPH. The ammunition carriers are designed to carry 12,000 pounds or 98 rounds of ammunition in various configurations. A crew of four soldiers operates the CAT.
  - The Army will equip the SPH and CAT with two armor configurations to meet two threshold requirements for force protection and survivability – Threshold 1 (T1) and Threshold 2 (T2).
  - The base T1 armor configuration is integral to the SPH and CAT. The Army intends the T2 configuration to meet protection requirements beyond the T1 requirement with add-on armor kits.
  - The Army plans to employ PIM vehicles in the T1 configuration during normal operations and will equip the SPH and CAT with T2 add-on armor kits during combat operations.
- The Army designed an underbody kit to determine the potential protection an SPH and CAT could provide against IEDs similar to those encountered in Iraq and Afghanistan. The Army purchased five underbody kits for test purposes. The Army does not intend to equip the SPH or CAT with the underbody kit at this time.
- The Army intends to employ the M109 FoV as part of a Fires Battalion in the Armored Brigade Combat Team and Artillery Fires Brigades. The Army plans to field up to 689 sets of the M109 FoV with full-rate production planned for FY19.

Mission

Commanders employ field artillery units equipped with the M109 FoV to destroy, defeat, or disrupt the enemy by providing integrated, massed, and precision indirect fire effects in support of maneuver units conducting unified land operations.

Major Contractor

BAE Systems – York, Pennsylvania

Activity

- The Army began the final unit training for the second IOT&E in January 2018. The IOT&E began with the pilot test on February 26; record test vignettes began on March 8; and the operational test ended on March 21. The Army conducted testing in accordance with a DOT&E-approved Test and Evaluation Master Plan (TEMP) and test plan.
- The Army conducted a second cybersecurity test in accordance with a DOT&E-approved test plan.
- DOT&E submitted a report to Congress for the second IOT&E in July 2018 and the LFT&E report in June 2018.
- The Army will continue to conduct developmental testing to address breech reliability fixes and will address missions not fired during the IOT&E, such as firing the Modular Artillery Charge System 5H at high quadrant elevation, in an excursion event with soldier crews as part of the breech reliability testing.
- The Army is developing concepts for design and production of an extended range cannon and breech assembly.

Assessment

- The M109A7 FoV PIM system is operationally effective. A field artillery unit equipped with the SPH provided accurate artillery fires. Both the CAT and SPH showed significant improvement over the speed and maneuverability demonstrated by the legacy ammunition carrier and howitzer; movement and maneuver was sufficient to keep pace with an Armored Brigade Combat Team.
- The SPH is operationally suitable in environments that require firing Modular Artillery Charges 1-4. In environments that require Modular Artillery Charge 5 with high rates of fire, volumes of fire, and range, such as those envisioned by the Army Operational Mode Summary/Mission Profile (OMS/MP), breech- and cannon-related subcomponent failures frequently prevented achievement of Army reliability and responsiveness standards.
  - In the IOT&E, breech- and cannon-related sub-component failures were the most common failure. The breech is a legacy component from the fielded M109A6 SPH and was not changed as part of the M109A7 PIM program. During the IOT&E, the cannon artillery unit equipped with the M1097A7 SPH generated a high demand for repair parts to correct the frequent failures and maintain operational availability consistent with Army requirements.
  - Since the first IOT&E, the Army began implementing a two-phased approach to correct legacy breech reliability failures. Phase one addresses subcomponents of the legacy breech; phase two comprises more comprehensive design changes for the gun mount and cradle. Neither phase changes the basic breech design. The Army implemented the phase one changes during the second IOT&E. The Army plans to implement and test the phase two breech changes in FY19 and 20. DOT&E will observe the firings.
- The Army updated technical manuals and training to address methods to mitigate toxic fumes, to amplify system maintenance requirements, and to prescribe recurring breech subcomponent preventive and corrective maintenance tasks.
- The M109A7 SPH met the Army's availability and maintainability requirements. It did not meet reliability requirements. The CAT did very well and met both its reliability and availability requirements.
- The Program Office made progress in correcting deficiencies identified in previous cyber testing. The results of the second cyber test can be found in the classified annex to the July 2018 DOT&E report.
- The Program Office has taken action to correct deficiencies identified in early testing and to validate associated fixes over the course of the Developmental Performance, Automotive, and LFT&E program.
  - During armor exploitation testing, most of the modified armored areas demonstrated that they provide protection against Key Performance Parameter threats.
  - Changes to the CAT crew compartment Automatic Fire Extinguisher System (AFES) mitigate the deficiency identified in early testing and reduce its vulnerability to fires.
- The crew compartment AFES in the SPH was designed to protect a small, localized area and is deficient in providing adequate fire survivability. The Program Office is developing courses of action to redesign this system and improve SPH crew survivability to fires. While not yet optimized, the M109A7 provides improved crew fire safety compared to the currently fielded M109A6 because:
  - The M109A7 has limited AFES capability in the crew compartment while the M109A6 has none.
  - The M109A7 has reduced fire hazards compared to the M109A6 because of the replacement of hydraulic systems, found on the M109A6, with electric drives.

Recommendations

The Army should:

1. Continue to pursue the final design, development, and integrated testing of a new cannon and breech assembly to address legacy breech and cannon reliability to mitigate range and rate of fire shortcomings in the M109A7 SPH.
2. Consider stockpiling breech parts with deployed artillery units or prepositioned fleets.
3. Resolve the identified cybersecurity vulnerabilities; refine tactics, techniques, and procedures relating to the identification of cybersecurity threat activity and responses.
4. Correct the deficiencies in the SPH's crew compartment AFES and validate those fixes in test.

MQ-1C Extended Range Gray Eagle Unmanned Aircraft System (UAS)

Executive Summary

- The Army conducted the MQ-1C Extended Range Gray Eagle Unmanned Aircraft System (UAS) FOT&E II, July 30 through August 17, 2018, in accordance with the DOT&E-approved Test and Evaluation Master Plan and operational test plan.
- DOT&E submitted an FOT&E II report in early FY19. In that report, DOT&E concludes:
  - The Extended Range Gray Eagle-equipped unit was effective at conducting Composite Flight Platoon (CFP) operations and can provide continuous multi-discipline intelligence collection, surveillance, reconnaissance, and precision strike support to combat units.
  - The Extended Range Gray Eagle-equipped unit demonstrated the ability to provide the time on-station at the operational range specified in the Army Capability Production Document.
  - The aircraft demonstrated a significant increase in endurance capability over the baseline Gray Eagle aircraft.
  - The Extended Range Gray Eagle system is operationally suitable.

System

- The Extended Range Gray Eagle Company UAS is composed of the following major components:
  - Twelve unmanned aircraft, each with a Common Sensor Payload with a high definition electro-optical/infrared (EO/IR) and a Laser Range Finder/Laser Designator capability, a STARLite Extended Range Synthetic Aperture Radar/Ground Moving Target Indicator (SAR/GMTI) radar, a Tactical Signals Intelligence Payload when fielded, and an Air Data Relay control capability
  - Each aircraft is equipped with a Standard Equipment Package that includes a communications relay package, Identification Friend-or-Foe equipment, and Air Traffic Control radios
  - Each aircraft has the ability to carry up to four HELLFIRE missiles
  - Six Ground Control Stations designated as the Universal Ground Control Station (UGCS)
  - Three Mobile Ground Control Stations (MGCS)

  - Nine Tactical Common Datalinks Ground Data Terminals
  - Three Satellite Communications Ground Data Terminals
  - Twelve Satellite Communications Air Data Terminals
  - Six Tactical Automatic Landing Systems
- The Army is initially fielding two Extended Range Gray Eagle UAS companies to the U.S. Army Special Operations Command, within the 160th Special Operations Aviation Regiment (SOAR) and the U.S. Army Intelligence and Security Command, within the Aerial Exploitation Battalions (AEB) of the 116th Military Intelligence Brigade.

Mission

The SOAR and AEBs employ Gray Eagle to support their core mission of continuous multi-discipline intelligence collection, surveillance, reconnaissance and precision strike during division, or echelons above division, offensive, defensive, and stability operations.

Major Contractor

General Atomics Aeronautical Systems, Inc., Aircraft Systems Group – Poway, California

Activity

- The Army conducted the MQ-1C Extended Range Gray Eagle UAS FOT&E II at Air Force Plant 42 Palmdale, California, and the National Training Center (NTC), Fort Irwin, California, July 30 through August 17, 2018, in accordance with the DOT&E-approved Test and Evaluation Master Plan and operational test plan.
- The FOT&E II unit conducted missions in support of a Brigade Combat Team and Special Operations Forces

conducting a training rotation at the NTC. This combination of testing with training created a realistic, challenging, and stressful test environment for the Gray Eagle CFP. The platoon flew 481 flight hours during the test.
- The Army collected data from the FOT&E II to assess the new MQ-1C capabilities and employment concepts. These include:
  - An aircraft endurance capability increase
  - The capacity of a CFP to conduct one 24-hour orbit on a continuous basis
  - Upgrades to the payloads and significant software functionality enhancements made to the system since the 2015 FOT&E
  - Employment concept from a company conducting split-based operations from two locations to the SOAR/AEB Company employment concept of deploying CFPs independently at disparate locations. The CFP consists of four Extended Range Gray Eagle aircraft, ground control equipment, two UGCS, one MGCS, three universal ground data terminals, one satellite communication ground data terminal, and an automatic take-off and landing subsystem
- DOT&E submitted a Gray Eagle FOT&E II report in early FY19.

Assessment
- During FOT&E II, the Extended Range Gray Eagle-equipped unit was effective at conducting CFP operations and could provide continuous multi-discipline intelligence collection, surveillance, reconnaissance, and precision strike support to combat units.
- The CFP demonstrated the capability to provide one 24-hour orbit on a continuous basis.
- The Extended Range Gray Eagle-equipped unit demonstrated the ability to provide the time on-station at the operational range specified in the Army Capability Production Document.
- The time and effort to perform routine aircraft maintenance has improved since the 2015 FOT&E. Aircraft design changes added new access panels and replaced captive fasteners with Arconic fasteners that enabled maintainers to complete tasks more quickly and reduced wear on fasteners. Greater accessibility to the avionics bay and other airframe areas improved maintenance efficiency.
- The Army has improved integration of the Gray Eagle capabilities into combined arms combat operations. Gray Eagle tactics, techniques, and procedures have matured since the 2015 FOT&E.
- The EO/IR and SAR/GMTI sensors provided imagery products that supported processing, exploitation, and dissemination of intelligence information.
- The Extended Range Gray Eagle system is operationally suitable.
- The Extended Range Gray Eagle demonstrated meeting reliability requirements specified in the Army Capability Production Document for the Ground Control Equipment, for the aircraft, and for the common sensor payload. It did not meet the reliability requirement for the SAR/GMTI radar.
- Even though the SAR/GMTI capability has improved since the 2015 FOT&E, a preponderance of the SAR/GMTI radar system aborts are attributed to operator error and complicated operational procedures. Soldiers described the sensor as difficult to operate and required frequent in-flight troubleshooting.
- The Gray Eagle cybersecurity posture has improved since the 2015 FOT&E, but the system remains vulnerable to cyber-attack.
- The design of the UGCS shelter has improved since the 2015 FOT&E, but has a number of deficiencies that reduce operator efficiency and increase operator stress and fatigue.
  - Operators reported that the government-furnished headsets became uncomfortable over a period of time and pose a health risk because the operators must share the few headsets. Toward the end of test, the unit procured commercial off-the-shelf headsets for crew member use. Survey feedback from soldiers reflected the commercially procured headsets were an improvement over the government-furnished headsets.
  - The Aviation Mission Planning System is not fully integrated into the UGCS set-up/starting procedures. Operators must manually input most pre-mission data.
- Due to insufficient cooling capability, when temperatures within the MGCS get excessive, there is potential for overheating of the electrical systems requiring the transfer of aircraft control to one of the other UGCSs. The process/procedure to transfer control during high heat conditions was in the standard operating procedures but not documented in the technical manual.

Recommendations

The Army should:
1. Increase reliability, simplify operating procedures, and improve training on the SAR/GMTI payload.
2. Simplify the transfer of the Aviation Mission Planning System mission data into pre-mission UGCS setup procedures through the use of a data transfer card much like that of manned aircraft systems.
3. Provide soldiers with better quality headsets that will reduce or eliminate operator discomfort and fatigue and issue them to each crew member to eliminate the health risks associated with the sharing of headsets.
4. Field the MGCS with an environmental control unit that is capable of cooling the shelter adequately. For the current MGCS, add the temperature limitations to the technical manuals to ensure that soldiers operating the MGCS are aware that it can potentially overheat and require transfer to a backup UGCS.
5. Eliminate the cybersecurity vulnerabilities and confirm corrections in follow-on testing.

Patriot Advanced Capability (PAC)-3

Executive Summary
- The Army concluded the Patriot Post Deployment Build (PDB)-8 IOT&E in November 2017. Data from the IOT&E supported the PDB-8 fielding and Patriot Advanced Capability (PAC)-3 Missile Segment Enhancement (MSE) Full-Rate Production decisions.
- The Army conducted one Patriot Missile Flight Test (MFT) in FY18, achieving intercepts of both close-range ballistic missile (CRBM) targets.
- Patriot demonstrated interoperability with the Terminal High-Altitude Area Defense (THAAD) system in a Missile Defense Agency (MDA) tracking exercise against a CRBM target.
- DOT&E issued a classified report on the results of the PDB-8 IOT&E in April 2018.

System
- Patriot is a mobile air and missile defense system that counters missile and aircraft threats. The latest version of Patriot hardware and software is PDB-8, which consists of improvements required to:
  - Counter the evolving threat
  - Improve combat identification and the Air Defense Interrogator Mode 5 Identification, Friend or Foe capability
  - Mitigate false tracks
  - Improve electronic protection
  - Integrate further the PAC-3 MSE interceptor/ground system capabilities
- The system includes the following:
  - C-band, multi-function, phased-array radars for detecting, tracking, classifying, identifying, and discriminating targets and supporting the guidance functions
  - Battalion and battery battle management elements
  - Communications Relay Groups and Antenna Mast Groups for communicating between battery and battalion assets

  - A mix of PAC-3 hit-to-kill interceptors and PAC-2 blast fragmentation warhead interceptors for negating missile and aircraft threats

Mission

Combatant Commanders use the Patriot system to defend deployed forces and critical assets from missile and aircraft attack and to defeat enemy surveillance air assets in all weather conditions.

Major Contractors
- Prime: Raytheon Company, Integrated Defense Systems – Tewksbury, Massachusetts (ground system and PAC-2 and prior generation interceptors)
- PAC-3 interceptor variants and PAC-3 Command and Launch System: Lockheed Martin Corporation, Missile and Fire Control – Grand Prairie, Texas

Activity
- The Army conducted testing in accordance with the DOT&E-approved Patriot System PDB-8 Test and Evaluation Master Plan and PDB-8 test plans and mission procedures.
- The Army conducted the PDB-8 IOT&E MFT-A2 in November 2017 at White Sands Missile Range (WSMR), New Mexico. During this test, Patriot conducted near simultaneous engagements and intercepted two CRBM targets using two mixed ripples of interceptors (PAC-3 MSE/PAC-3 Cost Reduction Initiative (CRI) and PAC-3 CRI/PAC-2 Guidance Enhanced Missile-Tactical (GEM-T)). This test was the final event in the PDB-8 IOT&E.
- DOT&E issued a classified report on the results of the PDB-8 IOT&E in April 2018.
- The MDA conducted Flight Test Other-35 (FTX-35) in April 2018 at WSMR. During this test, Patriot and THAAD tracked a CRBM target, exchanged messages over tactical datalinks, and conducted simulated engagements of the target.

Assessment

- During the PDB-8 MFT-A2, Patriot demonstrated the capability to detect, track, engage, intercept, and kill two CRBM targets using two mixed ripples of interceptors (PAC-3 MSE/PAC-3 CRI and PAC-3 CRI/PAC-2 GEM-T).
- During the MDA FTX-35 tracking exercise, Patriot demonstrated the capability to exchange track data, engagement coordination, and weapon engagement status messages with THAAD, and to detect, track, and perform a simulated engagement of a live CRBM target using two simulated PAC-3 missiles.
- Results from the PDB-8 IOT&E indicate that Patriot PDB-8 has comparable or improved effectiveness, suitability, and survivability compared with the Patriot PDB-7 system and that the PAC-3 MSE provides additional capability over previous PAC-3 missile variants, especially at higher altitudes and longer ranges. Patriot PDB-8 suitability is similar to PDB-7 suitability, with a continuation of long-standing shortfalls in reliability and training and new problems in human-systems integration (HSI). Patriot survivability improved between PDB-7 and PDB-8, but PDB-8 still has some survivability and cybersecurity shortfalls. Details can be found in the April 2018 classified DOT&E report. Data from the PDB-8 IOT&E supported the PDB-8 fielding and MSE Full-Rate Production decisions.

Recommendation

1. The Army should fix the HSI problems identified during the PDB-8 IOT&E.

Soldier Protection System (SPS)

Executive Summary

- The Soldier Protection System (SPS) consists of four subsystems. Each subsystem has its own acquisition strategy.
  - Torso and Extremity Protection (TEP)
  - Vital Torso Protection (VTP)
  - Integrated Head Protection System (IHPS)
  - -. Transition Combat Eye Protection (TCEP)
- The SPS TEP, VTP, IHPS, and TCEP met ballistic requirements.
- The Army made a Full-Rate Production decision for the TEP in September 2016 and for the IHPS in October 2018.
- Instead of making a Full-Rate Production decision on the current VTP, the Army plans to test a new, lighter-weight VTP design in 3QFY19.
- The Army will add TCEP to the Authorized Protective Eyeware List (APEL).

System

- The SPS is a suite of personal protection subsystems intended to provide equal or increased levels of protection against small-arms and fragmenting threats compared to existing personal protection equipment and at reduced weights. The SPS subsystems are designed to protect a soldier's head, eyes, and neck region; the vital torso and upper torso areas, as well as the extremities; and the pelvic region. Soldiers can configure the various components to provide different tiers of protection depending on the threat and the mission.
- The SPS consists of four subsystems:
  - VTP consists of front and rear hard armor torso plates, either the Enhanced Small Arms Protective Insert (ESAPI) or the X Threat Small Arms Protective Insert (XSAPI), along with the corresponding hard armor side plates Enhanced Side Ballistic Insert (ESBI) or the X Threat Side Ballistic Insert (XSBI).
  - TEP consists of the soft armor Modular Scalable Vest (MSV) with provision for adding the Ballistic Combat Shirt (BCS) for extremity protection, the Blast Pelvic Protector (BPP) for pelvic and femoral artery protection, and a Ballistic Battle Belt (B3) that provides the capability to redistribute some of the weight burden from the shoulders to the hips.
  - IHPS consists of a helmet with provision for adding a mandible and/or visor, as well as for mounting an applique to the outside of the helmet for additional ballistic protection.
  - TCEP consists of either ballistic spectacles or goggles to protect the soldier's eyes as well as provide the capability to transition from light to dark and dark to light in 1 second or less to enhance the soldier's vision in varying combat conditions.

- The Army plans to issue SPS via Rapid Fielding Initiative to deploying units rather than issue SPS to individual soldiers at each Army installation. The Army is developing plans to determine which soldiers will be individually issued SPS.

Mission

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

Major Contractors

- TEP Full-Rate Production Vendors/Designs (Multiple vendors to stimulate competition and achieve best price through Fair Opportunity awards):
  - KDH Defense Systems Inc. – Eden, North Carolina (MSV, BPP)
  - Bethel Industries Inc. – Jersey City, New Jersey (MSV, BPP)
  - Hawk Protection – Pembroke Pines, Florida (MSV, BPP)
  - Short Bark Industries – Venor, Tennessee (BCS)
  - Carter Enterprises Industries Inc. – Brooklyn, New York (BCS, B3)
  - Eagle Industries Unlimited – Virginia Beach, Virginia (BCS)
- IHPS Vendor:
  - 3M/Ceradyne – Costa Mesa, California
- VTP LRIP Vendors:

- BAE Systems – Chandler, Arizona (XSAPI, ESBI, XSBI)
- 3M/Ceradyne – Costa Mesa, California (ESAPI)

- TCEP Vendor:
  - Alpha Micron – Kent, Ohio

Activity

- While the SPS consists of four subsystems (TEP, VTP, IHPS, and TCEP), the development, testing, and production/fielding of the four subsystems have been on different timelines. The Army made a Full-Rate Production decision for the TEP in September 2016 and the IHPS in October 2018. Each SPS subsystem is compatible with existing (legacy) personal protective equipment (for example, soldiers can use existing hard armor plates in the new MSV).
- The Army tested TEP, VTP, and IHPS ballistic performance in accordance with DOT&E-approved test plans.
- The Army completed first article VTP testing in September 2017 and additional characterization of VTP performance against additional threats in February 2018. The Army intends to test a new, lighter-weight VTP in 3QFY19 and make a subsequent Full-Rate Production decision on this lighter-weight VTP design.
- The Army completed a series of first article and sub-system-level live fire tests of IHPS in December 2017. This testing began in August 2017 and included: (1) testing of the IHPS against various foreign threats, (2) characterization of the performance of the IHPS against blast threats, and (3) flash heat and fire threat testing to evaluate the IHPS's ability to protect an individual from flash fire induced burns. The Army plans to characterize IHPS against an additional foreign threat when that threat is available.
- The Army conducted first article testing of the TCEP in July 2017. While the lenses met ballistic requirements, the TCEP did not meet some non-ballistic requirements, so the vendor initiated action to correct the deficiencies. The Army completed TCEP First Article Test (third retest) in February 2018 and will add TCEP to the APEL.
- The Army plans to complete additional full-up system-level testing of the SPS (with all subsystems combined) against additional threats in 4FY19.

Assessment

- The SPS TEP, VTP, IHPS, and TCEP met ballistic requirements for first article testing.
- DOT&E documented the performance of the TEP subsystem in the report to Congress in September 2016, the VTP subsystem in April 2018, and the IHPS subsystem in May 2018.

Recommendations

The Army should:

1. Establish a credible correlation between threat-induced deformations in both the torso plates and combat helmet and the probability of injury.
2. Improve its free-field blast test methodology to enable a credible correlation between the blast pressure mitigation provided by the torso plate and combat helmet and the probability of blast-induced injury.
3. Improve its ability to model fragmenting threats against combat helmets and torso plates.

Spider Increment 1A M7E1 Network Command Munition

Executive Summary
- The Program Office conducted a Production Reliability Test (PRT) with technical experts and a Force Development Test (FDT) with soldiers in 2018.
- The Army Maneuver Support Center of Excellence lowered the reliability requirement in June 2018. The Remote Control Station (RCS) is now required to operate a Spider munition field for a 72-hour mission with a 91 percent chance of not having an Essential Function Failure (EFF). The original requirement was 96 percent chance of no EFFs.
- Spider Increment 1A has yet to meet the lowered reliability requirement. DOT&E assesses current demonstrated reliability is 81 percent based upon developmental testing. The Army reliability estimate is higher, which will preclude its application of successful corrective actions. The FDT demonstrated that units could employ Spider Increment 1A.
- During the August 2017 Cooperative Vulnerability and Penetration Assessment (CVPA), the Army demonstrated mitigation of most of the cyber vulnerabilities reported in the January 2017 DOT&E operational assessment. The Adversarial Assessment in October 2018 is intended to assess a unit's ability to operate in a cyber-contested environment.
- The Army conducted the Spider Increment 1A IOT&E in October 2018 at Fort Campbell, Kentucky.

System
- The Army uses Spider as a landmine alternative to satisfy the requirements outlined in the 2004 National Landmine Policy that directed the DOD to:
  - End use of persistent landmines after 2010
  - Incorporate self-destructing and self-deactivating technologies in alternatives to current persistent landmines
- A Spider munition field includes:
  - Up to 63 Munition Control Units (MCUs), each housing up to 6 miniature grenade launchers or munition adapter modules (the modules provide remote electrical firing capabilities)
  - An RCS consists of a Remote Control Unit (RCU) and RCU Transceiver (RCUT). An operator uses the RCS to maintain "man-in-the-loop" control of all munitions in a field. The RCU is the component upgraded in Spider Increment 1A.
  - A repeater or communications relay device for use in difficult terrain or at extended ranges

- Spider incorporates self-destructing and self-deactivating technologies to reduce residual risks to non-combatants and has the capability to use non-lethal munitions such as the Modular Crowd Control Munition that fires rubber sting balls.
- The Army fielded Spider Increment 1 systems in FY09 under an Urgent Materiel Release. The system reached Initial Operational Capability in FY11 and obtained its Full Materiel Release in FY13.

Mission
Brigade Combat Team commanders employ engineer units equipped with Spider to provide force protection and counter-mobility obstacles using lethal and non-lethal munitions. Spider functions either as a stand-alone system or in combination with other obstacles to accomplish the following:
- Provide early warning
- Protect the force
- Delay and attrite enemy forces
- Shape the battlefield

Major Contractor
Command and Control hardware and software: Northrop Grumman Information Systems Sector, Defense Systems Division – Redondo Beach, California

Activity
- The Army released several software updates for Spider Increment 1A since completing the LUT in 2016. In 2018, the Army made no software changes to address problems identified in testing. The Army made a hardware change to address a reliability issue. Other problems were addressed by changing the operating procedures and documenting those

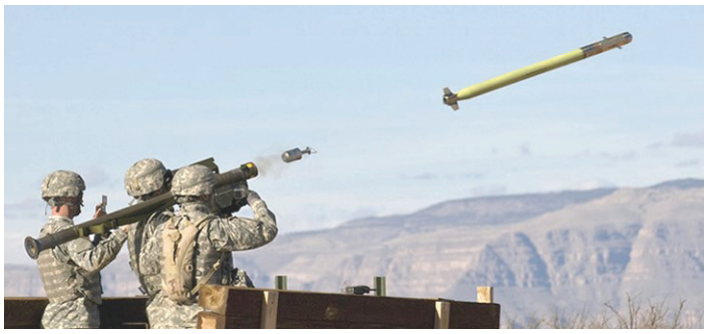
changes in the operator manuals and training programs of instruction.
- The Program Office conducted the Production Reliability Test (PRT) from January 29 through February 9, 2018, at Fort Leonard Wood, Missouri. The test was conducted in accordance with the DOT&E-approved Test and Evaluation Master Plan (TEMP).
- The Maneuver Support Center of Excellence conducted the FDT at Fort Hood, Texas, in April 2018. The FDT tested a unit's ability to operate Spider Increment 1A.
- The Army Engineering School lowered the Spider Increment 1A reliability requirement on June 26, 2018. The system is now required to operate a munitions field for 72 hours without an EFF, with 91 percent reliability rather than the original requirement of 96 percent.
- The Army Test and Evaluation Command (ATEC) delayed the IOT&E by 3 months to allow the Program Office to improve reliability and the operating manuals. ATEC continued planning for the IOT&E based on FDT results, validation tests of the operating manuals, and the reduction of the reliability requirement.
- The Army conducted the IOT&E in October 2018 in accordance with the DOT&E-approved TEMP and test plan.

Assessment
- The DOT&E operational assessment from the 2016 Limited User Test (LUT) found that a unit could employ Spider Increment 1A as a component of protection and counter-mobility missions, but not meet the Army reliability requirement.
- The CVPA found the updated software addressed many of the vulnerabilities identified in the 2017 DOT&E operational assessment. The Adversarial Assessment will provide information on the unit's ability to operate Spider Increment 1A in a cyber-contested environment.
- Spider Increment 1A did not meet its reliability requirement in developmental testing. DOT&E assesses Spider Increment 1A as having an 81 percent probability of completing a mission without a failure, which is below the adjusted 91 percent requirement. Spider Increment 1A is no longer required to send digital obstacle reports to the classified mission command system. At this time, there is no approved cross-domain solution allowing the unclassified Spider to pass digital information to the classified mission command system. This makes it more difficult for units to update the mission command system, which adversely affects the ability of units to know in real time where Spider fields are located on the battlefield.

Recommendation
1. The Army should update the current Increment 1A software to address known reliability problems rather than rely on changes in the operating procedures.

Stinger Proximity Fuze

Executive Summary
- The Army intends to add a proximity fuze (PROX) to the Stinger Block 1 missile to increase Stinger lethality against small and medium unmanned aircraft systems (UAS).
- The Army intends to field initial Stinger PROX missiles in support of the European Defense Initiative in FY19 followed by Full Material Release in FY21.
- During flight testing, the Army measured the PROX firing distance against static targets and demonstrated successful proximity intercept against free-flying targets. The Army intends to conclude flight testing in 2QFY19.



System
- First fielded in 1981, the FIM-92 Stinger is a shoulder-launched, fire-and-forget, short-range, man-portable, air defense weapon system. It provides low-altitude defense for ground forces against attack or observation by low-flying cruise missile, rotary-wing, fixed-wing, or UAS threats. The Stinger utilizes a high-explosive, hit-to-kill warhead. While typically fired by a two-man crew, the Stinger can also be operated by one person and adapted to fit on ground vehicles, helicopters, and UAS platforms.
- The Army initiated a Service Life Extension Program to extend the shelf life of expiring Stinger missiles by replacing missile components susceptible to degradation due to aging.
- The Army also initiated a PROX effort to improve effectiveness against UASs. The PROX effort integrates a Target Detection Device into the fuze to provide a proximity detonation capability. The Stinger PROX will upgrade the FIM-92E Stinger Block 1 and will result in the FIM-92J Stinger PROX missile.
- The Army plans to utilize its Urgent Material Release process to provide Stinger PROX missiles in support of the European Defense Initiative in FY19, followed by Full Materiel Release in FY21.

Mission
Army and Marine Corps commanders employ the Stinger missile system to defend ground forces and critical assets against low-level cruise missile, fixed or rotary-wing aircraft, and UAS attack or observation.

Major Contractors
- Raytheon Missile Systems – Tucson, Arizona
- Lockheed Martin Sippican – Marion, Massachusetts

Activity
The Army resumed flight testing against targets at Eglin AFB, Florida, in August 2018, conducting 22 flight tests against 12 static UAS targets, 9 free-flying UAS targets, and one hot plate target. The Army measured the PROX firing distance against the static targets and demonstrated successful proximity intercept against free-flying targets. The Army plans to conclude flight testing in January 2019.

Assessment
DOT&E will report on Stinger PROX performance upon test completion in FY19.

Recommendations
None.

Stryker 30 mm Infantry Carrier Vehicle – Dragoon (ICV-D)

Executive Summary

- The Army developed the Infantry Carrier Vehicle – Dragoon (ICV-D) in response to an Operational Needs Statement submitted by 2nd Cavalry Regiment (2CR) in March 2015. It is not a Program of Record. When fielding is complete, the 81 ICV-D will comprise 50 percent of the vehicles in the rifle and scout platoons in the 2CR.
- The Army conducted an Early User Test and Evaluation (EUT&E) from February through April 2018, and an LFT&E from April 2017 through February 2018. The EUT&E findings support the Army PEO Ground Combat Systems decision to field the ICV-D to the 2CR.
- When equipped with the ICV-D, the majority of infantry and scout platoons from the 2CR were able to qualify using the 30 mm automatic cannon and accomplish their assigned tactical task and purpose.
- The lethality upgrades of the ICV-D allow crews to detect, identify, and defeat targets at greater ranges and against a wider array of enemy targets than crews not equipped with the upgrades. Unit leadership unanimously stated they would rather take the ICV-D to combat against a near-peer threat than the legacy ICV.
- The platform met its reliability requirements for the turret and gun system without degrading the reliability of the base Stryker chassis.
- The Stryker ICV-D survivability, to include force protection, is comparable to the legacy Stryker flat-bottom ICV equipped with the same protection kits.
- The ICV-D has cybersecurity vulnerabilities that can be exploited. In most cases, the exploited vulnerabilities pre-date the integration of the lethality upgrades.

System

- The Stryker ICV-D is a flat-bottom ICV that the Army modified with an unmanned Medium Caliber Turret-30 mm (MCT-30) weapons system. The Army improved select Stryker mobility components to accommodate the increased weight of the turret and electrical power draw.
- The ICV-D turret is stabilized and electrically operated. A stabilized sensor suite contains a thermal camera, day camera, and laser rangefinder.
- The XM-813 30 mm main gun operates by an electric motor that powers the ammunition feed and weapons functions (chambering, firing, extraction, ejection). The 30 mm ammunition is gravity fed from two boxes on either side of the turret above the weapon.

- The weapon fires two types of service rounds (the MK 238 High Explosive Incendiary – Tracer (HEI-T) and the MK 258 Armor Piercing Fin-Stabilized Discarding Sabot-Tracer (APFSDS-T), plus two training round counterparts (the MK 239 Target Practice – Tracer (TP-T) round and the MK 317 Training Practice Discarding Sabot – Tracer (TPDS-T) round).
- The ICV-D features a coaxial machine gun and smoke grenades on the turret.
- The Army developed the ICV-D in response to an Operational Needs Statement submitted in March 2015 by the commander of the 2CR Stryker Brigade Combat Team. When fielding is complete, the ICV-D will comprise 50 percent of the vehicles in the rifle and scout platoons for a total of 81 vehicles in 2CR. The ICV-D is not a Program of Record.

Mission

Units equipped with the Stryker ICV-D will provide the Commander, European Command a medium-weight force capable of rapid strategic and operational mobility to disrupt or destroy enemy military forces, to control land areas including populations and resources, and to conduct combat operations to protect U.S. national interests.

Major Contractors

- General Dynamics Land Systems – Sterling Heights, Michigan; Anniston, Alabama
- Kongsberg Protech Systems – Kongsberg, Norway; Johnstown, Pennsylvania
- Northrop Grumman – Mesa, Arizona

Activity

- The Army conducted a two-phased EUT&E from February through April 2018 in accordance with DOT&E-approved test plans:
  - Phase I testing was conducted at Grafenwoehr (Germany) Training Area and consisted of crew gunnery qualification on an instrumented multi-lane range.
  - Phase II (force-on-force) was conducted at Hohenfels (Germany) Training Area from April 10 – 20, 2018. The test unit was an infantry company headquarters, an infantry rifle platoon, and a scout platoon. U.S. Army Training and Doctrine Command (TRADOC) accredited the opposing force (OPFOR) and represented current and near-future threats.
- The Army Test and Evaluation Command (ATEC) conducted a Cooperative Vulnerability and Penetration Assessment of the ICV-D in July 2017 and an Adversarial Assessment during Phase II of the EUT&E in April 2018.
- The Army completed the Stryker ICV-D LFT&E program from April 2017 through February 2018 in accordance with DOT&E-approved LFT&E Strategy and test plans. Live fire testing, executed at the Army Test Center, included armor coupon tests, ammunition sensitivity testing, controlled damage testing, sub-system and full-up system-level testing to support the evaluation of Stryker ICV-D survivability (including force protection and post-engagement vehicle repairability) against threats likely to be encountered in a European theater. Live fire testing also included ground testing to support the evaluation of Stryker ICV-D lethality against light to mid-armored adversary vehicles and dismounted targets.
- DOT&E published an Early Fielding Report in November 2018

Assessment

- The lethality upgrades of the ICV-D allow crews to detect, identify, and defeat targets at greater ranges and against a wider array of enemy targets than crews not equipped with the upgrades. Because of the increased lethality, unit leadership unanimously stated they would rather take the ICV-D to combat against a near-peer threat than the legacy ICV.
- The Stryker ICV-D survivability and force protection is largely comparable to the legacy Stryker flat-bottom ICV when equipped with the same protection kits. The Stryker ICV-D lethality is increased as compared to the legacy Stryker Family of Vehicles.
- During Phase I, six of nine crews qualified in accordance with Army gunnery standards. In addition, crew performance increased as they progressed through the gunnery tables demonstrating that the complexities introduced by the ICV-D advanced fire control unit can be mitigated as gunners gain experience and build "muscle memory" through practice and repetition. Crews noted a number of problems related to the design of the coaxial machine gun ammunition feed and ejection chutes that led to a number of stoppages during the gunnery tables.
- The lack of an appropriate Stryker training simulator poses a challenge to maintaining perishable gunner/crew proficiency gained through gunnery.
- During Phase II, when equipped with the ICV-D, infantry and scout platoons from the 2CR were able to accomplish their assigned task and purpose in 14 of 16 missions. During this phase, crews perceived their situational awareness degraded when operating mounted on the ICV-D.
- The platform met its reliability requirements for the turret and gun system without degrading the reliability of the base Stryker chassis.
- Adversaries demonstrated the ability to degrade select capabilities of the ICV-D when operating in a contested cyber environment. In most cases, the exploited vulnerabilities pre-date the integration of the lethality upgrades.

Recommendations

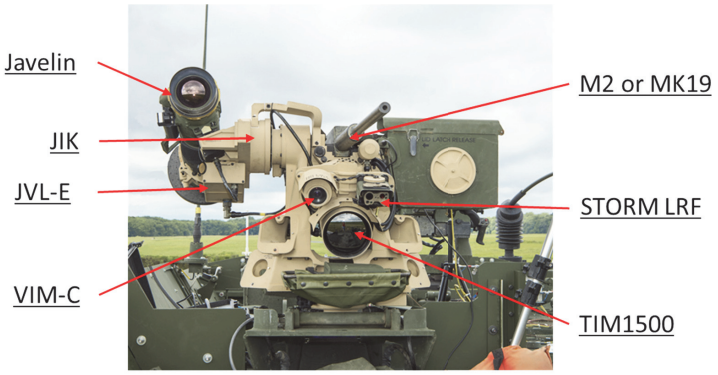
The Army should:

1. Restore lost situational awareness by providing true 360-degree situational awareness while on the move and stationary.
2. Improve design of coaxial machine gun assembly to reduce stoppages.
3. Provide higher fidelity simulation/simulator training resource for the ICV-D.
4. Correct or mitigate cyber vulnerabilities for the platform and government-furnished equipment.
5. Mitigate system design vulnerabilities to threats as identified in the classified report.

Stryker Common Remotely Operated Weapon Station – Javelin (CROWS-J)

Executive Summary

- The Army developed the Stryker Common Remotely Operated Weapons Station – Javelin (CROWS-J) in response to an Operational Needs Statement submitted in March 2015. It is not a Program of Record. When fielding is complete, the 81 Stryker CROWS-J will comprise 50 percent of the vehicles in the rifle and scout platoons in the 2nd Cavalry Regiment (2CR).
- The Army conducted an Early User Test and Evaluation (EUT&E) from February through April 2018. The EUT&E findings support the Army Program Executive Office decision to field the Stryker CROWS-J to the 2CR.
- When equipped with the Stryker CROWS-J, the majority of infantry and scout platoons from the 2CR were able to engage targets with the Javelin missile and accomplish their assigned tactical task and purpose.
- The Stryker CROWS-J improves unit lethality by enabling crews to detect, identify, and defeat targets at greater ranges and against a wider array of enemy targets than non-equipped crews.
- The platform meets reliability requirements for the weapon station without degrading the reliability of the base chassis.
- Leadership from the scout platoon experienced challenges manning the Long-Range Advanced Scout Surveillance System (LRAS3).
- The Stryker CROWS-J has cybersecurity vulnerabilities that can be exploited.



NO M6 SGL

CROWS FCU

RWS CG

FCU - Fire Control Unit
JIK - Javelin Integration Kit
JVL-E - Javelin Vehicle Launcher Electronics
RWS CG - Remote Weapon System Control Grip
SGL - Smoke Grenade Launcher
STORM LRF - Small Tactical Optical Rifle Mounted Laser Range Finder
TIM - Thermal Imaging Module
VIM-C - Visible Imaging Module Color

System

- CROWS-J is an M153 CROWS II system manufactured by Kongsberg that has been modified through the addition and fire control integration of the FGM-148 Javelin Anti-Tank Guided Missile (ATGM).
- In conjunction with the Javelin missile, the CROWS II mounts either a M2 .50 caliber machine gun, M240 7.62 mm machine gun, or an MK-19 40 mm automatic grenade launcher.
- The CROWS II is stabilized, electrically operated, and incorporates a Detached Line-of-Sight (DLOS), which allows the gunner to maintain a stable sight picture independent of weapon or ammunition selection. The CROWS-J replaces the legacy Remote Weapon Station (RWS) mounted on the Stryker Infantry Carrier Vehicle (ICV), and gives infantry and scout soldiers the ability to engage targets with the Javelin missile while under armor. It increases the range and expands the target array of enemy vehicles that can be defeated by the Stryker Brigade Combat Team, including armored vehicles.

Mission

Units equipped with the Stryker CROWS-J will provide the Commander, European Command with a medium-weight force capable of rapid strategic and operational mobility to disrupt or destroy enemy military forces, to control land areas including populations and resources, and to conduct combat operations to protect U.S. national interests.

Major Contractors

- Kongsberg Protech Systems – Kongsberg, Norway; Johnstown, Pennsylvania
- Raytheon & Lockheed Martin – Tucson, Arizona

Activity

- The Army conducted a two-phased EUT&E from February through April 2018, in accordance with DOT&E-approved test plans, and provided adequate data.
  - Phase I testing was conducted at Grafenwoehr (Germany) Training Area and consisted of crew gunnery qualification on an instrumented multi-lane range.
  - Phase II (force-on-force) was conducted at Hohenfels (Germany) Training Area (HTA) from April 10 – 20, 2018. The test unit was an infantry company headquarters, an infantry rifle platoon, and a scout platoon. U.S. Army Training and Doctrine Command (TRADOC) accredited the opposing force (OPFOR) and represented current and near-future threats.
- The Army Test and Evaluation Command (ATEC) conducted a Cooperative Vulnerability and Penetration Assessment of the CROWS-J in July 2017 and an Adversarial Assessment during Phase II of the EUT&E in April 2018.
- DOT&E intends to publish an Early Fielding Report in 2QFY19.

Assessment

- The Stryker CROWS-J improves combat lethality and force protection by enabling crews to destroy enemy heavy armor vehicles while under armor. Platoon-level formations present new tactical dilemmas to opposing forces that increase tactical risk to enemy vehicles and soldiers as a result of these improved capabilities.
- During Phase I, all five crews qualified in accordance with Army gunnery standards. In addition, the crews fired six live Javelin missiles, hitting their targets five times.
- During gunnery, a crew member bent the mounting fork while attempting to align the missile onto it, which prevented the missile from successfully connecting to the Javelin Integration Kit.
- During Phase II, infantry and scout platoons equipped with the Stryker CROWS-J were able to accomplish their assigned task and purpose in 14 of 16 missions. During this phase, scout platoon leadership stated that relocating the LRAS3 to the back of the scout vehicles created a manning dilemma for the crew. The scout platoon mitigated the problem by adjusting their internal manning.
- The platform met its reliability requirements for the turret and gun system without degrading the reliability of the base Stryker chassis.
- Crews experienced a significant number of software-related essential function failures when using training ammunition that caused them to have to reboot the CROWS system during Phase II missions.
- The design of the mounting fork for the Javelin Integration Kit is not structurally sound.
- Adversaries demonstrated the ability to degrade select capabilities of the Stryker CROWS-J.

Recommendations

The Army should consider the following recommendations:

1. Correct design deficiency in the mounting fork on the Javelin Integration Kit.
2. Correct or mitigate cyber vulnerabilities of both the platforms and government-furnished equipment.
3. Correct the Essential Function Failure rate observed when using training ammunition.

UH-60V BLACK HAWK

Executive Summary
- The UH-60V BLACK HAWK cockpit increases pilot awareness of aircraft status similar to the UH-60M cockpit and adds enhanced navigational functionality compared to the UH-60L.
- Additional work is ongoing to complete software development, improve reliability, develop a performance planning module for UH-60V engines, and improve the cybersecurity posture before IOT&E in 2019.

System
- The UH-60V BLACK HAWK is designed to modernize the existing UH-60L analog architecture to a digital infrastructure enabling a pilot-vehicle interface (PVI) similar to the UH-60M. Cockpit similarity with the UH-60M enables a single Army BLACK HAWK pilot training program. Once qualified on the UH-60M, pilots can transition to the UH-60V with minimal additional instruction.
- The program goal is to achieve UH-60M commonality at lower cost than production of a new UH-60M, reduce avionics obsolescence, and upgrade navigation functionality that meets Global Air Traffic Management (GATM) requirements. By meeting GATM standards, the UH-60V can file instrument flight plans and deploy anywhere GATM standards are enforced. GATM is in use in Europe.
- The basic mission configuration includes a crew of four (pilot, copilot, crew chief, and gunner), integral (internal) mission fuel, avionics, aircraft survivability equipment, armor protection, two M240 machine guns and ammunition, and other mission-related equipment.

Mission
The unit equipped with the UH-60V BLACK HAWK will employ the aircraft to conduct movement and maneuver, sustainment, and mission command flight operations.

Major Contractors
- The Corpus Christi Army Depot at Corpus Christi, Texas, will induct and refurbish existing UH-60L aircraft before applying the engineering changes that convert the UH-60L into the UH-60V configuration.
- Redstone Defense Systems at Huntsville, Alabama, conducts design and integration of the UH-60V. They are the prime contractor under the Prototype Integration Facility, at the U.S. Army Aviation and Missile Research Development and Engineering Center.
- Northrop Grumman in Woodland Hills, California, is leading the development and integration of flight control software.

Activity
- The Army conducted airworthiness and flight characteristics testing at Redstone Arsenal, Alabama, throughout 2018. As of September 2018, developmental testing included 256 productive flight hours and 240 ground test hours in day, night, and visual meteorological conditions on engineering release software versions up to and including 4.11. The program has continued software testing in a Systems Integration Laboratory (SIL) and flight testing of software version 4.12.
- The Army conducted a 45-hour Limited User Test (LUT) in July 2018 with operational pilots and aircrews from the 82nd Airborne Division, experimental test pilots, and two Engineering Design Model UH-60V aircraft. Aircrews completed six air assault, air movement, and external load missions, during day, night, and night vision goggle flight modes, in hot and humid conditions, in the vicinity of Redstone Arsenal. Aircrews flew the aircraft in contour and nap-of-the-earth mission profiles over Redstone Arsenal and local terrain. The Army simulated threat missile launches during some of the missions.
- The Army conducted a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) in February 2018 using one UH-60V aircraft in a hangar and the

UH-60V SIL to identify potential cyber-attack vectors. In July 2018, the Army conducted an Adversarial Assessment (AA), using an aircraft with aircrew in a hangar and the UH-60V SIL to identify and exploit cybersecurity vulnerabilities.
- The Army Survivability and Lethality Analysis Directorate completed a vulnerability analysis in September 2018 against expected, kinetic threats.
- The Army conducted all testing in accordance with a DOT&E-approved Test and Evaluation Master Plan and test plan.

Assessment
- The Army identified 12 deficiencies and 43 shortcomings at the completion of software version 4.9 testing in May 2018. Many of these shortcomings were observed during the LUT and have since been corrected and verified in flight testing.
- Aircrews successfully completed all six attempted single- and dual-ship missions during the LUT. Pilots made positive comments about increased awareness of aircraft status and enhanced navigation capabilities of the UH-60V compared to the UH-60L.
- The UH-60V is equipped with the General Electric 701D engine, which is capable of meeting UH-60V performance requirements. The UH-60V is limited at Milestone C to 701C engine power. The UH-60V does not have an Air Worthiness Release (AWR) allowing the full power of the 701D engines to be realized. Once the program attains the AWR, the UH-60V will meet the performance requirements for external lift and air assault range. In addition, the UH-60V will be equivalent to the UH-60L in the performance requirements for endurance and self-deployment. The software development of the performance planning software, which enables the attainment of the AWR for the UH-60V with 701D engines, has begun and the Program Office expects to demonstrate 701D power in IOT&E in 2019.
- The UH-60V aircraft was below planned reliability growth goals during the LUT. The LUT aircraft were configured with version 4.9 software that had a number of known reliability failure modes that have been corrected and verified as fixed in software version 4.11.
- The CVPA identified a number of potential insider and near-sider cyber-attack vectors. The AA confirmed that some of those vectors could be exploited and, to a limited extent, explored the likely mission effects of successful exploitation
- The vulnerability analysis found that there is no appreciable difference between the UH-60V and the legacy UH-60L in force protection, aircraft attrition, and forced landing kills when engaged by armor-piercing incendiary threats, high explosive incendiary threats, and rocket-propelled grenades.

Recommendations

The Army should:
1. Continue to develop UH-60V software to address the frequent reliability failure modes.
2. Develop performance planning software for the UH-60V with 701D engines.
3. Eliminate or reduce the cybersecurity vulnerabilities.
4. Conduct all post-Milestone C developmental flight testing with mission equipment (radios, aircraft survivability equipment, and crypto gear) installed and operational.

Warfighter Information Network – Tactical (WIN-T)

Executive Summary

- Warfighter Information Network – Tactical (WIN-T) Increment 2 upgraded the design of legacy Point of Presence (PoP) and Soldier Network Extension (SNE) assemblages. The program intends for the new Next Generation (Next Gen) design to better meet the size, weight, and power requirements of Army tactical vehicles.
- In April 2018, the Army Test and Evaluation Command (ATEC) presented a risk assessment briefing to DOT&E to recommend the proper size and scope of a Next Gen PoP and SNE test to support a planned April 2019 Amended Materiel Release decision. DOT&E approved the ATEC strategy of a developmental test combined with first unit equipped observations.
- The Army conducted the May 2018 Next Gen PoP and SNE developmental test, a cybersecurity assessment, safety certifications, a logistics demonstration, and collected first unit equipped data to produce an ATEC assessment to support the planned materiel release decision.
- ATEC assessed the Next Gen PoP and SNE as meeting or exceeding demonstrated legacy performance, reliability, and cybersecurity requirements. Along with size, weight, and power savings, the new capability recovered two crew seats in Next Gen equipped Stryker combat vehicles, and introduced a new capability to connect the WIN-T Satellite Tactical Terminal (STT).
- At the September 2018 WIN-T Increment 2 Configuration Steering Board (CSB), the Army acknowledged the 2018 WIN-T Increment 2 Selected Acquisition Report (SAR) will be the program's final SAR since they have expended over 95 percent of their funding. To continue network modernization, the Army intends to use Tactical Network Transport Modification in Service (TNT MIS) funding for fielding future tactical network capabilities. The Army and DOT&E are working to produce a T&E strategy for the numerous capabilities within the TNT MIS.

Next Generation (NG)
Point of Presence (PoP)

Next Generation (NG)
Soldier Network Extension (SNE)

1 - Network Centric Waveform (NCW) Antenna
2 - Highband Networking Waveform (HNW) Antenna

System

- The Army intends WIN-T to provide reliable, secure, and seamless communications for units operating at theater level and below.
- The WIN-T program consists of three funded increments. In May 2014, the Defense Acquisition Executive approved the Army's request to stop development of the Increment 3 aerial tier of networked, airborne communications relays and limit Increment 3 to network management and satellite waveform improvements.
  - Increment 1: "Networking At-the-Halt" enables the exchange of voice, video, data, and imagery throughout the tactical battlefield using a Ku-band and Ka-band satellite based network. The Army has fielded WIN-T Increment 1 to its operational forces.
  - Increment 2: "Initial Networking On-the-Move" provides command and control on-the-move down to the company level for maneuver brigades and implements an improved network security architecture.
    - WIN-T Increment 2 supports on-the-move communications for commanders with the addition of the PoP and the SNE, and provides a mobile network infrastructure with the Tactical Communications Node. It employs a terrestrial Highband Networking Waveform and a satellite Network Centric Waveform to support its network mobility goals.
    - WIN-T Increment 2 provides a downsized, air transportable variant of High Mobility Multipurpose Wheeled Vehicle (HMMWV)-mounted configuration items to support light brigades.
    - WIN-T Increment 2 upgraded the design of the legacy PoP and SNE assemblages. The program intends for the new Next Gen design to better meet the size, weight, and power requirements of Army tactical vehicles. The Next Gen PoP and SNE are the final enhancements provided by WIN-T Increment 2. TNT MIS will provide funding for future enhancements and tactical network modernization initiatives.
  - Increment 3: "Full Networking On-the-Move" was to provide full mobility mission command for all Army field commanders, from theater to company level using networked airborne communication relays. With program reductions, WIN-T Increment 3 now provides enhanced network operations and an improved satellite waveform to WIN-T Increments 1 and 2.

Mission

Commanders at theater level and below will use WIN-T to:

- Integrate satellite-based communications capabilities into an everything-over-Internet Protocol network to provide

connectivity, while stationary, across an extended, non-linear battlefield, and at remote locations (Increment 1).
- Provide division and below maneuver commanders with mobile communications capabilities to support initial command and control on-the-move (Increment 2).

Major Contractor
General Dynamics, Mission Systems – Taunton, Massachusetts

Activity
- WIN-T Increment 2 upgraded the design of legacy PoP and SNE assemblages via an engineering change proposal. The program intends for the Next Gen PoP and SNE to better meet the size, weight, and power requirements of Mine Resistant Ambush Protected All Terrain Vehicles (M-ATVs), HMMWVs, and Stryker combat vehicles. The program conducted non-recurring engineering to integrate Next Gen onto Joint Light Tactical Vehicles, but the Army has not developed a requirement or fielding plan for these system configurations.
- In February 2018, Johns Hopkins University Applied Physics Laboratory conducted a series of cybersecurity scans and penetration tests on the Next Gen configuration items within a representative WIN-T network.
- In April 2018, ATEC presented a risk assessment briefing to DOT&E to recommend the proper size and scope of a Next Gen PoP and SNE test to support a planned April 2019 Amended Materiel Release decision. DOT&E approved the ATEC strategy of a developmental test combined with first unit equipped observations.
- In May 2018, the Army conducted the WIN-T Increment 2 Developmental Test of the Next Gen PoP and SNE at White Sands Missile Range, New Mexico, using M-ATVs and soldiers from the 10th Mountain Division.
- The Army completed safety certification testing of the Next Gen PoP and SNE on M-ATVs, HMMWVs, and Stryker combat vehicles in August and September 2018.
- The Army completed a Logistics Demonstration of the HMMWV Next Gen PoP and SNE configurations in August and September 2018.
- During September to October 2018, ATEC collected Next Gen PoP and SNE observations at the 3rd Brigade, 25th Infantry Division first unit equipped fielding.
- ATEC completed its initial report on the Next Gen PoP and SNE, and will complete its analysis of instrumented and first unit equipped data to finalize an Operational Assessment Report (OAR) in December 2018. This report will support a Communications Electronics Command Amended Materiel Release decision planned for April 2019.
- At the September 2018 WIN-T Increment 2 CSB, the Army acknowledged the 2018 WIN-T Increment 2 SAR will be the program's final SAR since they have expended over 95 percent of their funding. To continue network modernization, the Army intends to use TNT MIS funding for fielding future tactical network capabilities. The Army and DOT&E are working to produce a T&E strategy for the numerous capabilities within the TNT MIS.

Assessment
•ATEC's initial report on the Next Gen PoP and SNE assessed the new systems as meeting or exceeding demonstrated legacy capabilities using both terrestrial and satellite transmission means. The Next Gen PoP and SNE:
- Met or exceeded performance, reliability, and maintainability requirements.
- Did not introduce new cybersecurity vulnerabilities to the WIN-T network.
- Received safety certification for the M-ATV, and expect to complete safety certifications for the HMMWV and Stryker combat vehicles in January 2019.
- Recovered two crew seats within Next Gen-equipped Stryker combat vehicles.
- Introduced a new fiber optic cable connection to allow use of the WIN-T STT.
- Soldiers recommended improvements on the fiber optic cable connection and signal entry panel.

Recommendations
The Army should:
1. Develop a T&E strategy for the numerous capabilities within the TNT MIS.
2. Implement the recommendations of the ATEC Next Gen PoP and SNE OAR.

XM17/XM18 Modular Handgun System (MHS)

Executive Summary

- The vendor conducted contractor testing of the XM17 and the XM18 Modular Handgun Systems (MHS) to implement reliability improvements from October 2017 through March 2018.
- The upgraded configuration of the MHS demonstrated improved reliability firing for both XM1152 ball ammunition and XM1153 jacketed hollow point ammunition during the Army's second Production Verification Test (PVT2).
- The MHS meets or exceeds requirements for accuracy, lethality, ergonomics, and safety.

System

- The MHS program is comprised of the XM17 full-size variant and XM18 compact variant 9 mm pistols. The majority of Army MHS users will use the XM17 variant. Individuals and units requiring a concealed weapon, will use the XM18 variant.
- Both variants include modular features to allow for the future addition of different targeting enablers (e.g., infrared and visible laser pointers), pistol grips, and alternate magazine options.
  - Targeting enablers can be mounted on the weapon using standard Picatinny rails.
  - Small, medium, and large polymer grip modules accommodate different hand sizes.
- The XM17 and XM18 pistols are mechanically locked, short-recoil operated weapons. Common features include: a reversible magazine catch to accommodate left- or right-handed shooters, ambidextrous manual safety, and external slide catch lever. Loading is automatic with each shot fired, until the magazine is empty. The slide is locked to the rear after the last shot is fired.
- The MHS incorporates a non-reflective, neutral color for detection avoidance. The Army intends for the MHS to be operable with a future sound suppressor.
- The Army requires the weapon to use ball ammunition and jacketed hollow point ammunition. The XM1152 ball cartridge uses an 115 grain truncated nose full metal jacket projectile, and the XM1153 jacketed hollow point cartridge uses a 147 grain jacketed hollow point projectile.
- The contractor provides two 21-round magazines and one 17-round magazine with each pistol as part of the system.
- The MHS is an Army program with joint interest. The Army, including Army Special Operations Command, intends to purchase approximately 233,429 pistols, of which approximately 4.5 percent will be XM18s. The Navy, Marine Corps, and Air Force may collectively purchase 224,000 pistols under the same contract.

1 - XM17, Full Size, with 21-round magazine
2 - XM18, Compact, with 17-round magazine
3 - XM1152 Ball round
4 - XM1153 Jacketed Hollow Point (JHP) round
5 - XM1156 Dummy round
6 - XM1157 Blank round

Mission

- Military personnel conducting core mission combat operations use the MHS for personal self-defense and as their secondary weapon system. Core missions include anti-terrorism, direct action, force protection, anti-hijacking, evasion, special investigations, special operations, reconnaissance, protective service, law enforcement, resource protection, base security, terminal air control, and combat search and rescue. Civil affairs and peacekeeping operations are also core missions in some Services.
- Military personnel conducting collateral activities use the MHS as their primary weapon system. Collateral activities include foreign and U.S. humanitarian assistance,

counter-terrorism, and counter-narcotics, all of which may involve military operations in urban terrain/operations, close quarters battle, and other operations on the battlefield.

Major Contractors
- Pistol: SIG SAUER Inc. – Newington, New Hampshire
- Ammunition: Olin-Winchester – East Alton, Illinois

Activity
- The MHS experienced a large number of stoppages in early developmental testing with ball ammunition. To address these problems, a tiger team was created consisting of government and contractor personnel to determine root cause.
- The Army completed IOT&E for the XM17 and the XM18 with jacketed hollow point ammunition in September 2017. The final IOT&E and LFT&E report were held until the completion of all developmental test events.
- To improve the reliability with ball ammunition without degrading any of the other attributes of the weapon, the vendor made adjustments to the magazine spring, magazine follower, slide geometry, and the internal components.
- The vendor conducted contractor testing on the XM17 and the XM18 with both ball and jacketed hollow point ammunition from October 2017 through March 2018 to address the deficiencies identified during early testing.
- The Army conducted PVT-2, in coordination with DOT&E and with the same procedures as the DOT&E-approved PVT-1 testing, to validate the fixes implemented during contractor testing. The Army released the preliminary results in September 2018.
- During PVT-2, the Army shot 16,500 rounds on five weapons for a total of 82,500 rounds per weapon/ammunition combination from the test stand. DOT&E published the IOT&E and LFT&E Report for the XM17 and XM18 in December 2018 upon completion of the Army's assessment of PVT-2.
- The Army intends to have a Full-Rate Production decision in November 2018.

Assessment
- DOT&E assessed that the XM17 and the XM18 are operationally effective and operationally suitable with jacketed hollow point ammunition. Both are lethal with the ball and jacketed hollow point ammunition. Details are found in the DOT&E IOT&E and LFT&E report.
- Analysis from PVT-2 and findings from IOT&E testing confirms that the upgraded MHS configuration met or exceeded their requirements for lethality, accuracy, ergonomics, and safety.
- Data from the Army Evaluation Center (AEC) analysis of PVT-2 reliability testing indicate that the changes made to the weapon and magazine have led to improvements to the MHS reliability with ball ammunition when compared to the PVT-1 conducted in 2017, as measured by Mean Rounds Between Failures (MRBF) and Mean Rounds Between Stoppages (MRBS).
- Both the XM17 and XM18 exceed the MRBF requirement of 5,000 MRBF (96 percent probability of completing two 99-round missions without a single failure).
- The XM18 with both ball and jacketed hollow point ammunition exceeds the MRBS requirement of 2,000 MRBS (95 percent probability of completing one 99-round mission without a single stoppage). The XM17 with ball and jacketed hollow point ammunition demonstrated 93 percent and 94 percent probability, respectively, of completing one 99-round mission without a single stoppage.

		XM17 with Ball	XM17 with JHP	XM18 with Ball	XM18 with JHP
PVT-1 (AEC Results)	MRBS	*431	2,709	*358	*1,779
	MRBF	7,009	15,501	4,352	8,895
PVT-2 (AEC Final Results)	MRBS	1,566	1,880	3,185	7,833
	MRBF	6,349	10,321	7,009	15,501

PVT – Production Verification Test; AEC – Army Evaluation Center; JHP – Jacketed Hollow Point Ammunition; MRBS – Mean Rounds Between Stoppages; MRBF – Mean Rounds Between Failures

* Due to high variance between results of the five weapons tested, and the inability to statistically combine all five weapons in the grouping, these are median values. All other figures in this table are 80 percent lower confidence bound of the combined data for the five weapons in those groupings.

Recommendation
1. The Army should confirm reliability fixes to both the XM17 and XM18 during initial fielding to confirm that fixes do not adversely affect operational effectiveness and suitability.

Navy Programs

Navy Programs

Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI) for AN/BQQ-10(V) Sonar

Executive Summary

- DOT&E submitted an FOT&E report on the Advanced Processing Build 2013 (APB-13) variant of the AN/BQQ-10 Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI) sonar system on June 29, 2018. APB-13 is operationally effective for the anti-submarine warfare (ASW) mission against moderately quiet nuclear and diesel submarines. APB-13 is operationally suitable.
- The Navy commenced FOT&E of the APB-15 variant of the A-RCI sonar system in September 2018. The Navy expects to complete testing in FY19. DOT&E will submit an FOT&E report on the APB-15 variant in FY19.

System

- The AN/BQQ-10 A-RCI sonar system is the undersea sensing system utilized by U.S. submarines. It uses active and passive sonar to conduct ASW and submerged operations in the execution of all assigned submarine missions. Acoustic energy is processed and displayed to enable operators to detect, classify, localize, and track threat submarines and other waterborne objects (surface ships, mines, bottom features, etc.).
- The AN/BQQ-10 A-RCI sonar system is an open-architecture system that includes staggered biennial software upgrades (APBs) and biennial hardware upgrades (Technical Insertions). These upgrades are intended to maintain an advantage in acoustic detection of threat submarines.
- The AN/BQQ-10 A-RCI sonar system consists of:
  - Interfaces to submarine acoustic sensors to include the spherical array or large aperture bow array, hull array, wide aperture array, conformal array, high-frequency array, and two towed arrays (i.e., the fat-line array consisting of the TB-16 or TB-34, and the thin-line array consisting of the TB-23, TB-29A, or TB-29A Reduced Length)

  - Processing capability that utilizes environmental data (e.g., water depth, bottom contour, sound velocity profiles, etc.) and received acoustic energy on all acoustic sensors and displays the processed data in a way that supports operator search, detection, classification, and localization/track of contacts of concern or contacts of interest.

Mission

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

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

Major Contractor

Lockheed Martin Maritime Systems and Sensors – Manassas, Virginia

Activity

- In June 2018, DOT&E submitted a classified FOT&E report on the APB-13 variant of the A-RCI sonar system.
- In April 2018, DOT&E approved a Test and Evaluation Master Plan covering the APB-15 variant of the A-RCI sonar system. The Navy has since completed the following operational testing of the APB-15 variant in accordance with DOT&E-approved test plans.
  - In June 2018, the Navy commenced in-lab comparison testing between variants APB-13 and APB-15 using real-world sonar recordings of non-U.S. submarines. Sonar recordings are played on each variant using 20 fleet operators to assess operator detection and classification metrics. The Navy expects to complete this testing in 1QFY19. This testing is conducted as combined developmental and operational testing.
  - In September 2018, the Navy completed 2 days of at-sea evaluation of APB-15 capability to support situational awareness in an environment with a large number of contacts.
- The Navy scheduled an APB-15 test event against a high-end, diesel electric submarine during the Rim of the Pacific Exercise. However, the event was canceled when the target

submarine became unavailable to support the test. The Navy continues to pursue fleet exercises as opportunities to obtain high-end, diesel electric submarine target services to test future APB capability.
- The Navy intends to complete remaining FOT&E test events for APB-15 in FY19, including 4 days of open ocean ASW search and cybersecurity evaluation.

Assessment
- The DOT&E FOT&E report dated June 29, 2018, concluded the following regarding performance:
  - APB-13 software is operationally effective for the ASW mission against moderately quiet nuclear and diesel submarines. Further, APB-13 demonstrated better performance than the previous APB-11 software and included modifications that reduce operator workload.
  - The Navy was not able to reschedule an evaluation of APB-13 capability to support situational awareness in a high-density contact management environment.
  - APB-13 is operationally suitable. No significant issues related to reliability or operational availability were identified.
  - Cybersecurity results that affect the systems operational effectiveness are included in the classified FOT&E report.
- Analysis of APB-15 test data is in progress and no preliminary assessment can be made. DOT&E intends to deliver an FOT&E report in FY19.

Recommendations

The Navy should:
1. Continue to pursue a high-end diesel submarine as a priority target for at-sea testing of future APBs.
2. Continue the use of in-lab comparison testing as a supplement to at-sea testing when assessing APB performance.
3. Address the recommendations in the DOT&E FOT&E report for the APB-13 variant of the A-RCI sonar system.

Aegis Modernization Program

Executive Summary

- The Navy is modernizing the Aegis Weapon System (AWS) on Aegis guided missile cruisers and destroyers via Advanced Capability Build (ACB)-12, ACB-16, and ACB-20 baseline upgrades.
- DOT&E will issue a final report on ACB-12 Baselines 9.A0 and 9.C1 in FY19. To date, the live firing area air defense flight test events on Baselines 9.A0 and 9.C1 indicate that performance against single subsonic and supersonic high diving targets remains consistent with historical results against comparable threats; testing against more stressing target presentations is planned for FY18-22 ACB-16 operational testing.
- In FY18, the Navy began air defense, surface warfare, and cyber survivability operational testing of ACB-16 Phase 0 (Baseline 9.A2A cruiser). The Navy will conduct Phase 1 and Phase 2 (Baseline 9.C2 cruiser and destroyer) integrated and operational test events in FY20-22.
- Previous results of Aegis Baseline 9.A (cruisers) cyber survivability testing can be found in the July 2015 DOT&E Early Fielding Report. Subsequent to that report and the cyber survivability testing of Aegis Ashore installation (Baseline 9.B), the Navy canceled cyber survivability testing of Baseline 9.C1. The September 2018 initial phase of cyber survivability testing on ACB-16 Baseline 9.A2A was postponed due to Hurricane Florence evacuation. This may result in Baseline 9.A2A deployment in FY19 with no cyber survivability testing.
- The Navy must provide an accredited modeling and simulation (M&S) suite of the Aegis Combat System (ACS) in order to adequately assess the Probability of Raid Annihilation requirement for the self-defense mission for Flight III DDG 51 destroyers/ACB-20.
- Navy Integrated Fire Control – Counter Air (NIFC-CA) From-the-Sea (FTS) Increment I became a fielded capability in 2015 and was fully integrated as a tactical option in fleet air defense. Future testing of ACB-16, ACB-20, and Standard Missile (SM)-6 will continue to evaluate the NIFC-CA FTS capability.

System

- The Navy Aegis Modernization program provides updated technology and systems for CG 47-class Aegis guided missile cruisers and DDG 51-class Aegis guided missile destroyers. This planned, phased program provides similar technology and systems for new construction destroyers.
- The AWS integrates the following components:
  - AWS AN/SPY-1 three-dimensional (range, altitude, and azimuth) multi-function radar
  - AN/SQQ-89 undersea warfare suite that includes the AN/SQS-53 sonar, SQR-19 passive towed sonar array

(DDGs 51 through 78, CGs 52 through 73), and the SH-60B or MH-60R helicopter (Flight IIA DDGs 79 and newer have a hangar to allow the ship to carry and maintain its own helicopter)
  - Close-In Weapon System
  - A 5-inch diameter gun
  - Harpoon anti-ship cruise missiles (DDGs 51 through 78, CGs 52 through 73)
  - Vertical Launch System that can launch Tomahawk land attack missiles, SM-2 and -6 surface to-air missile variants, Evolved Sea Sparrow Missiles, and Vertical Launch Anti-Submarine Rocket missiles
  - The AWS is upgraded through quadrennial ACBs. The Navy is currently upgrading the AWS to Baseline 9.A2A on CG 47 cruisers and to Baseline 9.2 on Flight IIA and new construction DDG 51 destroyers. Baseline 10 is planned for fielding on Flight III DDG 51 destroyers.
    - ACB-12 Baseline 9.A0 upgraded Baseline 3 *Ticonderoga* (CG 47)-class cruisers.
    - ACB-12 Baseline 9.C1 upgraded Flight I *Arleigh Burke* (DDG 51)-class destroyers.
    - ACB-12 Baseline 9.C1 also equipped new construction Flight IIA DDG 51 destroyers.
    - ACB-16 Baseline 9.C2 and 9.A2A upgrades will be installed on modernized Flight IIA DDG 51 destroyers and Service Life Extension Program for SPY-1B equipped cruisers and Baseline 8 SPY-1A CG 47 cruisers respectively.
    - ACB-20 Baseline 10 upgrades for Flight III DDG 51 destroyers.

Mission

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

- Area and self-defense anti-air warfare in defense of the Strike Group
- Anti-surface warfare and anti-submarine warfare
- Strike warfare, when armed with Tomahawk missiles
- Integrated Air and Missile Defense (IAMD), to include simultaneous offensive and defensive warfare operations
- Operations independently or in concert with Carrier or Expeditionary Strike Groups and with other joint or coalition partners

Major Contractors

- General Dynamics Marine Systems Bath Iron Works – Bath, Maine
- Huntington Ingalls Industries (formerly Northrop Grumman Shipbuilding) – Pascagoula, Mississippi
- Lockheed Martin Rotary Mission Systems – Moorestown, New Jersey

---

Activity

- In June 2018, the Navy conducted Phase 0 operational testing for Aegis ACB-16 (Baseline 9.A2A) on USS *Leyte Gulf* (CG 55). Phase 0 testing covered the software version installed on Aegis cruisers with the SPY-1A radar. Operational testing consisted of air defense tracking events conducted at Service Combat Systems Center, Wallops Island, Virginia. Additionally, three developmental live fire events conducted in the Virginia Capes Operating Area provided supplemental data. The Navy conducted the operational tests in accordance with DOT&E-approved test plans.
- In July/August 2018, at the Pacific Missile Test Center, Point Mugu, California, the Navy continued Phase 0 air defense and surface warfare operational testing on USS *Mobile Bay* (CG 53). Air defense testing consisted of raids of subsonic anti-ship cruise missile (ASCM) surrogate targets. Surface warfare test events included one firing exercise and several tracking exercises against small boats. Problems with aerial targets deviating from the planned flight profile in one event and ship schedule/range operational concerns precluded execution of the tests in accordance with the approved test plan.
- ACB-16 Phase 1 and 2 (Baseline 9.C2 cruisers and destroyers) follow-on integrated and operational testing is planned for FY20-22.
- Cyber survivability testing of Aegis Baseline 9.C1 has been deferred until ACB-16 Baseline 9.C2 operational testing. The first phase of planned cyber survivability testing for ACB-16 for cruisers, scheduled for September 2018, was postponed due to Hurricane Florence evacuation. Cyber survivability testing is planned for Phase 1 on cruisers in FY20 and Phase 2 on destroyers in FY21/22.
- The Navy is developing an M&S suite to supplement live testing and facilitate a more thorough evaluation of air defense performance for DDG 51 Flight III ships in FY23. As part of the overall M&S development strategy, the Navy plans to make limited use of the M&S suite for operational testing of the ACB-16 (Baseline 9.C2) in FY22.
- The Navy is developing Test and Evaluation Master Plans for Aegis ACB-16 (Baselines 9.A2 and 9.C2) and for DDG 51 Flight III/ACB-20 (Baseline 10).
- NIFC-CA FTS is being evaluated in conjunction with planned Aegis Modernization operational testing. Increment I became a fielded capability in 2015 and was fully integrated as a tactical option in fleet air defense. Future testing of ACB-16, ACB-20, and SM-6 will evaluate the NIFC-CA FTS Increment II capability.
- DOT&E intends to issue a final report on Baselines 9.A0 and 9.C1 in FY19.

Assessment

- Analysis of completed Phase 0 ACB-16 test events is ongoing. Testing to date is not sufficient to demonstrate the effectiveness of SPY-1A-equipped cruisers in air defense or to evaluate the cyber survivability posture of Aegis cruisers prior to the deployment in FY19. During the live fire test on USS *Mobile Bay*, the execution of one planned air defense firing event against a raid of ASCM surrogates resulted in a significantly different raid profile than planned. While all targets were successfully intercepted, the overall test objectives were not met. Similarly, a planned multi-mission firing event (planned to include small boats, a subsonic ASCM raid, and an unmanned aerial vehicle (UAV) attack) was reduced to an air defense firing against an UAV due to test range execution problems and ship schedule.
- Previous operational testing of Aegis Baselines 9.A0 and 9.C1 indicate that air defense performance against single subsonic and supersonic high-diving ASCM presentations is consistent with historical performance. Aegis Baseline 9 has incorporated software changes to address performance against certain stressing air defense threat presentations. Evaluation of these actions is ongoing throughout ACB-16 operational testing.
- The outcome of the single surface warfare operational testing firing event in FY18 indicates ACB-16 performance was

consistent with improvements noted in previous testing. This event alone is not sufficient to assess ACB-16 ship surface warfare performance.
- Due to range safety considerations self-defense mission test data collected in manned ship testing is limited and not sufficient to fully assess this mission area.
- Similarly, the Navy cannot fully assess Aegis IAMD until an AWS M&S test bed is developed and validated. The test bed is under development and is planned to be available by FY20. A limited Baseline 9.C1 IAMD operational assessment suggests that DDGs can simultaneously support limited air defense and ballistic missile defense missions within overall radar resource constraints. This assessment is supported by a single successful live firing event, managed by the Missile Defense Agency, which included simultaneous live firing of SM-2 and SM-3 missiles against threat-representative targets in an IAMD engagement. More stressing IAMD scenarios are planned for ACB-16 and ACB-20 testing
- Results of previous Aegis Baseline 9.A (cruisers) cyber survivability testing can be found in the July 2015 DOT&E Early Fielding Report. Subsequent to this report, and the cyber survivability testing of Aegis Ashore installation (Baseline 9.B), the Navy canceled cyber survivability testing of Baseline 9.C1 and will evaluate implementation of fixes to previous problems as part of ACB-16 operational testing.

Recommendation

1. The Navy needs an accredited M&S suite of the ACS to adequately assess the Probability of Raid Annihilation requirement for the self-defense mission for Flight III DDG 51 destroyers/ACB-20.

Amphibious Combat Vehicle (ACV)

Executive Summary

- The Marine Corps awarded contracts to BAE Systems and SAIC in November 2015, utilizing two vendors to facilitate a competitive Engineering and Manufacturing Development (EMD) phase. Each vendor delivered 16 prototypes for testing during the EMD phase. The Amphibious Combat Vehicle 1.1 (ACV 1.1) program conducted LFT&E from May 2017 to January 2018 and an operational assessment (OA) from January to March 2018 with both vendors participating.
- In June 2018, the Marine Corps selected BAE Systems as the vendor to build ACV.
- During the OA, the ACV-equipped unit demonstrated the ability to maneuver to an objective, conduct immediate action drills, and provide suppressive fires in support of dismounted infantry maneuver in a desert environment. The ACV-equipped unit was able to maneuver in the littorals; embark aboard a landing craft air cushioned (LCAC), transit the open ocean and surf zone, and debark from the LCAC. The ACV demonstrated water mobility and the ability to self-deploy from the beach, cross the surf zone, enter the ocean, swim, and return to the beach.
- Based on data from the OA, reliability is below the program reliability growth curve (58 hours Mean Time Between Operational Mission Failures (MTBOMF)). BAE vehicles demonstrated 24.9 hours MTBOMF. There were no systemic problems identified that indicate a major redesign is required.
- The EMD LFT&E program demonstrated that the EMD ACV design met Key Performance Parameter force protection requirements.

System

- The Marine Corps intends to field a vehicle capable of providing expeditionary protected mobility and general support lift to the Marine Infantry Battalion as part of a Ground Combat Element-based maneuver task force.
- The ACV 1.1 will serve to mitigate a shortfall in protected mobility by providing effective land and tactical water mobility (shore-to-shore), precise supporting fires, and high levels of force protection. This protection is intended to provide survivability against blasts, fragmentation, and kinetic energy threats while supporting combat-loaded marines as they close with and destroy the enemy, respond to crises, and/or conduct security and stability operations. The ACV 1.1 is a partial replacement for the legacy Amphibious Assault Vehicles (AAVs) fielded to the Assault Amphibian battalion within the Marine Division.

Mission

- Commanders intend to employ ACV-equipped units to land and maneuver the surface assault elements of the landing force in order to seize inland objectives and conduct mechanized operations in subsequent actions ashore.
- ACV-equipped units will provide protected mobility to embarked infantry and will deliver precision support-by-fire effects in support of dismounted infantry maneuver. ACV-equipped units will operate effectively with M1 series main battle tanks and conduct mounted security operations in urban or restrictive terrain alongside other wheeled vehicles within the Marine Division.

Major Contractor

BAE Systems – York, Pennsylvania

Activity

- The U.S. Army Aberdeen Test Center conducted live fire testing for EMD prototype ACVs from May 2017 to January 2018 at Aberdeen Proving Ground, Maryland, in accordance with DOT&E-approved test plans. EMD LFT&E focused on a limited number of tests to demonstrate specification compliance. Testing was adequate to support the Milestone C decision.

- The Marine Corps Operational Test and Evaluation Activity (MCOTEA) conducted a pre-Milestone C OA from January 2 to March 26, 2018, at Camp Pendleton, California, and the Marine Corps Air Ground Combat Center (MCAGCC) Twenty-Nine Palms, California, in accordance with DOT&E-approved Test and Evaluation Master Plan and test plan. The OA was adequate to support an evaluation of the ACV 1.1.
- The Program Manager conducted cybersecurity testing prior to the OA in the form of a Cooperative Vulnerability and Penetration Assessment (CVPA) and MCOTEA conducted the Adversarial Assessment during the OA.

Assessment

- This assessment is confined to the BAE ACV as it was the vendor selected to enter the Production and Deployment Phase. A full assessment of both vendors is contained in the June 2018 DOT&E OA report.
- The ACV section was successful in 15 of 16 missions and demonstrated the capability to negotiate terrain in the desert and littorals, operate with tanks and light armored vehicles, and maneuver to achieve tactical advantage over the opposing threat force. ACV crews, supported infantry, and the opposing force noted that the vehicles performed better than the legacy vehicle in a wide variety of areas.
  - On land, the ACV section was able to move in tactical formations, observe adjacent vehicles, and hold positions in formation.
  - During littoral operations, the ACV section was able to cross through the surf zone to enter the ocean, swim, and then come ashore through the surf zone. During one of the littoral missions, crews demonstrated the ability to load an ACV onto an LCAC, transport the ACV on the LCAC in the ocean and on land, and unload from the LCAC. LCAC crews noted that the BAE vehicle "bounced up and down" on the LCAC deck despite calm seas. This has the potential to cause the vehicle to break free of its tie-down chains in higher sea states.
- Tire failures and damage by battlefield debris delayed movement at times. One vehicle was damaged when concertina wire wrapped around drive train components, resulting in a cut brake line, damage to the inner sidewall of a tire, and damage to the central tire inflation system.
- The weight, height, and size of the ACV made recovery challenging and time consuming. When vehicles sustained severe damage to steering/suspension components or became mired, the unit relied on the M1A1 tank recovery vehicle (the M88A2) for recovery. Marine Corps M88A2s are assigned to the Tank battalion and Maintenance battalions within the Marine Division to support heavy wheeled and tracked vehicle recovery.
- The ACV threshold requirement for quantity of personnel carried is 3 crewmen and 10 embarked infantry with full combat loads, including 2 days of supply and combat essential equipment. The ACV accommodated 3 crew and 13 embarked infantry, but accommodations were cramped, which made it difficult for infantry to egress from the vehicle.
- Infantry troop commanders had difficulty moving between the hatch and their seat. Aligning the hatch with the seat could allow the commanders to stand up with their heads out of the hatch, but then drop down inside the vehicle to operate the troop commander's video display screen, talk to their marines, and prevent exposure to incoming fire.
- The Program Manager, Advanced Amphibious Assault provided a marinized remote weapons station (RWS) to both vendors as government-furnished equipment. The RWS offered several advantages over the legacy AAV reliability, availability, maintainability/rebuild to standard (RAM/RS) Upgunned Weapon Station, to include a dedicated gunner, weapon and sight stabilization, a laser range finder, and a fire control system. These features provide the capability to distinguish friendly forces from the enemy during both day and night and engage with greater precision than the legacy vehicle.
- During the OA, the BAE vehicles demonstrated an MTBOMF of 24.9 hours (50 OMFs during 1,242.6 hours of mission time), which was less than the 58-hour MTBOMF growth curve point estimate. The RWS, which is government-furnished equipment, was the source of the largest number of OMFs. The ACV program plans to continue reliability growth efforts after Milestone C.
- The CVPA focused on components in the vehicle that interacted with the Controller Area Network (CAN) bus. Test results confirmed that electronic segmentation of subsystems minimized the attack surface. Testing during the AA focused on six scenarios designed to assess time to detect, time to recover, and mission effects of cyber compromise. The classified appendix to the June 2018 DOT&E report provides additional details on the cyber vulnerabilities and recommendations.
- EMD LFT&E focused on a limited number of tests to demonstrate specification compliance and demonstrated that the ACV met all Tier 1 underbody force protection requirements (Key Performance Parameters). The classified appendix to the DOT&E June 2018 report details vulnerabilities and recommendations.

Recommendations

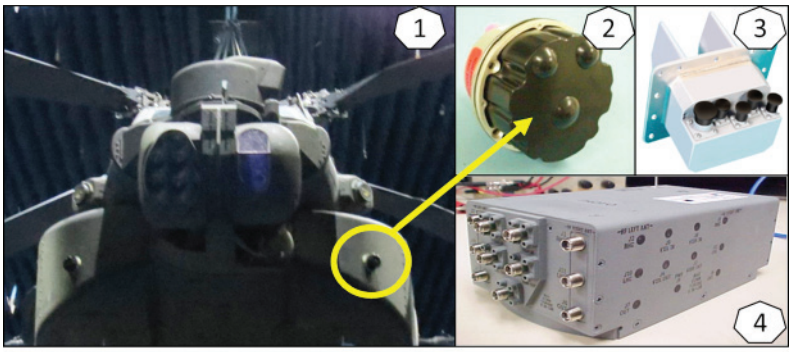
The following is a summary of key recommendations for the ACV. A complete list of recommendations for both vendors is contained in the June 2018 DOT&E OA report. The Program Manager, Advanced Amphibious Assault should:

1. Modify the infantry troop commander's station to make it easier to move between the hatch and seat.
2. Assess the capability of all existing Marine Corps recovery assets to recover the ACV.
3. Investigate options for preventing damage to steering/suspension when encountering battlefield debris, such concertina wire.

AN/APR-39D(V)2 Radar Signal Detection Set (RSDS)

Executive Summary

- Preliminary results from the Army's FOT&E and Cooperative Vulnerability and Penetration Assessment (CVPA) indicate the AN/APR-39D(V)2 radar signal detection set is effective and suitable as installed on the Army AH-64. It is effective because the D(V)2:
  - Overall, declares threat radio frequency emitters in a timely manner.
  - Overall, provides sufficient situational awareness for AH-64 aircrews to identify required threat systems and perform the prescribed tactics, techniques, and procedures (TTPs).
  - The CVPA did not identify any specific D(V)2 vulnerabilities.
- It is suitable because the few software failures had minimal mission effect because the D(V)2 system recovered immediately and automatically from each failure without requiring aircrew action.
- The Navy developmental testing identified several critical deficiencies related to aircraft integration on the MV-22B.



1. AH-64 Antenna Installation
2. High Band Quadrant Antenna
3. Low Band Directional Antenna
4. Quadrant Receiver

System

- The AN/APR-39D(V)2 is a digital upgrade to the AN/APR-39 family of analog radar warning receivers used by nearly all DOD rotorcraft.
- The AN/APR-39D(V)2 consists of the following:
  - Four new high band antennas, and a low band antenna
  - New quadrant receivers
  - A new radar data processor with two digital receivers
- The system uses either a separate display unit or integrates with the onboard aircraft displays to visually and aurally alert the pilots to active threat radars.
- For Navy aircraft, the system also acts as the electronic warfare bus controller.
- The lead Army aircraft is the AH-64 D/E and the lead Navy aircraft is the MV-22B.

Mission

Commanders employ units equipped with the AN/APR-39D(V)2 radar signal detection set to improve the mission survivability of Navy and Army aircraft by identifying radio frequency signals from threat surface-to-air missiles, airborne interceptors, and anti-aircraft artillery through cockpit alerts.

Major Contractor

Northrop Grumman – Rolling Meadows, Illinois

Activity

- All testing was completed in accordance with the DOT&E-approved test plan.
- The Army completed a CVPA at the Redstone Arsenal, Alabama, with the D(V)2 installed on an AH-64E aircraft in June 2018. This was the last test activity of the FOT&E that started in 3QFY17.
- DOT&E produced a classified report assessing the FOT&E in November 2018.
- The Navy completed Electromagnetic Environmental Effects testing on the MV-22B at Patuxent River, Maryland, in March 2018.
- The Navy completed an Integrated (combined developmental and operational) Test Three (IT-3) period with the MV-22B at the Electronic Combat Range (ECR), California, in February 2018.
- The Navy completed an anechoic chamber test with the D(V)2 installed on an MV-22B in December 2017 at the Air Combat Environment Test and Evaluation Facility (ACETEF) located in Patuxent River, Maryland.

Assessment

- The Navy IT-3 testing and anechoic chamber testing identified several critical deficiencies related to aircraft integration on the MV-22B.
- Preliminary results from the Army FOT&E demonstrated that the D(V)2 provides sufficient situational awareness for AH-64 aircrews to identify required threat systems and perform the prescribed TTPs. Aircrew operational response times, composed of the D(V)2 declaration time and the aircrew reaction time, were consistent across the different operational

missions for the AH-64. Specific detail is provided in the DOT&E classified FOT&E report.
- Preliminary results from the Army CVPA did not identify any D(V)2-specific vulnerabilities as installed on the AH-64E.
- Preliminary results based on the Army FOT&E suitability data demonstrated that the few software resets had minimal mission effect because the system recovered immediately and automatically without requiring aircrew action.

Recommendations

The Army and Navy should:

1. Implement fixes to all critical deficiencies identified in Navy integrated and anechoic chamber testing for the MV-22B before preceding into operational testing.
2. Conduct a cybersecurity Adversarial Assessment based on the CVPA to assess the ability of operational aircrews and maintainers to detect and mitigate cybersecurity threats then prioritize and implement corrective measures.
3. Implement corrections for software failures identified during the Army FOT&E to improve reliability.
4. Conduct a maintenance demonstration for both the AH-64 and the MV-22B to identify and mitigate any shortfalls that reduce system availability.

AN/SQQ-89A(V)15 Integrated Undersea Warfare (USW) Combat System Suite

Executive Summary

- In March 2016, the Navy's Operational Test and Evaluation Force (OPTEVFOR) completed operational testing on the Advanced Capability Build (ACB)-11 variant of AN/SQQ-89A(V)15, with the exception of an operational cybersecurity evaluation. The Navy was unable to schedule the cybersecurity evaluation in FY18. DOT&E submitted an IOT&E report in 1QFY19. DOT&E will submit an updated to the IOT&E report upon completion of the operational cybersecurity evaluation.
- DOT&E approved the Test and Evaluation Master Plan (TEMP) for the ACB-13 variant of AN/SQQ-89A(V)15 in December 2017.

System

- The AN/SQQ-89A(V)15 is an integrated undersea warfare (USW) combat system that is deployed on *Ticonderoga*-class cruisers and *Arleigh Burke*-class destroyers. It is composed of the sensors, processors, displays, and weapons controls to detect, classify, localize, and engage threat submarines and alert on threat torpedoes. It is an open-architecture system that includes staggered biennial software upgrades (ACBs) and biennial hardware upgrades (Technical Insertions).
  - Acoustic sensors include a hull-mounted array, Multi-Function Towed Array (MFTA) TB-37 (including a towed acoustic intercept component), calibrated reference hydrophones, helicopter, and/or ship-deployed sonobuoys.
  - Functional segments process and display active, passive, and environmental data.
- The AN/SQQ-89A(V)15 interfaces with the Aegis Combat System to prosecute threat submarines using MK 46 and MK 54 torpedoes from surface vessel torpedo tubes, Vertical Launch Anti-Submarine Rockets, or MH-60R helicopters.

Mission

- Theater and Unit Commanders use surface combatants equipped with the AN/SQQ-89A(V)15 to locate, monitor, and engage threat submarines.
- Maritime Component Commanders employ surface combatants equipped with the AN/SQQ-89A(V)15 as escorts to high-value units to protect against threat submarines during transit. Commanders also use the system to conduct area clearance and defense, barrier operations, and anti-submarine warfare (ASW) support during amphibious assault.

Major Contractor

Lockheed Martin Mission Systems and Training – Manassas, Virginia

Activity

- In December 2014, DOT&E submitted a classified Early Fielding Report for ACB-11. This report was submitted due to the installation of ACB-11 on ships that deployed prior to IOT&E.
- In March 2016, OPTEVFOR completed operational testing on ACB-11, with the exception of an operational cybersecurity evaluation. Testing was conducted in accordance with DOT&E-approved test plans.
- In September 2017, the Navy commenced development of a General Threat Torpedo (GTT) using the Resource Enhancement Project. GTT is a surrogate for threat torpedoes and supports testing torpedo defense capability. GTT is expected to overcome several current test limitations. The project delivers a single prototype.
- In FY17, the Navy scheduled the operational cybersecurity evaluation three times. Each event was deferred due to test platform operational commitments or maintenance requirements. The Navy did not schedule an operational cybersecurity evaluation in FY18.
- In December 2017, DOT&E approved the TEMP for the ACB-13 variant of AN/SQQ-89A(V)15.

Assessment

- DOT&E submitted a classified IOT&E report for ACB-11 in 1QFY19. The preliminary analyses indicate the following.
  - Testing was sufficient to evaluate ACB-11 operational effectiveness and operational suitability.
  - ACB-11 capability against cyber-attack is untested by operational testers.
  - ACB-11 submarine detection capability met Navy requirements in one test environment.
  - ACB-11 capability to support prosecution (simulated kill) with an ASW-capable aircraft (MH-60R helicopter or P-8A fixed-wing) is uncertain from the ACB-11 test events. This capability will be a primary component of ACB-13 operational effectiveness and Littoral Combat Ship operational effectiveness in ASW.
  - ACB-11 is untested against operationally relevant midget and coastal diesel submarine threats. The Navy has no representative surrogate for this type of submarine to use for test.
  - ACB-11 met Navy performance metrics for torpedo detection against a limited set of torpedoes. The Navy expects to meet these metrics against the remaining torpedoes with capability delivered in the ACB-19 variant.
  - ACB-11 software had no significant reliability or operational availability deficiencies.
  - Operational availability of MFTA is low, primarily due to extensive logistical delays associated with its repair. ACB-11 uses MFTA as a primary sensor for submarine search and torpedo defense. MFTA operational availability has demonstrated some improvement, likely due to Navy action to increase MFTA spare parts inventory.
- An updated to the IOT&E report for ACB-11 will be submitted upon completion of the operational cybersecurity evaluation. The Navy expects to schedule the cybersecurity evaluation in FY19.
- The GTT is being developed to overcome several test limitations when assessing torpedo defense capability. However, the utility of GTT in operational test depends on future Navy decisions to procure a sufficient quantity of GTTs.

Recommendations

The Navy should:

1. Complete the cybersecurity evaluation of ACB-11 as soon as practical.
2. Develop a representative surrogate for testing AN/SQQ-89A(V)15 performance against midget and coastal diesel submarine threats
3. Continue efforts to improve the operational availability of MFTAs.

CH-53K – Heavy Lift Replacement Program

Executive Summary

- CH-53K flight testing continues, using the four Engineering Development Model (EDM) aircraft, three system developmental test articles (SDTA), and the Ground Test Vehicle (GTV). The seven flyable aircraft have flown 1,212 flight hours as of September 12, 2018.
- The late December 2019 Initial Operational Capability (IOC) will be delayed. Current projections estimate that IOT&E will start in early 2021 due to the need to correct multiple design deficiencies discovered during early testing. These include: airspeed indication anomalies, low reliability of main rotor gearbox, hot gas impingement on aircraft structures, tail boom and tail rotor structural problems, overheating of main rotor dampers, fuel system anomalies, high temperatures in the #2 engine bay, and hot gas ingestion by the #2 engine, which could reduce available power. The Program Office is working a major schedule revision.
- The Program Office is requesting additional funding to complete sufficient developmental testing to enter IOT&E with a KPP compliant system. Technical problems have extended SDD well beyond original projections.
- The Program Office is transitioning the CH-53K production line from West Palm Beach, Florida, to Stratford, Connecticut. With the exception of the first four STDA aircraft, final assembly of all remaining aircraft will be completed at the Stratford facility. DOT&E is working with the Program Executive Office and the Program Office to ensure aircraft produced on the Stratford production line are production representative.
- LFT&E is ongoing. Testing of tail rotor components, cockpit and cabin armor, and the GTV against threshold threats is deferred due to funding until FY20. Live fire testing against objective, operationally relevant threats has not yet been funded.
- Navy analysis indicates the CH-53K is on track to meet the Survivability Key Performance Parameter (KPP) only if technical mitigations to unexpected deficiencies, which the Navy is currently developing, are successful. Preliminary analyses indicate that the CH-53K is more survivable than the legacy CH-53E aircraft.

System

- The CH-53K is a new-build, fly-by-wire, dual-piloted, three-engine, heavy lift helicopter slated to replace the aging CH-53E. The CH-53K is designed to carry 27,000 pounds of useful payload (three times the CH-53E payload) over a distance of up to 110 nautical miles, climbing from sea level at 103 degrees Fahrenheit to 3,000 feet above mean sea level at 91.5 degrees Fahrenheit.
- The CH-53K design incorporates the following survivability enhancements:
  - Large Aircraft Infrared Countermeasures with advanced threat warning sensors (combines infrared, laser, and hostile fire functions into a single system), an AN/APR-39D(V)2 radar warning receiver, and an AN/ALE-47 countermeasure dispensing system
  - Pilot armored seats, cabin armor for the floor and sidewalls, fuel tank inerting, self-sealing fuel bladders, and 30-minute run-dry capable gear boxes
- The Navy intends the CH-53K to maintain a shipboard logistics footprint equivalent to that of the CH-53E.

Mission

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

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

Major Contractor

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

Activity

- The Defense Acquisition Executive approved the CH-53K program's Milestone C decision for entry into low-rate initial production (LRIP) on February 28, 2017. USD(AT&L) delegated the CH-53K program to the Navy and it became an Acquisition Category 1C program on November 21, 2017.
- The program has seven flyable aircraft to support integrated developmental and operational flight testing. All four EDM aircraft have been flying in the integrated test program since EDM-4 achieved first flight on August 31, 2016. The contractor has delivered three of the six SDTAs, all of which are participating in the test program. The seven flyable aircraft have flown 1,212 flight hours as of September 12, 2018. Delivery of SDTA-4 to Patuxent River is projected for August 2019.
- The Navy used the GTV to qualify key dynamic components; assess aircraft stresses, vibrations, and rotor performance; and support long-term reliability testing and verification of aircraft systems performance. The GTV is a complete CH-53K that is fully representative of the EDM aircraft. The Navy is transporting the GTV via a transportability demonstration on a C-17 airlifter to China Lake, California. The GTV will then be the test article for full-up system-level LFT&E projected for FY20.
- Sikorsky manufactured the first four of six SDTA aircraft at its facility in West Palm Beach, Florida. The Navy intends for four SDTA aircraft to be used for IOT&E. The Program Office has incorporated retrofit periods into the master schedule to ensure these SDTA aircraft will be production representative. Final assembly of all CH-53K aircraft is transitioning to its Stratford, Connecticut, facility for the fifth and sixth SDTAs and LRIP aircraft. SDTA-5 and SDTA-6 are at the first stages of assembly. Full-rate production is planned for the Stratford plant.
- The Navy completed live fire testing of the CH-53K engine disk in November 2017 and the main and tail rotor servos in December 2017. Live fire testing of the tail rotor flex beam (which connects the tail rotor blade to the hub) is delayed pending finalization of a new design that will meet design lifetime requirements without fracturing or delaminating. The Navy is continuing to develop live fire test plans to support testing of the GTV and cabin armor at China Lake, beginning in FY20.
- In March 2018, the Program Office conducted a comprehensive survivability summit to rebaseline the assessment of overall aircraft survivability. The Navy is modifying aircraft survivability equipment (ASE) to address cybersecurity requirements (data at rest protection), mitigate obsolescence (removable media and computer processors), and reduce life-cycle cost (via elimination of components). The Navy is upgrading the infrared countermeasure subsystem and adding hostile fire indication.
- Due to ASE program delays, the Navy has deferred deployment and testing of the updated ASE and it will not be available for IOT&E. The Navy will use legacy ASE during IOT&E and will employ legacy ASE for IOC, which is slipping. The Navy intends to examine updated ASE in FOT&E and retrofit it to the fleet as it becomes available.
- The Program Office completed Revision C of the U.S. Marine Corps CH-53K Heavy-Lift Replacement Program Test and Evaluation Master Plan (TEMP) to reflect programmatic changes and updates to the cybersecurity test strategy, including a new emphasis on cybersecurity.
- The Navy is continuing testing in accordance with the DOT&E-approved TEMP and a DOT&E-approved 2010 Alternative LFT&E plan.

Assessment

- The Program Office lacks sufficient funding to complete the SDD Phase on the original timeline due to technical problems that have extended SDD beyond original projections. SDD must be fully funded as soon as possible. The December 2019 IOC may not be not achievable. Current projections estimate that IOT&E cannot start until early 2021. The Program Office is working a major schedule revision. Schedule compression pressure has the potential to adversely affect training for the IOT&E aircrews and maintainers.
- Design of the CH-53K is not finalized, aggravating schedule and cost concerns. Sikorsky continues to address design deficiencies discovered in developmental testing:
  - The aircraft pitot-static system does not provide reliable airspeed indications in various flight regimes resulting in poor automatic flight control system performance. Sikorsky is investigating relocating the pitot-static sensors but has not finalized a solution.
  - Service life projections for the main rotor gearbox are falling short of the requirement. Sikorsky is developing solutions involving modification of internal gears and their interfaces.
  - Engine and auxiliary power unit hot gas impingement on the aircraft structure during some flight regimes has not been solved. On several test flights, telemetry indicated temperatures on the composite skin of the aircraft were approaching structural limits. This necessitated termination of some maneuvers to prevent aircraft damage.
  - Testing revealed performance anomalies in the CH-53K tail boom design. The tail structure experienced unexpected vibrations and resonances, and redesign efforts are in progress to mitigate vibration-induced damage to hydraulic lines and other components in the tail.
  - The tail rotor flexbeam experienced material delamination and cracking. The first shipset of the redesigned flexbeam has been installed on EDM-1 and flight testing is in progress.
  - Main rotor dampers are overheating. The contractor has proposed a new rotor damping configuration involving lower damping action, which has been installed on EDM-1. Sikorsky is gathering and analyzing flight test data, but evaluation of the change effectiveness has not yet been completed for the entire CH-53K flight envelope.

  - Sikorsky has not finalized the fuel system configuration; the original design called for a suction-only fuel feed to reduce vulnerability to ballistic threats. General Electric is developing a liquid ring fuel pump to replace the existing pumps. Component qualification testing is underway with the first pumps to be delivered for flight test in 2QFY19. If boost pumps are required, additional live fire testing may be required.
  - The #2 engine bay is experiencing high temperatures that could damage components in that bay. The contractor has not yet identified a permanent solution.
- LFT&E against the threshold threats is ongoing. While testing revealed some vulnerabilities, preliminary analyses indicate that the CH-53K is more survivable than the legacy CH-53E against small-arms, automatic weapons fire, and legacy man-portable air-defense system threats.
- Ballistic testing of the main and tail rotor servos showed a potential for the servos to jam in some conditions when impacted with the threshold threat. Component testing of the engine disk did not indicate any significant aircraft-level vulnerability resulting from cascading damage when subjected to ballistic impact.
- The CH-53K is currently on track to meet the survivability KPP but not without mitigations to address deficiencies uncovered in testing. This includes a self-sealing coating for the main gearbox lubrication sump, which the Navy is currently investigating. Any design changes to the aircraft design to address technical deficiencies may require additional live fire testing to fully assess their effects on aircraft survivability.
- The planned Phase II live fire testing against objective threats, described in the DOT&E-approved Alternate LFT&E Strategy, has not been funded. This phase is essential for an adequate survivability assessment against operationally relevant threats. This phase includes component tests for the main rotor assembly and tail rotor hub against threshold threats, originally scheduled to support the Milestone C decisions. As a result, any deficiencies identified in this phase of testing will need to be addressed after IOC likely with engineering change proposals.

Recommendations

The Navy should:

1. Secure additional funding to:
   - Complete the SDD phase of the program
   - Complete live fire testing against objective threats
   - Accelerate LFT&E to minimize problem discovery post-IOC
2. Revise the program schedule for achievable, event-driven milestones.
3. Continue to investigate mitigations to address design deficiencies identified in test.

Coastal Battlefield Reconnaissance and Analysis (COBRA) System

Executive Summary
- The Navy conducted the Coastal Battlefield Reconnaissance and Analysis (COBRA) Block I IOT&E to evaluate the system's capability to detect and classify mine lines, mine fields, and obstacles on the beach zone in daylight.
- COBRA Block I provides an operational capability for beach reconnaissance.

System
- The COBRA system is a mission payload on the MQ-8B Fire Scout unmanned air system (UAS), which can be embarked on a Littoral Combat Ship (LCS) or other air-capable ships. The COBRA system is a component of the mine countermeasures (MCM) mission package (MP) when employed from LCS.
- The COBRA program is using evolutionary acquisition and incremental development to meet overall mine and obstacle reconnaissance requirements.
  - Block I capability is intended to provide tactical reconnaissance for detection and location of unburied mine lines, mine fields, and obstacles on the beach in daylight. The MQ-8B Fire Scout currently serves as the Block I sensor platform. The Navy declared Block I system Initial Operational Capability (IOC) in July 2017.
  - Block II is intended to enhance the COBRA system sensor to provide daytime and nighttime detection and location of unburied mine lines, mine fields, and obstacles in the beach and surf zones. The Navy expects Block II to reach IOC in FY22.
  - As currently envisioned, Block III will add the capability to detect buried mines in the beach and surf zones. The Block III IOC date has not yet been established.
- The COBRA Block I system consists of the COBRA Airborne Payload Subsystem (CAPS) and Post Mission Analysis (PMA) subsystem.
  - CAPS consists of a multi-spectral camera, installed on an MQ-8B Fire Scout as a modular payload. The system saves collected multi-spectral imagery of the target area to a Data Storage Unit (DSU) for post-mission analysis.
  - Upon aircraft recovery, the DSU is removed from CAPS and connected to the PMA subsystem. When the PMA operator has completed analysis of the data, the processed imagery is forwarded to the Mine Warfare (MIW) Environmental Decision Aids Library (MEDAL) for message formatting and further dissemination to the Mine Countermeasures Commander and other operational commanders via tactical data networks.
- The COBRA system is dependent on the UAS and shipboard systems to perform its mission.

  - Shipboard operators use the Tactical Common Data Link (TCDL) to communicate with CAPS from the MQ-8B Mission Control System (MCS) while the MQ-8B Fire Scout is in flight.
  - On LCS, MEDAL resides in the mission package application software (MPAS). The PMA subsystem and MPAS, in turn, reside on the mission package computing environment, which provides operator control, computing, networking, and storage infrastructure.
- The COBRA system provides the sensing capability for Joint Direct Attack Munition (JDAM) Assault Breaching System (JABS), a component of the Assault Breaching System, which can be used to neutralize mines and obstacles on the beach prior to an amphibious assault. The COBRA system precision location capability supports JABS targeting or identification of clear lanes to bypass mines and obstacles.
- The COBRA system provides beach reconnaissance capability for the LCS Coastal Mine Reconnaissance Mission Module in the LCS MCM MP.

Mission
- The Joint Force Commander will use LCS units equipped with the COBRA Block I system as part of the MCM MP to conduct unmanned aerial tactical reconnaissance of potential landing sites for an amphibious assault.
- The Joint Force Commander will use LCS units equipped with the COBRA Block II system as part of the MCM MP to conduct daytime and nighttime unmanned aerial tactical reconnaissance of both beach and surf zones for potential landing sites for an amphibious assault.

Major Contractor
Areté Associates – Tucson, Arizona

Activity

- DOT&E approved the COBRA Block I Cybersecurity IOT&E Plan and Change 1 to the COBRA Block I IOT&E Plan in March 2018.
- The Navy completed COBRA Block I IOT&E Test Periods Two through Five in FY18. The testing was conducted in accordance with DOT&E-approved test plans.
  - During Test Period Two, fleet sailors operated the system in the Southern California Operational Area from LCS 4 in March 2018. The MQ-8B Fire Scout with the COBRA payload completed four missions to assess its shipboard performance at sea. After each flight, trained fleet operators completed post-mission analysis of COBRA data.
  - During Test Period Three, fleet sailors conducted a Maintenance Demonstration (M-DEMO) on LCS 4 in March 2018. The M-DEMO included five maintenance vignettes each on the CAPS and PMA subsystem using simulated system faults.
  - The Navy Operational Test and Evaluation Force (OPTEVFOR) completed cybersecurity testing during Test Periods Four (Cooperative Vulnerability and Penetration Assessment) and Five (Adversarial Assessment) pier-side on LCS 4 in early March 2018 and April 2018, respectively.

Assessment

- COBRA Block I provides an operational capability for beach reconnaissance. The system did not meet the Navy Block I Capability Production Document threshold requirements for one class of targets but provides an organic, remotely operated, beach reconnaissance capability to support amphibious assault operations.
  - Test Period One of the COBRA Block I IOT&E, completed in June 2017, provided the data to evaluate the search rate, percentage of targets (mine fields, mine lines, and obstacles) detected and classified, and the target location error and false alarm rate for the targets.
  - Test Period Two (March 2018) provided additional data to assess the effectiveness of the system to detect, classify, and localize mine lines, mine fields, and obstacles in a beach zone that transitioned from plain sand to areas with beach vegetation on sand.
- The system exceeds the Navy threshold requirements for maximum false alarm rate.
- COBRA Block I exceeded all suitability threshold requirements based on results from Test Periods One through Three.
  - Test Period Two provided data that were adequate to assess the shipboard suitability.
  - The M-DEMO during Test Period Three was adequate to assess COBRA Block I maintainability using simulated system faults, but fleet sailors lacked spare parts to complete some identified parts replacement actions.
  - The COBRA Block I system performed reliably with four minor operational mission failures during IOT&E.
  - MQ-8B Fire Scout test platforms were not operational for several days during the COBRA IOT&E. MQ-8B troubleshooting and repairs required significant maintenance and technical support. The Navy acquired the MQ-8B Fire Scout variant in response to an Urgent Operational Need and did not fully assess its operational performance or suitability in IOT&E.
- COBRA Block I is cyber survivable based on testing in Test Periods Four and Five.

Recommendations

The Navy should:

1. Fund and integrate the COBRA Block I system on a more robust and reliable platform (i.e., MQ-8C).
2. Implement COBRA Block I software upgrades for image processing to reduce the false alarm rate.
3. Fund and develop the COBRA Block II system to provide nighttime and surf zone reconnaissance capability.

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

Executive Summary

- The DOT&E assessment of CVN 78 remains consistent with previous assessments. Poor or unknown reliability of systems critical for flight operations including newly designed catapults, arresting gear, weapons elevators, and radar, could affect the ability of CVN 78 to generate sorties. Reliability of these critical subsystems poses the most significant risk to the CVN 78 IOT&E timeline.
- CVN 78 completed eight Independent Steaming Event (ISE) at-sea periods in support of developmental test and ship certification. Four of these at-sea periods included fixed-wing flight operations for a total of 747 F/A-18E/F launches and arrestments. Mechanical problems forced CVN 78 to return to port early on three of the eight ISE events.
- CVN 78 will probably not achieve the Sortie Generation Rate (SGR) (number of aircraft sorties per day) requirement. Unrealistic assumptions underpin the SGR threshold requirement. These assumptions ignore the effects of weather, aircraft emergencies, ship maneuvers, and current air wing composition on flight operations. DOT&E plans to assess CVN 78 performance during IOT&E by comparing it to the demonstrated performance of the *Nimitz*-class carriers as well as to the SGR requirement.
- As of September 30, 2018, the development, installation, and delivery of the Advanced Weapons Elevators (AWE) remains behind schedule. All 11 elevators have been installed, and 2 of the 11 elevators are in government certification testing. The Navy has yet to accept delivery of any elevators due to the shipbuilder's continued development of this first of a kind system without a land-based prototype.
- The Navy previously identified an inability to readily electrically isolate Electromagnetic Aircraft Launching System (EMALS) and Advanced Arresting Gear (AAG) components to perform maintenance. This limitation precludes some types of maintenance during flight operations.
- The Navy continued performance testing of the AAG at the Jet Car Track Site at Join Base McGuire-Dix-Lakehurst, New Jersey, with 2,230 arrestments completed as of September 30, 2018. Runway Arrested Landing Site (RALS) testing with manned aircraft continues and has completed a total of 928 aircraft arrestments as of September 30, 2018. RALS testing began on E-2 and C-2 on May 24, 2018, with the first propeller aircraft fly-in arrestment occurring on the C-2 on July 18, 2018.
- CVN 78 will likely be short of berthing spaces. Reduced manning requirements drove the design of CVN 78. The berthing capacity is 4,660; more than 1,100 fewer than *Nimitz*-class carriers. Manning requirements for new technologies such as catapults, arresting gear, radar, and elevators are not well understood. Some of these concerns have required the redesignation of some berthing areas and may require altering standard manpower strategies to achieve mission accomplishment. Recent estimates of expected combined manning of CVN 78, its air wing, embarked staffs, and detachments range from 4,656 to 4,758. The estimates do not include Service Life Allowance for future crew growth.

- The Navy conducted sea-based developmental testing (SBDT) of the ship self-defense combat system aboard CVN 78 from August 2017 through June 2018. The Navy successfully corrected many previously discovered deficiencies. However, the Dual Band Radar's (DBR) false and dual tracks propagation through the integrated combat system affect its performance.
- CVN 78 exhibits more electromagnetic compatibility problems than other Navy ships. The Navy continues to characterize the problems and develop mitigation plans.
- The development and testing of AWE, EMALS, AAG, DBR, and the Integrated Warfare System will continue to drive the *Gerald R. Ford* timeline as it progresses toward IOT&E.
- The Navy continued to execute the LFT&E program to provide the data and analyses required for the evaluation of the survivability of the ship to operationally significant threats.

System

- The CVN 78 *Gerald R. Ford*-class aircraft carrier program introduces a new class of nuclear-powered aircraft carriers. It uses the same hull form as the CVN 68 *Nimitz*-class but introduces a multitude of new ship systems.
- According to design, the new nuclear power plant reduces manning levels by 50 percent compared to a *Nimitz*-class ship and produces significantly more electricity. CVN 78 uses the increased electricity to power electromagnetic catapults (instead of steam) and AAG, both designed to increase reliability and expand the aircraft launch and recover envelopes.

- CVN 78 also incorporates a phased-array DBR for air traffic control and ship self-defense ,which replaced several legacy radars used on current carriers.
- The Navy redesigned weapons elevators, handling spaces, and stowage to reduce manning, improve safety, and increase weapon throughput. AWE utilize linear electrical motors instead of legacy cable driven systems.
- CVN 78 incorporates a more efficient flight deck layout, dedicated weapons handling areas, and an increased number of aircraft refueling stations designed to enhance its ability to launch, recover, and service aircraft. The Navy set a sortie generation requirement for CVN 78 to sustain 160 sorties per 12-hour fly day for 26 days and surge to 270 sorties per 24-hour fly day for 4 days.
- The Navy intends for the ship to have increased self-defense capabilities (hard- and soft-kill), compared to current aircraft carriers. Additionally, the ship includes the following enhanced survivability features:
  - Improved protection for magazines and other vital spaces as well as shock-hardened systems/components
  - Installed and portable damage control, firefighting, and dewatering systems intended to expedite recovery from peacetime fire, flooding, and battle damage
- CVN 78 includes a new Heavy underway replenishment system capable of transferring cargo loads of up to 12,000 pounds. Currently, only one supply ship, the USNS *Arctic*, has the Heavy replenishment system installed. The Navy has no current plans to include the system on other ships.
- The Navy intends to achieve CVN 78 Initial Operational Capability in FY19 after successful completion of Post-Shakedown Availability (PSA) and Full Operational Capability in FY22 after successful completion of IOT&E and Type Commander certification.

Mission

Carrier Strike Group Commanders will use CVN 78 to:

- Conduct power projection and strike warfare missions using embarked aircraft
- Provide force and area protection
- Provide a sea base as both a command and control platform and an air-capable unit

Major Contractor

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

---

Activity

- A Test and Evaluation Master Plan (TEMP) 1610 revision is under development to update the currently approved TEMP 1610, Revision B. The Program Office is in the process of refining the Post Delivery Test and Trials (PDT&T) schedule to further integrate testing and to include the Full Ship Shock Trial (FSST) and SGR assessment.
- The Navy's long-standing, stated intent was to conduct a live test to demonstrate the SGR with 6 consecutive 12-hour fly days followed by 2 consecutive 24-hour fly days. The Navy's current strategy for assessing the SGR Key Performance Parameter during operational test is being reviewed by DOT&E, the Navy Operational Test and Evaluation Force (OPTEVFOR), and the Program Executive Officer for Carriers. OPTEVFOR leads the development of a strategy to assess the sortie generation capability of CVN 78 for inclusion in the upcoming TEMP 1610 revision. All current versions of the proposed strategy include a combination of live flights with modeling using the Navy Seabasing/Seastrike Aviation Model.
- Delays in the Independent Steaming Event (ISE) schedule and an expanded Post Shakedown Availability (PSA) adversely affected the schedule for the at-sea OT&E of CVN 78. The Program Office plans for two back-to-back phases of initial operational testing. The first phase focuses on routine unit-level operations and ship's internal workings (including cyclic flight operations with an embarked Air Wing) and culminates with successful completion of Tailored Ship's Training Availability and Final Evaluation Problem (TSTA/FEP). Phase two focuses on more complex evolutions, including tests of the integrated combat system in self-defense scenarios, and includes integrated operations with an embarked Air Wing, Destroyer Squadron and Carrier Strike Group staffs during the Composite Training Unit Exercise (COMPTUEX) at-sea period. The Navy plans to start the first phase of operational testing in FY21 and complete the second phase of operational testing in FY22. To save resources and lower costs, the test phases align with standard carrier training periods required for deployment.
- CVN 78 entered PSA on July 14, 2018.

  EMALS
  - The Navy conducted 747 F/A-18E/F launches from CVN 78.
  - As of September 30, 2018, the program conducted 3,807 dead loads (non-aircraft, weight equivalent sled) and 523 aircraft launches at the land-based test site.

  AAG
  - The Navy conducted 747 F/A-18E/F arrestments on CVN 78.
  - The Navy continues to test the AAG on a jet car track at Joint Base McGuire-Dix-Lakehurst, New Jersey. Earlier testing prompted system design changes that the program is now testing. The jet car track testing examined the F/A-18E/F performance envelope with the new design, and initial E-2C/D and C-2A testing. As of November 3, 2018, land-based jet car track testing accomplished a total of 2,230 dead load arrestments and land-based RALS testing accomplished a total of 456 F/A-18E/F, 65 EA-18G, 226 C-2A, 84 E-2C+, and 140 E-2D aircraft arrestments.

Combat System

- The Navy conducted five sea-based developmental test (SBDT) events onboard CVN 78 between August 2017 and June 2018. The Navy intended to use these events to determine the CVN 78 integrated combat system (ICS) baseline performance with respect to DBR, Ship Self-Defense System (SSDS), and Cooperative Engagement Capability (CEC) track management and support for Rolling Airframe Missile (RAM) and Evolved Seasparrow Missile (ESSM) engagements. The Navy plans to start the first phase of air warfare operational testing in 3QFY19 by conducting several missile events on the unmanned, remote-controlled self-defense test ship (SDTS).

DBR

- The radar consists of fixed array antennas both in the X- and S-bands. The X-band radar is the Multi-Function Radar and the S-band radar is the Volume Search Radar.
- The Navy completed testing of DBR at Wallops Island, Virginia, and over the course of the last year tested the system during SBDT. Multi-Function Radar testing on the SDTS began in late 2018.

Propulsion

- Propulsion issues caused the ship to return to port early from three ISE at-sea events. Main reduction gear thrust bearing problems cut short two of the ISE events and another propulsion system failure caused the third. The Navy is addressing the problems with the manufacturer.

Electromagnetic Compatibility

- Preliminary electromagnetic interference (EMI) and radiation hazard testing has been conducted by Naval Surface Warfare Center, Dahlgren Division and Naval Air Systems Command. Further testing and mitigation are planned both at sea and in port throughout PDT&T.

Live Fire Test & Evaluation

- In FY18, the Navy resumed the planning of CVN 78 FSST, which included shock trial logistics, environmental requirements, instrumentation, and related analyses. The Navy is on track to support the execution of the FSST in CY20.
- The Navy delivered two draft volumes of their latest vulnerability assessment report in August 2018. This report updates earlier (2007) survivability analyses to account for ship design maturation.

Assessment

- The delays in the ship development and initial trials pushed both phases of initial operational testing until FY21 and FY22. The delay in the ship's delivery and development added approximately 2 years to the timeline. As noted in previous annual reports, the CVN 78 test schedule has been aggressive, and the development of EMALS, AAG, AWE, DBR, and the Integrated Warfare System delayed the ship's first deployment to FY22.

Reliability

- Four of CVN 78's new systems stand out as being critical to flight operations: EMALS, AAG, DBR, and AWEs. Overall, the poor reliability demonstrated by AAG and EMALS and the uncertain reliability of DBR and AWEs could delay CVN 78 IOT&E. The Navy continues to test all four of these systems in their shipboard configurations aboard CVN 78. Reliability estimates derived from test data for EMALS and AAG are discussed in following subsections. For DBR and AWE, only engineering reliability estimates have been provided.

EMALS

- Testing to date involved 747 shipboard launches and demonstrated EMALS capability to launch aircraft planned for the CVN 78 Air Wing.
- Through the first 747 shipboard launches, EMALS suffered 10 critical failures. This is well below the requirement of 4,166 Mean Cycles Between Critical Failures, where a cycle represents the launch of one aircraft.
- The reliability concerns are exacerbated by the fact that the crew cannot readily electrically isolate EMALS components during flight operations due to the shared nature of the Energy Storage Groups and Power Conversion Subsystem inverters onboard CVN 78. The process for electrically isolating equipment is time-consuming; spinning down the EMALS motor/generators takes 1.5 hours by itself. The inability to readily electrically isolate equipment precludes EMALS maintenance during flight operations.

AAG

- Testing to date included 763 attempted shipboard landings and demonstrated AAG capability to recover aircraft planned for the CVN 78 air wing.
- The Program Office redesigned major components that did not meet system specifications during land-based testing. Through the first 763 attempted shipboard landings, AAG suffered 10 operational mission failures (which includes one failure of the barricade system). This reliability estimate falls well below the re-baselined reliability growth curve and well below the requirement of 16,500 Mean Cycles Between Operational Mission Failures, where a cycle represents the recovery of one aircraft.
- The reliability concerns are magnified by the current AAG design that does not allow electrical isolation of the Power Conditioning Subsystem equipment from high power buses, limiting corrective maintenance on below-deck equipment during flight operations.

Combat System

- Results of SBDT events indicate good SSDS performance in scheduling and launching simulated RAMs and ESSMs, as well as scheduling DBR directives for ESSM acquisition and target illumination. Insufficient interoperability testing with a CEC network and Link 16 prevents an estimate of performance in this area. It is unknown if the integration problems between SSDS and Surface Electronic Warfare Improvement Program (SEWIP) Block 2 identified during engineering testing at Wallops Island have been resolved because SEWIP Block 2 was not installed on the ship during these SBDT events.

- CVN 78's combat system testing on the SDTS is at risk due to schedule constraints, lack of funding, and insufficient planned developmental testing.

DBR

- Throughout the five CVN 78 SBDTs, DBR was plagued by extraneous false and close-in dual tracks adversely affecting its performance.
- Integration of the DBR electronic protection capabilities remains incomplete and unfunded. With modern threats, a lack of electronic protection places the ship in a high-risk scenario if deployed to combat.
- The Navy analysis noted that DBR performance needs to be improved to support carrier air traffic control center certification.

Sortie Generation Rate

- CVN 78 is unlikely to achieve its SGR requirement. The target threshold is based on unrealistic assumptions including fair weather and unlimited visibility, and that aircraft emergencies, failures of shipboard equipment, ship maneuvers, and manning shortfalls will not affect flight operations. During the 2013 operational assessment, DOT&E conducted an analysis of past aircraft carrier operations in major conflicts. The analysis concludes that the CVN 78 SGR requirement is well above historical levels.
- DOT&E plans to assess CVN 78 performance during IOT&E by comparing it to the SGR requirement as well as to the demonstrated performance of the *Nimitz*-class carriers.
- Poor reliability of key systems that support sortie generation on CVN 78 could cause a cascading series of delays during flight operations that would affect CVN 78's ability to generate sorties. The poor or unknown reliability of these critical subsystems represents the most risk to the successful completion of CVN 78 IOT&E.

Manning

- Based on current expected manning, the berthing capacity for officers and enlisted will be exceeded by approximately 100 personnel with some variability in the estimates. This also leaves no room for extra personnel during inspections, exercises, or routine face-to-face turnovers.
- Planned ship manning requires filling 100 percent of the billets. This is not the Navy's standard practice on other ships, and the personnel and training systems may not be able to support 100 percent manning. Additionally, workload estimates for the many new technologies such as catapults, arresting gear, radar, and weapons and aircraft elevators are not yet well understood.

Electromagnetic Compatibility

- Developmental testing identified significant EMI and radiation hazard problems. The Navy continues to characterize and develop mitigation plans for the problems, but some operational limitations and restrictions are expected to persist into IOT&E and deployment. The Navy will need to develop capability assessments at differing levels of system utilization in order for commanders to make informed decisions on system employment.

Live Fire Test & Evaluation

- The vulnerability of CVN 78's many new critical systems to underwater threat-induced shock is unknown. The program plans to complete shock testing on EMALS, AAG, and the AWE components during CY19, but because of a scarcity of systems, shock testing of DBR components lags and will likely not be completed before the FSSTs.
- The Vulnerability Assessment Report provides an assessment of the ship's survivability to air-delivered threat engagements. The classified findings in the report identify the specific equipment that most frequently would lead to mission capability loss. In FY19, the Navy is scheduled to deliver additional report volumes that will assess vulnerability to underwater threats and compliance with Operational Requirements Document survivability criteria.

Recommendations

The Navy should:

1. Provide schedule, funding, and an execution strategy for assessing SGR. This strategy should specify which testing will be accomplished live, a process for accrediting the Seabasing/Seastrike Aviation Model for operational testing, and a method for comparing CVN 78 performance with that of the *Nimitz* class.
2. Continue to characterize the electromagnetic environment onboard CVN 78 and develop operating procedures to maximize system effectiveness and maintain safety. As applicable, the Navy should utilize the lessons learned from CVN 78 to inform design modifications for CVN 79 and future carriers.
3. Develop and implement DBR electronic protection to enhance ship survivability against modern threats.
4. Submit an updated TEMP.

Distributed Aperture Infrared Countermeasure System (DAIRCM)

Executive Summary

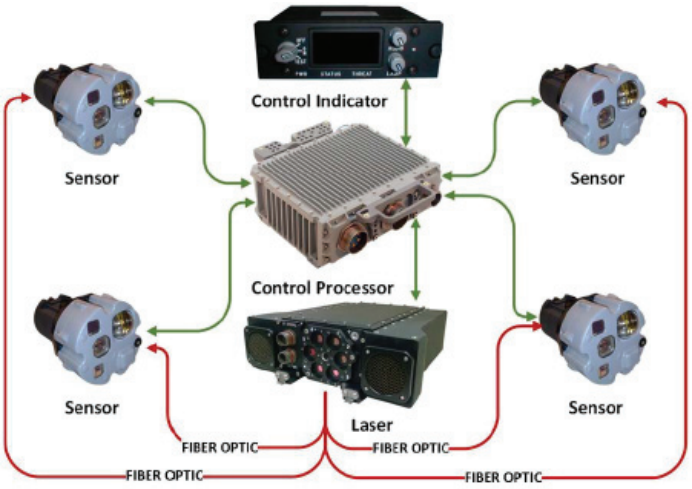
Preliminary results from Air Force and Navy testing indicate the Distributed Aperture Infrared Countermeasures (DAIRCM) system has the capability to defeat the required threat identified in the Joint Urgent Operational Needs (JUON) Statement SO-0010 dated March 30 ,2015, and defeat vehicle-launched infrared-guided missiles and man-portable air-defense systems (MANPADS).

System

- The DAIRCM system is an integrated suite of missile warning, laser warning, hostile fire indicator, and infrared countermeasure (IRCM) components designed to protect rotary-wing aircraft from the threat posed by infrared missiles.
- The system uses a single-centrally installed laser that can feed all of the beam directors. The missile warning sensor detects an incoming missile threat and sends the information to the processor which then notifies the aircrew through the control interface unit and initiates the laser to direct jamming energy at the incoming missile.
- The Navy's Program Office for Advanced Tactical Aircraft Protection Systems, PMA-272, is the lead for developing the DAIRCM System.

Mission

- Commanders employ rotorcraft equipped with the DAIRCM system to conduct medium and heavy lift logistical support, medical evacuation, search-and-rescue, armed escort, and attack operations.



- During missions, the DAIRCM system is intended to provide automatic protection for rotary-wing aircraft against shoulder-fired, vehicle launched, and other infrared missiles.

Major Contractors

- Leonardo Digital/Retrieval Systems (DRS) Infrared Sensors and Systems – Dallas, Texas
- Leonardo DRS Daylight Solutions – San Diego, California

Activity

- The Air Force accomplished effectiveness testing on a limited functionality configuration of the DAIRCM system (software version 1.0) installed on an HH-60G aircraft at Nellis AFB, Nevada, and at Redstone Arsenal, Huntsville, Alabama. The Air Force accomplished infrared environmental clutter testing while flying between Nellis AFB and Redstone Arsenal Range. Testing occurred from May 15 through July 20, 2018, and the Air Force conducted operational testing in accordance with the DOT&E-approved test plan.
- The Navy accomplished live missile firings against a DAIRCM system mounted on a scaffold (not installed on an aircraft) with software version 1.0 to assess the system's ability to identify, track, and defeat actual incoming missiles. Testing was accomplished at Dugway Proving Ground, Utah, from September 10 – 28, 2018.
- The Navy accomplished Electromagnetic Environmental Effects testing with DAIRCM installed on an MH-60 aircraft at the Naval Air Station Patuxent River, Maryland, in October and November 2018.
- The Navy continues to develop and mature the full functionality DAIRCM system (software version 2.0), which includes full built-in-test (BIT) capabilities, for the Navy's planned Quick Reaction Assessment.
- The Navy continues to develop and mature the missile warning digital system model (DSM) at the Air Combat Environment Test and Evaluation Facility (ACETEF) located at Naval Air Station Patuxent River, Maryland.

Assessment

- Preliminary results indicate that the DAIRCM system as installed on the HH-60G has the capability to defeat the required threat identified in the JUON Statement SO-0010 dated March 30, 2015.
- Preliminary results indicate that the DAIRCM system as installed on the HH-60G has the capability to defeat vehicle-launched infrared-guided missiles and MANPADS.

Recommendations

The Navy should:

1. Conduct hostile fire and laser warning testing on the full functionality DAIRCM configuration (software version 2.0).
2. Conduct regression testing for missile warning performance with the full functionality DAIRCM configuration (software version 2.0).
3. Complete the verification and validation of the missile warning DSM.

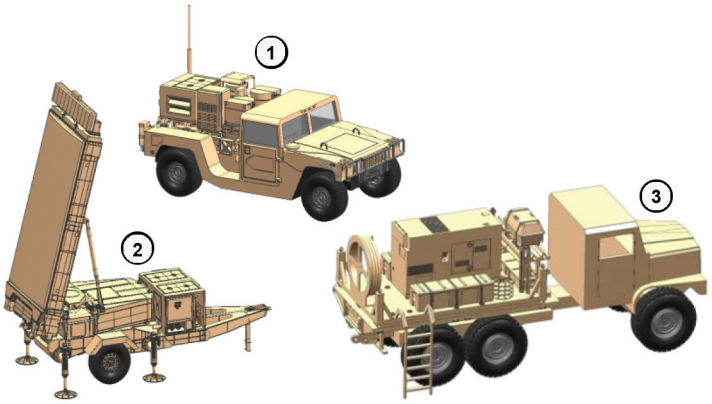
Ground/Air Task Oriented Radar (G/ATOR)

Executive Summary

- The Ground Air/Task Oriented Radar (G/ATOR) Block 1 and Block 2 Developmental Test (DT) 1C and 1D are complete. Operational Assessments (OAs) for Block 1 and Block 2 are also complete. Six low-rate initial production (LRIP) systems in the Gallium Arsenide (GaAs) configuration supported DT1C, DT1D, and both OAs. LRIP systems in the Gallium Nitride (GaN) configuration will support DT1E and both IOT&Es.
- DT1C testing at Marine Corps Outlying Landing Field (MCOLF) Atlantic, North Carolina, was limited in scope; however, Block 1 demonstrated the ability to detect and track aircraft targets in the littoral environment and its ability to support the intended mission areas.
- During DT1C, the Program Management Office (PMO) led and the Marine Corps Operational Test and Evaluation Activity (MCOTEA) observed a Cooperative Vulnerability Assessment (CVA) and a limited Adversarial Assessment (AA). Though the CVA and AA identified cyber vulnerabilities, they were not sufficient to support a full assessment.
- During the Block 1 OA, the system demonstrated the capability to integrate into the Marine Air Command and Control System and to successfully track targets in support of air surveillance and air defense missions, but was not assessed against all target types. Block 1 demonstrated progress towards meeting reliability requirements, and did meet its operational availability requirement. The OA data were used to support an early fielding decision for two Block 1 systems in the GaAs configuration. DOT&E endorsed the early deployment in February 2018.
- During the Block 2 OA, the system demonstrated the capability to track targets in support of counterfire missions and demonstrated significant progress towards meeting reliability and availability requirements. Block 2 did not meet the time requirements for displacement and emplacement of the system. The PMO did not request an early fielding for Block 2.
- DT1E for both Block 1 and Block 2 in the GaN receiver/transmitter configuration are complete.
- IOT&E of Block 1 completed in October 2018. Evaluation and reporting are in progress. IOT&E for Block 2 is scheduled for 1QFY19.

System

- The AN/TPS-80 G/ATOR is a short- to medium-range, air-cooled Active Electronically Scanned Array (AESA) radar under development for the Marine Corps. It is intended to replace up to five current radar systems and augment the AN/TPS-59 long-range radar. The PMO plans to procure 45 G/ATOR systems.



1 - Communications Equipment Group (CEG)
2 - Radar Equipment Group (REG)
3 - Power Equipment Group (PEG) on MTVR pallet
MTVR - Medium Tactical Vehicle Replacement

- The PMO is developing G/ATOR in three increments.
  - Block 1 develops the basic hardware and provides Air Defense/Surveillance Radar (AD/SR) capability. It replaces the AN/UPS-3, AN/MPQ-62, and AN/TPS-63 radar systems.
  - Block 2 is a Ground Weapons Locating Radar (GWLR) to acquire, track, and classify hostile indirect fire and replaces the AN/TPQ-46 radar system.
  - Block 3 was a series of enhancements, including Identification Friend or Foe Mode 5/S that will now be engineering changes. The term Block 3 is no longer used.
  - Block 4 replaces the AN/TPS-73 radar system for Expeditionary Airport Surveillance Radar capability, which will be a future development effort.
- The G/ATOR baseline system configuration is comprised of three subsystems:
  - The Radar Equipment Group consists of the radar array mounted on an Integrated Mobile Pallet trailer towed by a Medium Tactical Vehicle Replacement.
  - The Power Equipment Group includes a 60-kilowatt generator and associated power cables mounted on a pallet. The generator pallet is carried by a Medium Tactical Vehicle Replacement.
  - The Communications Equipment Group provides the ability to communicate with and control the radar and is mounted inside the cargo compartment of a High Mobility Multi-purpose Wheeled Vehicle.
- The first six LRIP systems have receiver/transmitter modules built using GaAs. Subsequent systems, representing the majority of the production buy, will have GaN receiver/transmitter modules.

Mission

The Marine Air-Ground Task Force (MAGTF) commander will employ G/ATOR within the Air Combat Element (ACE) and the Ground Combat Element (GCE). Within the ACE, G/ATOR Block 1 will provide enhanced situational awareness and additional capabilities to conduct short- to medium-range radar surveillance and air defense, and air traffic control missions. Within the GCE, G/ATOR Block 2 will provide ground weapons locating capability for conduct of counter-battery/counter-fire missions.

Major Contractor

Northrop Grumman Mission Systems – Linthicum, Maryland

Activity

- The PMO delivered six G/ATOR LRIP systems with GaAs semi-conductor technology. LRIP systems supported DT1C, DT1D, and both OAs.
- The PMO conducted DT1C for Block 1 from May 2017 to September 2017 at NASA Wallops Flight Facility, Virginia; Marine Corps Air Station (MCAS) Cherry Point, North Carolina; MCOLF Atlantic, North Carolina; and MCAS Yuma, Arizona. DT1C included interoperability testing at Wallops Flight Facility, and at MCAS Cherry Point, while littoral testing was conducted at MCOLF Atlantic. Additionally, a PMO-led Marine Corps Information Assurance Red Team conducted a CVA and a limited AA during DT1C.
- DT1D for Block 2 was conducted from September 2017 to March 2018 at U.S. Army Yuma Proving Ground (YPG), Yuma, Arizona, and White Sands Missile Range, New Mexico. During DT1D data were collected in support of counter-battery/counter-fires missions against rocket, mortar, and artillery munitions.
- The Marine Corps completed OAs for both Block 1 and Block 2 during FY18 in accordance with DOT&E-approved test plans. The Block 1 OA was completed in October 2017 at MCAS Yuma, Arizona, and the Block 2 OA was completed in May 2018 at YPG, Yuma, Arizona. The results from the Block 1 OA supported an early fielding decision. DOT&E endorsed the early deployment in February 2018. The PMO did not request an early fielding for Block 2.
- DT1E for both Block 1 and Block 2 in the new GaN receiver/transmitter configuration was completed at MCAS Yuma, Arizona, and at YPG, Yuma, Arizona.
- Since the Marine Corps was collecting data in an operationally realistic environment, DOT&E approved DT1C, DT1D, and DT1E as integrated tests with MCOTEA observation. Further, DOT&E approved data collected to support the Block 1 and Block 2 OAs and IOT&Es.
- The IOT&E of Block 1 completed in October 2018. Block 2 IOT&E is scheduled for 1QFY19.

Assessment

- The CVA and limited AA conducted during DT1C helped to characterize system cyber vulnerabilities. However, they were not conducted under operationally realistic conditions and did not assess operator responses to various cyber-attacks in end-to-end scenarios and therefore cannot support a full assessment.
- Littoral testing at MCOLF Atlantic was limited in scope, using scheduled aircraft sorties as well as aircraft targets of opportunity. Block 1 was able to detect and track these targets in the littoral environment, demonstrating its support of the following mission areas: surveillance, positive control of friendly aircraft, and intercept of hostile aircraft and missiles.
- During the Block 1 OA, the system maintained connectivity with the Composite Tracking Network and integrated into a Cooperative Engagement Capability Network. Further, Block 1 integrated with the Phase 2, Common Aviation Command and Control System and was capable of successfully supporting Marines conducting air surveillance/air defense missions from within the Tactical Air Operations Center. However the target resources during the OA were limited and data were not collected against all target types to make a full operational assessment of the system's capabilities. Block 1 demonstrated progress, but did not meet all reliability requirements, predominately due to software instability. Block 1 met its availability requirement.
- During the Block 2 OA, the system was capable of tracking counter-battery threat targets; however, the system did not quite meet availability requirements. As with Block 1, software stability problems, particularly during startup, degraded system reliability. This is amplified for Block 2 because the counter-battery mission requires more frequent displacement and emplacement of the system, when compared to Block 1. Additionally, Block 2 did not meet time requirements for displacement and emplacement.

Recommendations

1. The PMO should continue to monitor G/ATOR reliability and availability during the current developmental testing in preparation for the upcoming IOT&Es scheduled for 1QFY19. Additionally, the PMO should note any changes to reliability and availability as a result of the introduction of the GaN-based technology.
2. In order to fully assess G/ATOR capabilities, MCOTEA should ensure that the Marine Corps Information Assurance Red Team conducts a Cooperative Vulnerability and Penetration Assessment (CVPA) and an AA on both the Block 1 and Block 2 systems in an operationally realistic environment in support of IOT&E. The CVPA and AA should also assess operator responses to various cyber attacks in end-to-end scenarios.

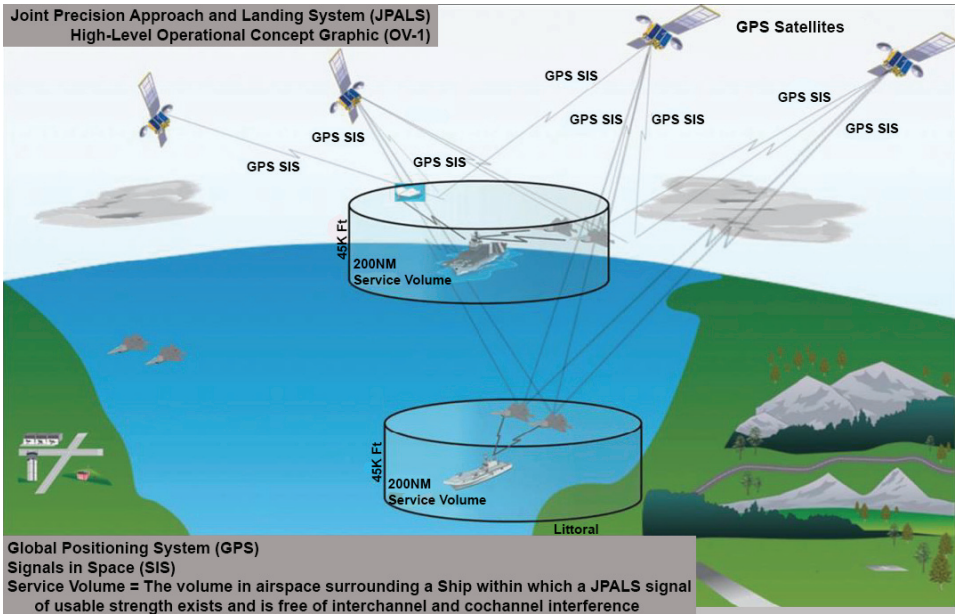
3. MCOTEA should ensure that operationally realistic testing is conducted for all target types during IOT&E or during integrated test to fully assess G/ATOR capabilities to meet operational requirements.

Joint Precision Approach and Landing System (JPALS)

Executive Summary

- As of the end of FY18, DOT&E's analysis of the data and results for the Joint Precision Approach and Landing System (JPALS) Block 0 is ongoing; however, preliminary observations from the Navy's IOT&E period indicate JPALS Block 0 will meet the Program Office's objectives to support an Early Operational Capability decision.
- The Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted the JPALS Block 0 IOT&E. This consisted of an at-sea period with an F-35B, an at-sea period with an F-35C, and one pier-side test period.
- The Navy will conduct an operational assessment of the JPALS Block 1 Full Operational Capability in 3QFY19.

Joint Precision Approach and Landing System (JPALS)
High-Level Operational Concept Graphic (OV-1)



Global Positioning System (GPS)
Signals in Space (SIS)
Service Volume = The volume in airspace surrounding a Ship within which a JPALS signal of usable strength exists and is free of interchannel and cochannel interference
The JPALS OV-1 description:
The OV-1 describes a Sea-Based JPALS program that will secure the minimum acceptable capability to support the joint military requirement and safeguard the future precision approach and landing capability of any JPALS-equipped aircraft (e.g., F-35B/C and MQ-25A) during operations at sea in virtually any weather condition within platform limitations.

System

- JPALS is composed of modular open-system hardware and software components integrated with shipboard Air Traffic Control and landing system architectures for JPALS data display and functional operation.
- JPALS major subsystems include the following: GPS sensor, navigation processing, datalink, ship motion sensor, maintenance, and ship interface subsystems.
- JPALS Block 0 is an interim solution/Early Operational Capability of JPALS, specifically to support the F-35B. Block 0 uses an ultrahigh frequency data broadcast to transmit a subset of the JPALS precision approach data and on-deck Inertial Navigation System alignment from ship to aircraft.
- JPALS Block 1 will further support the F-35B/C and MQ-25A with a two-way datalink capability by providing the accuracy, integrity, and continuity required for future F-35C and MQ-25A autoland capability on CVN-type ships and F-35B coupled flight capability on LH-type ships.

Mission

- The Navy will use JPALS to address precision approach and landing as an enabling capability for F-35B/C and MQ-25A to conduct their missions with minimal impact from conditions at point of departure or landing.
- The Navy will use JPALS to provide joint operational capability for F-35B/C and MQ-25A to perform missions for stand-alone or close-proximity air operations from CVN- and LH-type ships throughout the world.

Major Contractor

Raytheon Network Centric Systems – Fullerton, California

Activity

- JPALS Block 0 IOT&E consisted of one pier-side test period and two at-sea test periods.
- OPTEVFOR conducted pier-side testing on USS *Essex* (LHD 2) from September 9 – 24, 2017, at Naval Base San Diego, California, and focused on cybersecurity and system maintainability.
  - The OPTEVFOR Cyber Test Team (CTT) conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) followed by an Adversarial Assessment (AA).
  - OPTEVFOR, with Navy and Raytheon contractors, performed operational maintenance tasks to assess system maintainability.
- OPTEVFOR conducted the following at-sea test periods of JPALS operational usage on CVN and LHD ships to support the Navy's Early Operational Capability decision:
  - JPALS with F-35B aircraft tested at-sea onboard USS *Wasp* (LHD 1) in May 2018

  - JPALS with F-35C aircraft tested at-sea onboard USS *Lincoln* (CVN 72) in August 2018
- The Navy will conduct an operational assessment of the JPALS Block 1 Full Operational Capability in 3QFY19.
- OPTEVFOR conducted all testing in accordance with a DOT&E-approved Test and Evaluation Master Plan and test plan.

Assessment

- As of the end of FY18, DOT&E's analysis of the data and results from the IOT&E, CVPA, and system maintainability tests for JPALS Block 0 are ongoing.
- Preliminary observations from the IOT&E period indicate JPALS Block 0 will meet the Program Office's objectives to support an Early Operational Capability decision.

Recommendation

1. The JPALS Program Office should continue to coordinate with the F-35 and MQ-25 Program Offices to ensure synchronized testing.

LHA 6 New Amphibious Assault Ship (formerly LHA(R))

Executive Summary

- In FY18, the Navy completed the ship self-defense portion of IOT&E. LHA 6 deployed in July 2017 with a Marine Expeditionary Unit (MEU) Aviation Combat Element (ACE) that includes AV-8B Harrier aircraft. The Navy will not complete the operational evaluation of the ship's ability to support a complement of 20 F-35B aircraft until FY21.
- DOT&E will publish an IOT&E report in early 2QFY19 detailing findings of the LHA 6 operational effectiveness, suitability, and survivability.
- LHA 6 is effective for mobility and seaworthiness.
- Operational testing demonstrated that LHA 6 is effective at supporting some Marine Corps missions, but testing was not adequate to demonstrate the ship's effectiveness at supporting the full Marine Corps range of operations at an operationally realistic tempo.
- LHA 6 is suitable for mobility and amphibious warfare.
- LHA 6 cybersecurity testing identified deficiencies.
- Detailed results of ship self-defense testing, cybersecurity testing, and survivability can be found in the classified DOT&E LHA 6 IOT&E report.

System

- LHA 6 is the lead ship of this new class of large-deck amphibious assault ships designed to support a notional mix of MEU ACE fixed- and rotary-wing aircraft consisting of 12 MV-22 Ospreys, 6 F-35B (Short Take-Off/Vertical Landing (STOVL) variant), 4 CH-53Es, 7 AH-1s/UH-1s, and 2 Navy MH-60 Search and Rescue aircraft, or an alternate loadout of 20 F-35Bs and 2 MH-60 Search and Rescue aircraft. Key ship features and systems include the following:
  - A greater aviation storage capacity and an increase in the size of the hangar bay to accommodate the enhanced aviation maintenance requirements for the MEU ACE with embarked F-35B and MV-22. Additionally, two maintenance areas with high-overhead clearance have been incorporated in the hangar bay to accommodate maintenance on MV-22s in the spread configuration (wing spread, nacelles vertical, and rotors spread).
  - The ship does not have a well deck. Aviation assets must be used to transfer personnel and equipment to and from the beach.
  - Shipboard medical spaces were reduced in size by approximately two thirds compared to contemporary LHDs to accommodate the expanded hangar bay.
- The LHA 6 combat system used for defense against air threats and small surface threat craft includes the following major components:
  - The Ship Self-Defense System (SSDS) MK 2 Mod 4B supporting the integration and control of most other combat system elements

  - The AN/SPS-48E and AN/SPS-49A air search radars and the AN/SPQ-9B horizon search radar
  - USG-2 Cooperative Engagement Capability (CEC) real-time sensor netting system
  - The Rolling Airframe Missile (RAM) and the Evolved Seasparrow Missile (ESSM), with the NATO Seasparrow MK 9 Track Illuminators
  - The AN/SLQ-32B(V)2 with the Surface Electronic Warfare Improvement Program Block 1 (SEWIP Block 1) with the Nulka electronic decoy-equipped MK 53 Decoy Launching System
  - The Phalanx Close-In Weapon System Block 1B and the MK 38 Mod 2 Gun Weapon System
- Two marine gas turbine engines, two electric auxiliary propulsion motors, and two controllable pitch propellers provide propulsion. Six ship service diesel generators provide electric power.
- Command, control, communications, computers, and intelligence (C4I) facilities and equipment support Marine Corps Landing Force operations. The Navy is currently installing the Consolidated Afloat Networks and Enterprise Services (CANES) on the LHA 6, and the LHA 7 design and beyond will deploy with CANES incorporated.
- To reduce vulnerability and enhance recoverability following threat impact, the ship has the following survivability features:
  - Improved ballistic protection for magazines and other vital spaces as well as the inclusion of some shock hardened systems and components
  - Various installed and portable damage control, firefighting, and dewatering systems
- The Navy classifies both LHA 6 and LHA 7 as LHA Flight 0 ships. The Navy will introduce a Flight 1 variant of the LHA(R) program with the third ship, LHA 8. It will gain a well deck for deploying surface connectors to move troops and

equipment ashore, a modified flight deck, and smaller island intended to enable an aviation support capability similar to LHA 6.

Mission

The Joint Maritime Component Commander will employ LHA 6 to:

- Serve as the primary aviation platform within an Amphibious Ready Group providing space and accommodations for Marine Corps vehicles, cargo, ammunition, and more than 1,600 troops
- Serve as an afloat headquarters for an MEU, Amphibious Squadron, or other Joint Force commands using its C4I facilities and equipment to provide mission support
- Accommodate elements of a Marine Expeditionary Brigade when part of a larger amphibious task force
- Carry and discharge combat service support elements and cargo to sustain the landing force

Major Contractors

- LHA 6: Huntington Ingalls Industries, Ingalls Shipbuilding Division – Pascagoula, Mississippi
- SSDS: Raytheon – San Diego, California
- RAM: Raytheon – Tucson, Arizona, and RAMSys – Ottobrunn, Germany
- ESSM: Raytheon – Tucson, Arizona
- CEC: Raytheon – St. Petersburg, Florida
- SEWIP Block 1: General Dynamics Advanced Information Systems – Fair Lakes, Virginia

---

Activity

- The Navy Operational Test and Evaluation Force (OPTEVFOR) completed the ship self-defense Probability of Raid Annihilation (PRA) Modeling and Simulation (M&S) test bed phase of IOT&E in January 2018 in accordance with a DOT&E-approved test plan.
- LHA 6 deployed in July 2017. The Navy will not complete the operational evaluation of the ship's ability to support a complement of 20 F35-B JSF aircraft until 2021.
- The Navy did not conduct the Advanced Mine Simulation System (AMISS) trial to characterize the susceptibility of the LHA 6 to mines, as agreed to in the DOT&E-approved Test and Evaluation Master Plan (TEMP) Revision A. Because this test was not conducted, the evaluation of mine susceptibility is limited.
- The Navy is developing a revision to the LHA(R) TEMP (Revision B) to address near-term developmental testing and follow-on test and evaluation events, to include the LHA 8 Operational Assessment and LHA Flight 0 F-35 FOT&E. Once Revision B is approved, the Navy intends to commence development of TEMP Revision C to support detailed planning for the operational test (including cybersecurity) and LFT&E of LHA Flight 1.

Assessment

- LHA 6 is effective for mobility and seaworthiness.
- Operational testing demonstrated that LHA 6 is effective at supporting some Marine Corps missions, but testing was not adequate to demonstrate effectiveness at supporting the full Marine Corps range of operations. LHA 6 can support Marine Corps amphibious warfare mission tasks: load and unload cargo and vehicles from aircraft, launch and recover aircraft, and muster and load marines. However, the movement of marines, cargo, and vehicles executed during testing was insufficient to generate a realistic operational tempo required by the Operational Test Agencies for an adequate operational test. If the Navy and Marine Corps desire to combine pre-deployment exercises with IOT&E for future amphibious ship programs, this shortcoming must be mitigated.
- LHA 6 is suitable for mobility and amphibious warfare.
- LHA 6 cybersecurity testing identified deficiencies.
- Detailed results of ship self-defense testing, cybersecurity testing, and survivability can be found in the classified DOT&E IOT&E report.

Recommendations

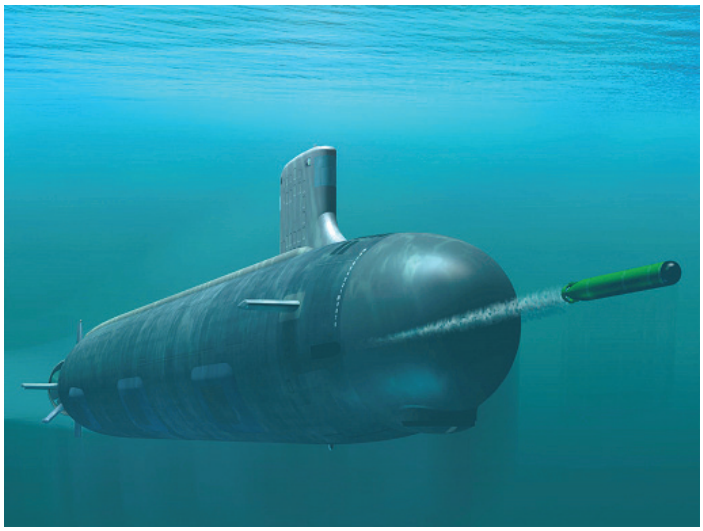
The Navy should:

1. Not repeat the LHA 6 Amphibious Warfare (AMW) IOT&E execution. For future amphibious ship test programs in which the Navy desires to combine IOT&E with fleet pre-deployment exercises, organize a subset of days in which the Operational Test Agencies have control over mission planning, mission execution, and data collection to ensure execution of an adequate AMW IOT&E.
2. Program and resource an AMISS trial in the LHA(R) TEMP Revision B.

MK 48 Torpedo Modifications

Executive Summary
- The Navy commenced operational test of the MK 48 torpedo with Advanced Processor Build (APB-5) software in FY18, specifically APB-5 torpedo capability against threat submarines. The Navy used an integrated testing approach and completed the following test events:
  - Three developmental test events that incorporated operational test objectives.
  - One dedicated operational test event.
- The Navy deferred operational test of APB-5 torpedo capability against surface ships pending completion of additional developmental testing.
- The Navy expects to complete operational test of the APB-5 torpedo in early 2020.

System
- The MK 48 torpedo is the only anti submarine and anti-surface ship weapon used by U.S. submarines.
- Fielded MK 48 torpedo variants include MK 48 Mod 6, Mod 6 ACOT, and Mod 7 Common Broadband Advanced Sonar System (CBASS).
- Torpedo improvements are made within CBASS variants as a shared development effort with the Royal Australian Navy. Torpedo improvements are primarily software based and the torpedo is commonly referred to by its software build (e.g. APB-5 torpedo).
- The torpedo software in development is APB-5. APB-5 is for Mod 7 CBASS only.



Mission
The Submarine Force employs the MK 48 torpedo to destroy surface ships and submarines in all ocean environments.

Major Contractor
Lockheed Martin Sippican Inc. – Marion, Massachusetts

Activity
- In November 2017, DOT&E approved the Joint Test and Evaluation Master Plan for the MK 48 Mod 7 Heavyweight Undersea Weapons Improvements Increment I program, referred to as the APB-5 torpedo.
- In March 2018, the Navy completed development of the Submarine Launched Modular 3-inch Device (SLAM-3D) with combined funding from the Resource Enhancement Project and the Navy. SLAM-3D was developed as a surrogate for threat representative torpedo countermeasure capability.
- In April 2018, the Navy conducted developmental testing that was coordinated with operational testers to support operational test objectives. Testing was conducted in accordance with a DOT&E-approved data collection plan and included the following events.
  - In April 2018, the Navy tested 10 APB-5 torpedoes against a U.S. naval warship.
  - In June 2018, the Navy tested five APB-5 torpedoes against a U.S. submarine.
  - In July 2018, the Navy tested nine APB-5 torpedoes against an Australian naval vessel and a Canadian naval vessel.
- In August 2018, the Navy concluded the APB-5 torpedo is ready to undergo operational testing against submarines. The Navy deferred operational testing against surface ships pending completion of additional developmental testing.
- In September 2018, the Navy conducted operational testing of the APB-5 torpedo in accordance with a DOT&E-approved test plan. The Navy tested 14 APB-5 torpedoes in anti-submarine warfare scenarios against a U.S. nuclear submarine and an Australian diesel submarine. The Navy employed SLAM-3D during several of the target evasions.

Assessment
- Operational testing of the APB-5 torpedo will continue through FY20. No preliminary assessment can be made on APB-5 torpedo capability against either threat submarines or threat surface ships.

- SLAM-3D supports a more complete evaluation of APB-5 torpedo capability by providing threat representative countermeasure performance to test against.

Recommendation

1. The Navy should develop an unmanned and mobile submarine surrogate for operational test of future MK 48 torpedo capability. The surrogate should support operationally representative response to an incoming torpedo and should allow minimal depth separation to be used between the tested torpedo and the target.

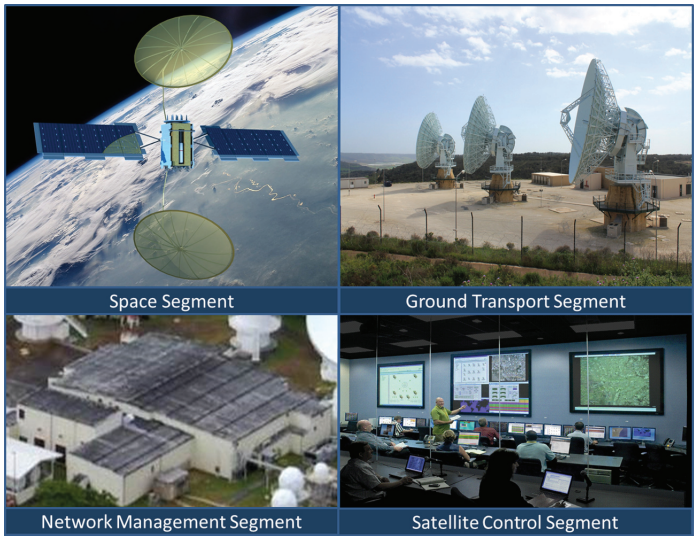
Mobile User Objective System (MUOS)

Executive Summary

- The Mobile User Objective System (MUOS) Program Office conducted five Developmental Test Assist (DTA) events with the Navy's Operational Test and Evaluation Force (OPTEVFOR) and DOT&E observation. The DTA events demonstrated new capability and system improvements made since the previous FY16 Multi-Service Operational Test and Evaluation (MOT&E-2), when DOT&E assessed MUOS as not effective, not suitable, and not cyber-secure.
- The U.S. Army Space and Missile Defense Command/ Army Forces Strategic Command (SMDC/ARSTRAT) conducted an operational management exercise from July 16 – 20, 2018, with geographically-dispersed Regional Satellite Communications (SATCOM) Support Centers (RSSC) planners and the MUOS Network Management Facility (NMF) managers in Wahiawa, Hawaii, that exercised and refined help desk operations and system restoral standing operations procedures to improve support for MUOS operational users.
- The Navy plans to conduct Developmental Test Technical Evaluation-3 (TECHEVAL-3) from November 26 through December 21, 2018, followed by an Integrated Test period from January 7 through May 1, 2019, to demonstrate readiness to enter into FOT&E.
- OPTEVFOR plans to conduct the MUOS FOT&E from June 3 through August 15, 2019 with operational users from the Army, Navy, and Marine Corps.

System

- MUOS is a satellite-based communications network designed to provide worldwide, narrowband, beyond line-of-sight, point-to-point, and netted communication services to multi-Service organizations of fixed and mobile terminal users. The Navy designed MUOS to provide 10 times the throughput capacity of the current narrowband satellite communications. The Navy intends for MUOS to provide increased levels of system availability over the current constellation of ultrahigh frequency (UHF) Follow-On satellites and to improve availability for small, disadvantaged terminals.
- MUOS consists of six segments:
  - The Space Segment consists of four operational satellites and one on-orbit spare. Each satellite hosts two payloads: a legacy communications payload that mimics the capabilities of a single UHF Follow-On satellite and a MUOS communications payload.
  - The Ground Transport Segment is designed to manage MUOS communication services and allocation of radio resources.
  - The Network Management Segment consists of a single NMF designed to manage MUOS ground resources and allow for government-controlled, precedence-based communication planning.
  - The Ground Infrastructure Segment is designed to provide transport of both communications and command and control traffic between MUOS facilities and other communication facilities.
  - The Satellite Control Segment consists of MUOS telemetry, tracking, and commanding facilities at the Naval Satellite Operations Center Headquarters and Detachment Delta.
  - The User Entry Segment provides a MUOS waveform hosted on MUOS-compatible terminals. The Army's Project Manager for Tactical Radios is responsible for developing and fielding MUOS-compatible radios. The Air Force, Navy, and Marine Corps are upgrading legacy UHF radios to be MUOS-compatible.



Mission

Combatant Commanders and U.S. military forces deployed worldwide will use the MUOS satellite communications system to accomplish operational missions, especially those involving highly mobile users. Such missions include major conventional war; regional conflicts; search and rescue; humanitarian or disaster relief; homeland security; and homeland defense.

Major Contractors

- Lockheed Martin Space Systems – Sunnyvale, California
- General Dynamics C4 Systems – Scottsdale, Arizona

Activity

- The MUOS Program Office conducted five DTA events in 2018, with OPTEVFOR and DOT&E observing. The purpose of the DTA events were to demonstrate to the MUOS community that the program has resolved problems found in MOT&E-2 and to build confidence in the system's readiness to enter TECHEVAL-3.
- The MUOS Program Office conducted DTA One (DTA-1) from January 29 through February 2, 2018, at SMDC/ARSTRAT and at RSSC-West on Peterson AFB, Colorado. DTA-1 focused on demonstrating improvements made to the MUOS communications planning and provisioning capability.
- The Navy conducted DTA-2 from March 26 – 28, 2018, at the NMF in Wahiawa, Hawaii. The purpose of DTA-2 was to demonstrate the new Bulk Key-loading Management capability. The Navy designed the capability to provide NMF managers the ability to load several thousand cryptographic keys concurrently from a compact disk, where previously the operator would have to load each key individually.
- The Navy conducted DTA-3 from May 15 – 16, 2018, to demonstrate the Automated Monitoring System – Geolocation Service capability. SMDC/ARSTRAT personnel used this capability to estimate the geographic location of an unknown emitter.
- SMDC/ARSTRAT conducted an Operational Management Exercise from July 16 – 20, 2018, with geographically-dispersed RSSCs and the MUOS NMF managers in Wahiawa, Hawaii, to exercise and refine standard operating procedures for help desk operations and resolving system outages.
- The Navy conducted DTA-4 from July 30 through August 8, 2018, at the MUOS NMF and at the RSSC – Pacific in Hawaii to demonstrate improvements made to the system situational awareness and fault management capabilities.
- The Navy conducted DTA-5 from September 10 – 21, 2018, at the Hawaii ground facility to demonstrate improvements to their cybersecurity posture and readiness to conduct the Cooperative Vulnerability and Penetration Assessment (CVPA).
- The Navy plans to conduct the developmental test TECHEVAL-3 from November 26 through December 21,2018, followed by an Integrated Test period from January 7 through May 1, 2019, to demonstrate readiness to enter into FOT&E.
- OPTEVFOR plans to conduct the MUOS FOT&E from June 3 through August 15, 2019, with operational users from the Army, Navy, and Marine Corps. The Navy cyber team plans to conduct a CVPA in January 2019 and an Adversarial Assessment (AA) in June 2019.
- The Navy conducted all testing in accordance with the DOT&E-approved test plans.

Assessment

- The Navy completed DTA-1 as planned. The system demonstrated improved capabilities compared to the FY16 MOT&E-2. ARSTRAT operators were able to accomplish initial and group provisioning successfully; however, the operators had to sometimes retry provisioning steps due to unexplained application error messages, or screens not fully displaying or properly updating.
- The MUOS NMF managers executed DTA-2 events and performed bulk key management per the program manager's test plan until the NMF managers discovered that the cryptographic key authority had issued them an incorrect version of cryptographic key. Due to the incorrect cryptographic keys, the test was terminated. The incorrect keys prevented the Program Office from being able to validate the cryptographic keys could be correctly sent to and loaded on remote MUOS radios. While the system appeared to work correctly, DOT&E cannot verify it did so without the remote radios communicating with MUOS using the new keys. OPTEVFOR plans to collect additional data during the integrated and operational test periods. The new bulk key-loading capability should reduce the time to load cryptographic keys into the MUOS system from days to minutes.
- The SMDC/ARSTRAT operators successfully completed DTA-3 on May 16, 2018. The testers met all test objectives and used the system to measure geolocation accuracy and timeliness of the system in locating a variety of reference emitters.
- The Navy successfully completed DTA-4 on August 3, 2018. The MUOS NMF managers and RSSC planners were able to demonstrate situational awareness and fault management capability improvements.
- Based on the Operations Management Exercise results, ARSTRAT made significant progress revising their standard operating procedures for help desk operations and resolving system outages. The improvements should result in support that is more responsive to MUOS operational users.
- During DTA-5 the Navy demonstrated an improved cybersecurity posture. The MUOS Program Office is working to mitigate remaining vulnerabilities in preparation for additional cyber testing during FY19 TECHEVAL-3 and the FOT&E.
- OPTEVFOR is on track in their planning to conduct the FY19 operational test. DOT&E approved their test concept on October 3, 2018. OPTEVFOR is developing their operational test plan in preparation for DOT&E approval.

Recommendation

1. The Navy should fix or mitigate cyber vulnerabilities found during DTA-5 and the CVPA in preparation for the AA in 3QFY19.

MQ-4C Triton Unmanned Aircraft System

Executive Summary
The Navy updated and DOT&E approved the MQ-4C Triton Unmanned Aircraft System (UAS) Test and Evaluation Master Plan (TEMP) in January 2017 following instruction given in the August 2016 Milestone C Acquisition Decision Memorandum. The update reflects the alignment of the program's Acquisition Strategy with the development and fielding of the Multiple Intelligence (Multi-INT) configuration as the Initial Operational Capability (IOC).

System
- The MQ-4C Triton is an intelligence, surveillance, and reconnaissance (ISR) UAS consisting of the high-altitude, long-endurance MQ-4C air vehicle; sensor payloads; and supporting ground control stations. The MQ-4C system is a part of the Navy Maritime Patrol and Reconnaissance family of systems with capabilities designed to complement the P-8A Poseidon. It will provide ISR data on maritime and land targets over wide areas of the open ocean and littorals.
- The MQ-4C air vehicle design is based on the Air Force RQ-4B Global Hawk air vehicle with significant modifications that include strengthened wing structures and an anti-ice and de-icing system.
- The baseline configuration includes a maritime surveillance radar to detect, classify, and track surface targets; an electro-optical/infrared (EO/IR) full motion video sensor; electronic support measures to detect, identify, and geolocate threat radars; and an Automatic Identification System (AIS) receiver to collect AIS broadcasts from cooperative maritime vessels.
- The Multi-INT configuration provides a signals intelligence capability, and includes sensors, supporting software and hardware, and changes to permit processing of Top Secret and Sensitive Compartmented Information. The Navy intends for the MQ-4C Multi-INT configuration to replace the EP-3 Aries II aircraft for most missions.
- Onboard line-of-sight and beyond line-of-sight communications systems provide air vehicle command and control and transmit sensor data from the air vehicle to ground control stations for dissemination to fleet tactical operation centers and intelligence exploitation sites.
- Future system upgrades planned for after IOC include an air traffic collision avoidance radar system.

Mission
Commanders employ units equipped with MQ-4C to conduct long-endurance maritime surveillance operations and provide high- and medium-altitude intelligence collection.
- MQ-4C operators will detect, classify, identify, track, and assess maritime and littoral targets of interest and collect imagery and signals intelligence information.
- Operators disseminate sensor data to fleet units to support a wide range of maritime missions to include surface warfare, intelligence operations, strike warfare, maritime interdiction, amphibious warfare, homeland defense, and search and rescue.

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

Activity
- The Navy updated and DOT&E approved the MQ-4C TEMP in January 2017 following instruction given in the August 2016 Milestone C Acquisition Decision Memorandum. The update reflects the realignment of the program's Acquisition Strategy with the development and fielding of the Multi-INT configuration. As part of the realignment, the program has moved IOT&E from 4QFY17 to 2QFY21.
- The Navy is currently conducting an Operational Assessment (OA) of the baseline configuration to support early fielding of two aircraft. This Early Operational Capability (EOC) will allow the Navy to gain experience operating and maintaining the MQ-4C in a deployed environment. On September 12, 2018, aircraft #168461 executed a gear-up landing at Point Mugu, California, following an in-flight emergency. Mishap investigation is in progress.
- The Navy plans to conduct integrated testing of the MQ-4C Multi-INT configuration in FY20 to support an EOC of a limited number of Multi-INT aircraft.

Assessment

- In general, the system demonstrated positive trends for sensor performance and reliability during the FY16 OA supporting the Milestone C decision. However, the OA revealed deficiencies in the following areas: Due Regard capability (capability to independently maintain prescribed minimum separation distances); EO/IR sensor control; Electronic Support Measures interface; and managing the temperature of the radar. DOT&E's classified OA report, dated May 2016, provides specific information on these and other aspects of the assessment.
- The Due Regard capability provides critical mission capability for operation of the MQ-4C in civil and international airspace in support of global naval operations. Limitations to this capability at IOT&E may reduce the effectiveness of the MQ-4C.

Recommendations

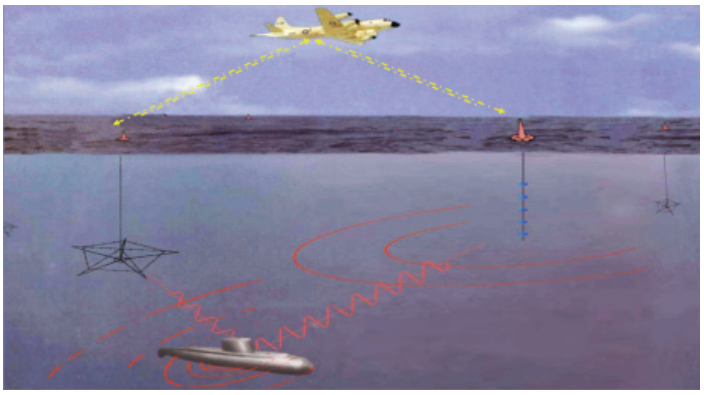
None. DOT&E may provide recommendations separately pending results of the mishap investigation.

Multi-Static Active Coherent (MAC) System

Executive Summary
The Navy continued FOT&E of the submarine search capability provided by the Engineering Change Proposal (ECP) 2 version of P-8A aircraft using Multi-Static Active Coherent (MAC). The Navy has now completed 11 of the 24 planned flights needed to complete the submarine search portion of the ECP 2 FOT&E. Analysis remains in progress and no preliminary assessment is available.

System
- The MAC system is an active sonar system composed of two types of sonobuoys (source and receiver) and an acoustic processing and aircraft mission computer software suite. It is employed by the Navy's maritime patrol aircraft (P-3Cs and P-8As) to search for and locate threat submarines in a variety of ocean conditions.
- Initial MAC capability (MAC Phase I) was delivered for P-3C aircraft in FY13 and for P-8A aircraft in FY15. MAC Phase II is expected to deliver in FY24.
- The P-8A aircraft delivers incremental improvements, including submarine search capability, in ECPs to the P-8A aircraft. ECP 2 of the P-8A aircraft included system software and display modifications to MAC Phase I.

Mission
The Navy intends for P-3C and P-8A crews equipped with MAC to support the search, detect, and localization phases of the ASW mission. MAC is particularly focused on large-area search for threat submarines.



Major Contractors
- Lockheed Martin – Manassas, Virginia
- Sparton Electronics Florida, Inc. – De Leon Springs, Florida
- Ultra Electronics, Undersea Sensor Systems Incorporated (USSI) – Columbia City, Indiana
- Boeing Defense, Space, and Security – St. Louis, Missouri

Activity
- In FY13, the Navy delivered initial MAC capability (MAC Phase I) for P-3C aircraft.
- In July 2014, DOT&E submitted a classified IOT&E report for MAC Phase I installed on P-3C Aircraft.
- In FY15, the Navy delivered initial MAC capability (MAC Phase I) for P-8A aircraft. The Navy modified MAC to operate with P-8A specific systems.
- In December 2015, DOT&E submitted a classified FOT&E report for MAC Phase I integration on P-8A aircraft.
- In FY16, the Navy delivered ECP 2 for P-8A aircraft. ECP 2 included MAC system software and display improvements specific to its use on P-8A aircraft.
- Between December 2016 and May 2017, the Navy completed 7 of 24 planned flights for FOT&E of the submarine search capability provided by the ECP 2 version of P-8A aircraft using MAC.
- In July 2018, the Navy continued FOT&E of the submarine search capability provided by the ECP 2 version of P-8A aircraft using MAC, completing an additional 4 of the 24 flights planned for this FOT&E. The Navy conducted the testing in accordance with DOT&E-approved test plans.

Assessment
Analysis is in progress for completed testing on the submarine search capability of the ECP 2 version of P-8A aircraft using MAC. No preliminary assessment is available.

Recommendation
1. The Navy should continue to pursue opportunities to complete FOT&E on the ECP 2 version of the P-8A aircraft using MAC as soon as feasible.

Offensive Anti-Surface Warfare (OASuW) Increment 1

Executive Summary
- The Navy completed a Quick Reaction Assessment (QRA) of the Offensive Anti-Surface Warfare (OASuW) Increment 1 program for weapon employment on the B-1B aircraft in FY18 and intends to complete a QRA for the F/A-18E/F aircraft in FY19.
- The OASuW Increment 1 program conducted limited testing in FY18 with partially successful results. Accrediting the modeling and simulation (M&S) environment to determine long-range anti-ship missile (LRASM) operational performance is at risk.
- During Integrated Test Events (ITEs) 1, 2/4, 3, 5, and 6B, the LRASM, employed from a B-1B aircraft, successfully engaged the mobile ship target with limitations.

System
- The OASuW Increment 1 program is the first program in an incremental approach to produce an OASuW capability in response to a U.S. Pacific Fleet Urgent Operational Need generated in 2008.
- The OASuW Increment 1 is an accelerated acquisition program to procure a limited number of air-launched missiles to meet a near-term U.S. Pacific Fleet capability gap in 2018 by leveraging the Defense Advanced Research Projects Agency (DARPA) LRASM.
- LRASM, the weapon system for the OASuW Increment 1, is a 2,400-pound, long-range, conventional, air-to-surface, precision standoff missile. The Navy's F/A-18E/F or the Air Force's B-1B aircraft will launch LRASM.
- LRASM, designated the AGM-158C, is derived from the Joint Air-to-Surface Standoff Missile Extended Range (JASSM-ER) and will use the same 1,000-pound penetrator/blast fragmentation warhead. An anti-jam GPS guidance system, radio frequency sensor (RFS), and an infrared sensor support guidance and targeting.
- Once launched against a target ship, LRASM guides to an initial point and employs onboard sensors to locate, identify, and provide terminal guidance to the selected aimpoint on the target. LRASM is designed to operate individually or as part of a salvo.
- OASuW Increment 2 is required to deliver the long-term, air-launched anti-surface warfare (ASuW) capabilities to counter 2028 threats (and beyond). The Department continues to plan for OASuW Increment 2 to be developed via full and open competition. To inform the long-term path forward, the Navy will leverage Next Generation Land Attack Weapon (NGLAW) Analysis of Alternatives results to inform the required ASuW capabilities. Due to Increment 2 budget marks, the Navy planned an incremental upgrade to LRASM to bridge the gap until an OASuW Increment 2 program of record can be established. Increment 2 Initial Operational Capability is now planned for the FY28-30 timeframe.

Mission
Combatant Commanders will use units equipped with LRASM to destroy high-value, well-defended ships from standoff ranges.

Major Contractor
Lockheed Martin Missiles and Fire Control – Orlando, Florida

Activity
- The Navy and Air Force conducted testing in FY18 in accordance with the DOT&E-approved Master Test Strategy and QRA test plan.
- The Navy and Air Force conducted flight testing and end-to-end M&S runs of the LRASM system in FY18.
- The Navy and Air Force conducted six free-flight test events of LRASM, four flights with a single missile, and two flights with two-missile salvos launched from a B-1B. Flight testing for the QRA on F/A-18E/F aircraft will continue into FY19.
- The Navy completed Integrated Test Event for M&S 3 (ITEM 3) in August 2018, which is the QRA run-for-record M&S test using the Kill Chain Testbed (KCT).
- The Navy began developmental cybersecurity testing in July 2018. Additional developmental cyber testing will occur in FY19 with updated LRASM hardware and software after an update to the Signal Processor-In-the-Loop (SPIL) simulation environment has been completed.

- The Air Force and Navy completed captive carry events on a B-1B and F/A-18 aircraft to evaluate weapon integration in FY18.
- In FY16, the Navy completed the sled tests to demonstrate warhead fuze functionality of the weapon against intended ship targets. Analysis to characterize the lethal effects on the target as a function of weapon hit location was completed in FY18 using the Advanced Survivability Assessment Program. These damage predictions were then used by the KCT to evaluate damage from specific, operationally representative, weapon engagements.
- The Navy completed a QRA of the OASuW Increment 1 program and declared Early Operational Capability (EOC) for weapon employment on the B-1B aircraft in October 2018 and plan to do the same for the F/A-18E/F aircraft in FY19. DOT&E delivered an Early Fielding Report on the B-1B EOC decision in September 2018, and intends to do the same for the F/A-18E/F in FY19.
- The Navy started planning in August 2018 for a future IOT&E of a Lot 4-configured LRASM.

Assessment

- The OASuW Increment 1 program conducted limited testing in FY18, including ITEs with the B-1B and developmental cybersecurity testing in the SPIL simulation environment, with partially successful results.
- Lethality evaluation of the LRASM has been completed and summarized in the classified Quick Reaction Assessment Early Fielding Report, published by DOT&E in September 2018.
- Accrediting the M&S environment to determine LRASM operational performance is at risk due to difficulties in correctly modeling RFS performance and lack of validated models. The M&S environment is required to validate Key Performance Parameter achievement in this program. Further details are classified.
- The OASuW Increment 1 program continued development of missile software based on lessons learned from ITEs with B-1B aircraft, and plans further software development for ITEs with the F/A-18E/F.
- Developmental cybersecurity testing revealed areas for improvement.

Recommendations

The Navy should:

1. Accomplish cybersecurity testing of the weapon system in accordance with a DOT&E-approved cybersecurity test plan.
2. Complete remaining ITEs with operationally representative hardware and software configurations.
3. Plan and complete IOT&E for LRASM in accordance with FY19 congressional direction.

P-8A Poseidon Multi-Mission Maritime Aircraft (MMA)

Executive Summary

- The P-8A Engineering Change Proposal (ECP) 2 upgrade provides new and operationally effective capabilities including P-8A receiver air refueling, AGM-84D Harpoon Block 1 advanced employment modes, and multiple communication system upgrades. Despite significant efforts to improve P-8A intelligence, surveillance, and reconnaissance (ISR) sensors, overall P-8A ISR mission capabilities remain limited by sensor performance shortfalls.
- P-8A operational suitability has declined since initial fielding in 2013. P-8A ECP 2 OT&E data and fleet-reported metrics show consistently negative trends in fleet-wide aircraft operational availability due to a shortage of critical spare parts and increased maintenance requirements. Despite negative fleet availability and reliability trends, forward-deployed P-8A units currently report relatively high mission capable rates when sufficient spare parts, expedited logistics supply support, and priority maintenance support are available. However, prioritizing support for forward-deployed units frequently reduces aircraft availability and increases part cannibalization rates at other fleet operating locations.
- The Navy plans to incrementally improve baseline P-8A capabilities by integrating the Advanced Airborne Sensor (AAS), AGM-84 Harpoon Block II+, and High Altitude ASW Weapon Capability (HAAWC) MK 54 torpedo.

System

- The P-8A Poseidon Multi-mission Maritime Aircraft (MMA) design is based on the Boeing 737-800 aircraft with modifications to support Navy maritime patrol mission requirements. It is replacing the P-3C Orion.
- The P-8A incorporates an integrated sensor suite that includes radar, electro-optical, and electronic signal detection sensors to provide search, detection, location, tracking, and targeting capability against surface targets. An integrated acoustic sonobuoy launch and monitoring system provides search, detection, location, tracking, and targeting capability against submarine targets. Sensor systems also provide tactical situational awareness information for dissemination to fleet forces and ISR information for exploitation by the joint intelligence community. The P-8A carries MK 54 torpedoes and the AGM-84D Block 1C Harpoon anti-ship missile system to engage submarine and maritime surface targets.
- The P-8A aircraft incorporates aircraft survivability enhancement and vulnerability reduction systems. An integrated infrared missile detection system, flare dispenser, and directed infrared countermeasure system is designed to improve survivability against infrared missile threats. On- and off-board sensors and data transfer systems provide tactical situational awareness. Fuel tank protection and fire suppression systems reduce aircraft damage vulnerability.
- Incremental future upgrades include the addition of the HAAWC MK 54 torpedo, AAS radar, AGM 84 Harpoon II+ anti-ship missile, ASW signals intelligence sensors, and avionics architecture improvements.

Mission

- Theater Commanders primarily use units equipped with the P-8A MMA to conduct ASW operations including the detection, localization, tracking, and destruction of submarine targets.
- Additional P-8A maritime patrol missions include:
  - SUW operations to detect, identify, track, and destroy enemy surface combatants or other maritime targets
  - ISR operations to collect and disseminate imagery and signals information for exploitation by the joint intelligence community
  - Command, control, and communication (C3) operations to collect and disseminate tactical situation information to fleet forces
  - Identification and precise geolocation of targets ashore to support fleet strike warfare missions

Major Contractor

Boeing Defense, Space, and Security – St. Louis, Missouri

Activity

- The Navy Operational Test and Evaluation Force (OPTEVFOR) completed P-8A ECP 2 OT&E flight events in December 2017 and operational suitability data collection in May 2018. This testing included evaluation of initial P-8A air-to-air receiver refueling capabilities, ISR mission system improvements, advanced AGM-84 Block 1C Harpoon missile employment modes, communication system enhancements, and corrective actions for additional deficiencies identified during previous test periods. The Navy also conducted a system-level cybersecurity assessment and a complete re-evaluation of P-8A fleet availability, reliability, and maintainability. The P-8A ECP 2 OT&E was conducted in accordance with a DOT&E-approved test plan.
- The Navy did not complete the planned Multi-Static Active Coherent (MAC) wide area ASW search sensor testing during the ECP 2 OT&E period due to submarine target unavailability. As a result, OPTEVFOR submitted a separate operational test plan to complete remaining MAC ASW test events during future operational test periods.
- The Navy continues to plan and progressively execute an incremental series of ECPs and associated follow-on test events to improve baseline P-8A aircraft capabilities. In addition, the P-8A program is coordinating with other Navy weapon and sensor programs to integrate new capabilities. The Navy plans to conduct operational test events for the AAS, AGM-84 Harpoon Block II+, and HAAWC MK 54 torpedo in the FY19 through FY20 timeframe.
- Upon completion of the P-8A ECP 2 OT&E period, DOT&E issued a P-8A ECP 2 FOT&E Report in August 2018 and removed the P-8A aircraft from formal operational test oversight. DOT&E will continue to oversee major P-8A capability upgrades through operational test oversight for the separate AAS, MAC, and HAAWC sensor and weapon upgrade programs.

Assessment

- The P-8A ECP 2 upgrade provides new and operationally effective capabilities including P-8A receiver air refueling, AGM-84D Harpoon Block 1 advanced employment modes, and multiple communication system upgrades. The associated Operational Flight Program Fleet Release 40.2 software also includes effective corrections for 28 previously identified system performance deficiencies. Despite significant efforts to improve P-8A ISR sensors, overall P-8A ISR mission capabilities remain limited by persistent performance shortfalls.
- P-8A ECP 2 cybersecurity testing identified five priority areas for improvement. The ECP 2 operational test report includes specific test results and recommendations to improve the cybersecurity posture.
- P-8A operational suitability has declined since initial fielding in 2013. P-8A ECP 2 OT&E data and fleet-reported metrics show consistently negative trends in fleet-wide aircraft operational availability due to a shortage of spare parts and increased maintenance requirements. Despite these negative trends, forward-deployed P-8A units currently report relatively high mission capable rates when sufficient spare parts, expedited logistics supply support, and priority maintenance support are available. However, prioritizing support for forward-deployed units frequently reduces aircraft availability and increases part cannibalization rates at other fleet operating locations.
- Supply support system spare part contracting and delivery delays also exacerbate the impact of current mission critical spare part shortages. Navy Supply Systems Command reliance on engineering model predictions, instead of actual fleet reliability data, ensures that some mission critical spare part contracts lag actual fleet needs. This lag time further extends the already lengthy 6 to 9 month contracting process for repairable spare parts. These delays are a major contributing factor to the observed increases in aircraft downtime awaiting parts and higher part cannibalization rates. Defense Logistics Agency consumable item procurement processes also lag actual fleet needs by requiring stock depletion and backorders before initiating procurement actions. The P-8A program is currently working with Naval Supply Systems Command to implement a more flexible and proactive parts contracting strategy and, to transition to use of fleet reliability data as the basis for advance parts procurement.

Recommendations

The Navy should:

1. Continue planning and execution of MAC, AAS, and HAAWC MK 54 operational testing to demonstrate and characterize improved P-8A operational capabilities.
2. Continue efforts to correct remaining P-8A aircraft and mission system shortfalls and deficiencies identified in P-8A ECP 2 OT&E and previous operational test periods.

Rolling Airframe Missile (RAM) Block 2

Executive Summary

- The Navy's Operational Test and Evaluation Force (OPTEVFOR) completed the final IOT&E phase for the Rolling Airframe Missile (RAM) Block 2 program in March 2018 in accordance with a DOT&E-approved test plan. Testing consisted of conducting RAM Block 2 Probability of Raid Annihilation (PRA) Modeling and Simulation Test Bed runs to gather RAM Block 2 operational effectiveness data.
- DOT&E published a classified IOT&E report in September 2018. The report states that RAM Block 2 is operationally effective and suitable.

System

- The RAM, jointly developed by the United States and the Federal Republic of Germany, provides a short-range, lightweight self-defense system to defeat anti-ship cruise missiles (ASCMs). There are three RAM variants:
  - RAM Block 0 uses dual mode, passive radio frequency/infrared guidance to home in on ASCMs.
  - RAM Block 1/1A adds infrared guidance improvements to extend defenses against ASCMs that do not radiate radio frequencies.
  - RAM Block 2 incorporates changes to improve its kinematic capability and capability to guide on certain types of ASCM radio frequency threat emitters in order to defeat newer classes of ASCM threats. The warhead in Block 2 is the same as in Blocks 1 and 1A. A significant RAM Block 2 upgrade, the RAM Block 2B, is under development.
- The Navy can launch RAM Block 2 from the 21-round RAM Guided Missile Launch System resident on *San Antonio*-class amphibious transport dock ships, *America*-class amphibious assault ships, *Whidbey Island*-class and *Harpers Ferry*-class dock landing ships, *Freedom*-class littoral combat ships, and *Nimitz*-class aircraft carriers.

- RAM Block 2 is also launched from the SeaRAM standalone self-defense system, which is composed of the Close-In Weapon System radar/electronic warfare sensor suite and command/decision capability combined with an 11-round missile launcher. The SeaRAM system is resident on selected *Arleigh Burke*-class Aegis destroyers and the *Independence*-class littoral combat ships.

Mission

Commanders employ naval surface forces equipped with RAM to provide a defensive short-range, hard-kill engagement capability against ASCM threats.

Major Contractors

- Raytheon Missiles Systems – Tucson, Arizona
- RAMSys – Ottobrunn, Germany

Activity

- OPTEVFOR completed the final IOT&E phase for the RAM Block 2 program in March 2018 in accordance with a DOT&E-approved test plan. Testing consisted of conducting RAM Block 2 PRA Modeling and Simulation Test Bed runs to gather RAM Block 2 operational effectiveness data.
- DOT&E published a classified IOT&E report in September 2018.
- The Navy did not test RAM Block 2 cybersecurity during IOT&E due to a lack of test resources.

Assessment

- RAM Block 2 is operationally effective and suitable.
- Further details are contained in the classified September 2018 DOT&E IOT&E report.

Recommendations

The Navy should:

1. Resource and conduct FOT&E of RAM Block 2 cybersecurity as soon as possible.
2. Conduct FOT&E of the RAM Block 2B upgrade prior to fleet use.

SSN 774 *Virginia*-Class Submarine

Executive Summary

- The Navy completed FOT&E on the *Virginia*-class Block III submarine. FOT&E focused on testing significant modifications from Block I to Block III, specifically the replacement of a legacy submarine spherical array with a Large Aperture Bow (LAB) array and the replacement of 12 vertical launch tubes with 2 large diameter *Virginia* Payload Tubes (VPTs). The Navy tested the *Virginia*-class Block III submarine in anti-submarine, anti-surface, and strike warfare, and situational awareness in areas with significant shipping activity.
- DOT&E will submit a classified FOT&E report in 2QFY19. Based on preliminary assessment, the primary modifications (LAB array and two VPTs) are effective replacements to their legacy components in the *Virginia*-class Block I submarine. *Virginia*-class Block III is operationally effective and operationally suitable for the primary missions affected by these modifications, specifically anti-submarine and strike warfare.

System

- The *Virginia*-class submarine is the Navy's latest fast-attack submarine and is capable of targeting, controlling, and launching MK 48 torpedoes and Tomahawk land-attack missiles (TLAMs).
- The Navy is procuring *Virginia*-class submarines incrementally in a series of blocks; the block strategy is for contracting purposes, not necessarily to support upgrading capabilities.
  - Block I (hulls 1-4) and Block II (hulls 5-10) ships were built to the initial design of the *Virginia*-class.
  - Block III (hulls 11-18) and Block IV (hulls 19-28) ships, starting with SSN 784, include the following affordability enhancements:
    - A LAB array in place of the spherical array in the front of the ship
    - Two large diameter VPTs replace the 12 vertical launch tubes; each payload tube is capable of storing and launching 6 TLAMs used in strike warfare missions
  - Block V and beyond will increase strike payload capacity from 12 to 40 TLAMs by adding a set of 4 additional VPTs in an amidships payload module, capable of storing and launching 7 TLAMs each, as well as providing the potential to host future weapons and unmanned systems.

Mission

The Operational Commander will employ the *Virginia*-class Block III submarine to conduct open-ocean and littoral covert operations that support the following submarine mission areas:

- Strike warfare
- Anti-submarine warfare
- Intelligence, surveillance, and reconnaissance
- Mine warfare
- Anti-surface warfare
- Naval special warfare
- Battle group operations

Major Contractors

- General Dynamics Electric Boat – Groton, Connecticut
- Huntington Ingalls Industries, Newport News Shipbuilding – Newport News, Virginia

Activity

- In September 2015, DOT&E submitted a classified Early Fielding Report on the first *Virginia*-class Block III submarine due to Block III submarine deployment prior to the completion of operational testing.
- In December 2017, the Navy completed FOT&E of the *Virginia*-class Block III submarine. The Navy completed FOT&E events in accordance with DOT&E-approved test plans. The *Virginia*-class Block III submarine employed the Advanced Processing Build (APB-09) software version of the submarine sonar system and the submarine combat system. FOT&E events tested the following capabilities.
  - Anti-submarine warfare against a high-end nuclear submarine
  - Surface warfare, including torpedo employment
  - Strike warfare capabilities, including operator employment of TLAMs using a new common weapon launcher and a

demonstration of two TLAMs (without warheads) fired from the new VPTs
  - Submarine mobility to include the crew's ability to maintain situational awareness in the presence of significant shipping activity
  - Cybersecurity
- The Navy concluded FOT&E on *Virginia*-class Block III with insufficient data collected on the anti-surface warfare mission. The Navy collected data; however, post-test evaluation determined the data were not valid for assessment. The Navy determined that the limited impact of Block III modifications on submarine capability to support this mission did not warrant extending the FOT&E to collect additional data.
- The Navy completed development of a *Virginia*-class Block V submarine Test and Evaluation Master Plan, which is in formal routing for approval.
- The Navy issued the *Virginia*-class Block III Vulnerability Assessment Report (VAR) supplement for Block III.
- The Navy issued the VPT Shock Test Report. Based on the VPT shock tests, completed in 2014, Electric Boat requested the shock qualification of hatch components. The Navy is evaluating the request.

Assessment

- DOT&E will submit an FOT&E report on the *Virginia*-class Block III submarine in 2QFY19. The preliminary analyses indicate the following:
  - *Virginia*-class Block III submarine is operationally effective for anti-submarine warfare. The LAB array is an effective replacement for the legacy spherical array. The *Virginia*-class Block III submarine capability against diesel submarines remains unknown because submarine acoustic security restricts operational testing against real-world diesel submarines. Further, the absence of a mobile set-to-hit target limits the Navy's evaluation of submarine torpedo performance.
  - *Virginia*-class Block III submarine is operationally effective for strike warfare. Two VPTs are an effective replacement for 12 legacy vertical launch tubes.
  - *Virginia*-class Block III submarine did not meet Navy requirements for situational awareness in the presence of significant shipping activity. This capability of *Virginia*-class Block III submarine is highly dependent upon the submarine sonar system and the submarine combat system, which have undergone three increments of improvement from the APB-09 variants employed in the *Virginia*-class Block III submarine test. Operational testing of APB-15 software of these tactical systems in FY19 will directly inform *Virginia*-class Block III submarine capability to support situational awareness upon scheduled upgrades.
  - *Virginia*-class Block III submarine is operationally suitable with no significant deficiencies identified with operational availability or reliability.
  - Analysis of the *Virginia*-class Block III VAR supplement identify that the modifications from Block I to Block III do not degrade the *Virginia*-class submarine's ability to support fleet missions.
- DOT&E intends to provide cybersecurity results that affect operational effectiveness in the classified FOT&E report.
- The Navy's decision to conclude FOT&E on *Virginia*-class Block III submarine is appropriate. The Navy completed adequate testing on the primary missions impacted by the significant modifications between Block I and Block III of the *Virginia*-class submarines. The *Virginia*-class Block III submarine derives its mission capability in anti-surface warfare primarily from the submarine sonar system, the submarine combat system, and the submarine torpedoes. The Navy intends these supporting systems to undergo periodic improvement on a 2- to 3-year cycle, and each system has a formal operational test program. DOT&E will evaluate anti-surface warfare capability of the *Virginia*-class Block III submarine through the test programs of these supporting systems.

Recommendations

The Navy should:

1. Monitor *Virginia*-class Block III submarine capability to support anti-surface warfare during the test programs associated with the submarine sonar system, the submarine combat system, and submarine torpedo improvement.
2. Monitor *Virginia*-class Block III submarine capability to support situational awareness in environments with significant shipping activity during the test programs associated with submarine sonar and submarine combat system improvement.

Standard Missile (SM)-6

Executive Summary
- Standard Missile (SM)-6 Block I (BLK I) has attained Full Operational Capability; Initial Operational Capability for SM-6 BLK IA is expected in FY19.
- In FY18, the Navy completed SM-6 BLK I FOT&E testing that satisfactorily demonstrated interoperability with the Aegis Baseline 9 combat system and Integrated Fire Control capability. At the conclusion of FOT&E, SM-6 BLK I remains effective and suitable.
- Deficiencies identified in the classified May 2013 IOT&E report remain unresolved. Verification of Corrected Deficiency (VCD) events demonstrated that the software correction mitigated the effects of the deficiency but did not eliminate it. The VCD testing identified two new concerns that contributed to the deficiency not being completely eliminated:
  - A classified concern with the missile Target Detection Device
  - A classified concern with the missile active seeker
- The Navy completed live-fire operational testing of SM-6 BLK IA. The SM-6 BLK IA testing consisted of SM-6 BLK IA firings against subsonic and supersonic aerial targets and modeling and simulation (M&S) runs for the record. DOT&E will issue an FOT&E report covering this testing in FY19.

System
- SM-6 BLK I and BLK IA are the latest evolution of the Standard Missile family of fleet air defense missiles.
- The Navy employs the SM-6 from Aegis-equipped cruisers and destroyers (i.e., *Ticonderoga*-class cruisers and *Arleigh Burke*-class destroyers).
- The SM-6 seeker and terminal guidance electronics derive from technology developed in the Advanced Medium-Range Air-to-Air Missile program.
- SM-6 retains the legacy Standard Missile semi-active radar homing capability.
- SM-6 receives midcourse flight control from the Aegis Weapon System (AWS) via ship's radar; terminal flight control is autonomous via the missile's active seeker or supported by the AWS via the ship's illuminator.
- The SM-6 BLK IA provides improved performance against advanced threats.
- SM-6 Dual I capability is fielded and provides Sea-Based Terminal Ballistic Missile Defense (BMD) capability against short-range ballistic missiles.

- The Navy upgraded the SM-6 to add an anti-surface target capability but it has not yet operationally tested the capability.

Mission
- The Joint Force Commander/Strike Group Commander will employ naval units equipped with the SM-6:
  - For air defense against fixed-/rotary-winged targets and anti-ship missiles operating at altitudes ranging from very high to sea-skimming
  - As part of the Navy Integrated Fire Control – Counter Air From the Sea (NIFC-CA FTS) operational concept to provide extended range over-the-horizon capability against at-sea and overland threats
  - As part of the mission expansion upgrade to provide extended-range capability against surface targets
- The Joint Force Commander/Strike Group Commander will use SM-6 Dual I to provide Sea-Based Terminal capability against short- and medium-range ballistic missiles in their terminal phase of flight, anti-ship cruise missiles, and all types of aircraft.

Major Contractor
Raytheon Missile Systems – Tucson, Arizona

Activity

- In FY18, the Navy conducted multiple phases of test for SM-6 in accordance with the DOT&E-approved test plans.

SM-6 BLK I M&S FOT&E

- The Navy completed SM-6 BLK I M&S FOT&E in December 2017. These runs demonstrated SM-6 BLK I compatibility with the Aegis Baseline 9 combat system.
- DOT&E published an FOT&E report in FY18 addressing all SM-6 BLK I live fire tests and M&S tests. This report focused on SM-6 BLK I performance when employed from Aegis Baseline 9 ships.
- The Navy declared SM-6 BLK I Full Operational Capability in December 2017.

SM-6 BLK IA Operational Testing

- The focus of SM-6 BLK IA was to demonstrate compatibility with the Aegis Baseline 9 combat system during the FOT&E.
- In August 2018, the Navy successfully completed live fire operational testing of the SM-6 BLK IA.
- The four phases of testing occurred at Point Mugu Sea Range, California, from September 2017 to August 2018 and consisted of SM-6 BLK IA firings against subsonic and supersonic aerial targets.

SM-6 BLK IA M&S FOT&E

- The Navy plans to commence SM-6 BLK IA M&S FOT&E in FY19.
- DOT&E will publish an SM-6 BLK IA FOT&E report once SM-6 BLK IA M&S is completed.

Naval Integrated Fire Control-Counter Air from the Sea

- The Navy conducted NIFC-CA FTS At-Sea-04 (AS-04) at the Point Mugu Sea Range in July 2018. This test employed a single SM-6 BLK I.

Assessment

- As reported in the DOT&E FY18 SM-6 BLK I FOT&E Report, the SM-6 remains effective and suitable with the exception of the classified deficiency identified in the FY13 IOT&E Report. The SM-6 Block 1 satisfactorily demonstrated compatibility with Aegis Weapon System Baseline 9 Integrated Fire Control capability.
- In FY17-18, the Navy developed and tested specific software improvements to SM-6 BLK I to mitigate the classified performance problems discovered during IOT&E. As previously reported, testing conducted by the Navy demonstrated the software improvements perform as intended, but did not eliminate them.

Recommendation

1. The Navy should continue to improve software based on IOT&E results and verify corrective actions with flight tests.

Surface Ship Torpedo Defense (SSTD) System: Torpedo Warning System (TWS) and Countermeasure Anti-Torpedo (CAT)

Executive Summary

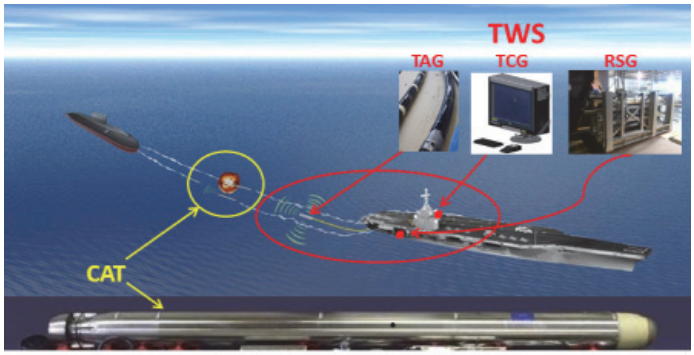
- In April 2018, DOT&E submitted a third update to the 2015 Early Fielding Report on the Surface Ship Torpedo Defense (SSTD) system. The classified update provides an assessment based on a Quick Reaction Assessment (QRA) conducted by the Navy Operational Test and Evaluation Force (OPTEVFOR) and system-level contractor testing. Insufficient data were available to assess operational effectiveness and operational suitability; however, significant observations include:
  - Qualified sailors with the support of contractors used the Torpedo Warning System (TWS) to successfully alert on inbound torpedoes.
  - Countermeasure Anti-Torpedo (CAT) demonstrated some capability to defeat an incoming torpedo.
  - Towed Active Acoustic Source (TAAS) reliability is improved.
  - CAT reliability is uncertain.
- In September 2018, the Navy suspended its effort to develop the SSTD system. The Navy plans to restore all carriers to their normal configurations during maintenance availabilities between FY19 and FY23. DOT&E removed the SSTD system from DOT&E oversight.

System

- SSTD is a system of systems that includes TWS and CAT. Combined, TWS and CAT are referred to as the Anti-Torpedo Torpedo Defensive System (ATTDS).
- TWS is being built as an early warning system to detect, localize, classify, and alert on incoming threat torpedoes.
- CAT is a hard-kill countermeasure intended to neutralize threat torpedoes.

Mission

Commanders of nuclear-powered aircraft carriers and Combat Logistic Force ships will use the SSTD system to defend against incoming threat torpedoes.



Major Contractors

TWS

- Ultra Electronics 3 Phoenix (Prime Contractor) – Chantilly, Virginia, and Wake Forest, North Carolina
- Alion Science and Technology (Acoustics and testing consultant) – New London, Connecticut
- In-Depth Engineering (Tactical Control Group software development) – Fairfax, Virginia
- Pacific Engineering Inc. (Ready Stow Group manufacture) – Lincoln, Nebraska
- Rolls-Royce (Winch manufacture) – Ontario, Canada
- Teledyne (Towed Array manufacture and assembly) – Houston, Texas

CAT

- Pennsylvania State University Applied Research Laboratory (ATT Systems) – State College, Pennsylvania
- Pacific Engineering Inc. (Canister fabrication) – Lincoln, Nebraska
- SeaCorp (All Up Round Equipment fabrication and assembly) – Middletown, Rhode Island

Activity

- In October 2017, OPTEVFOR conducted a third QRA in conjunction with system-level contractor testing. Because of reliability problems with test target surrogates, test equipment, and CAT hardware, the Navy did not execute the test scenarios per the contractor test plans or the DOT&E-approved test plans. The Navy completed two salvo events (a salvo is two torpedoes launched near simultaneously at the test ship) and one single incoming torpedo event during the QRA. The contractor completed five TWS detection events and one salvo event.

- In April 2018, DOT&E issued a classified update to the Early Fielding Report. This update includes analysis of data collected during the October 2017 QRA and contractor testing.
- In September 2018, the Navy suspended its efforts to develop the SSTD system. The Navy plans to restore all carriers to their normal configurations during maintenance availabilities between FY19 and FY23. DOT&E removed the SSTD system from DOT&E oversight.

Assessment

The April 2018 QRA and contractor testing demonstrated that the TWS and CAT contractors made progress towards developing capability that meets the systems operational requirements. The DOT&E classified update provides detailed analysis. Significant observations include:

- Test data were insufficient to assess operational effectiveness and operational suitability of TWS and CAT.
- Operators with contractor support used TWS to successfully alert on inbound torpedoes during simple and structured scenarios. However, additional data are required to characterize capability within the envelope of relevant environments, operating profiles of the supported platforms, and employment tactics of threat torpedoes.
- TWS demonstrated some capability to detect incoming torpedoes. The significance and effect of false target alerts on TWS capability are unknown.
- CAT demonstrated some capability to defeat an incoming torpedo.
- CAT has uncertain reliability.
- The lethality of CAT is untested.

Recommendations

None.

VH-92A Presidential Helicopter Fleet Replacement Program

Executive Summary

- The VH-92A program is progressing on schedule with excellent teamwork and open communication among all agencies involved.
- The Navy has modified two Sikorsky S-92A helicopters to produce two VH-92A Engineering Development Model (EDM) aircraft. The first aircraft has entered government-led integrated testing at Naval Air Station Patuxent River, Maryland, with the second to follow in December 2018.
- This effort includes the integration of the Mission Communications System (MCS) designed by Naval Air Systems Command (NAVAIR) at St. Inigoes, Maryland. MCS software development is progressing on schedule.
- The Navy started integrated flight testing at Patuxent River in August 2018. It will be followed by an operational assessment (OA) planned for 2QFY19 to support a Milestone C decision in 3QFY19. Preparations for the OA are on schedule; DOT&E approved the OA test plan on June 21, 2018.
- The program is making changes to the MCS design due to a late change in security protocols levied by the Defense Information Systems Agency (DISA) after the MCS design was finalized. The program is pursuing several solutions in parallel with a short-term workaround in place.
- In FY18, the VH-92 program completed live fire testing in accordance with DOT&E-approved test plans. Data analysis is ongoing and will be finalized in FY19.

System

- The VH-92A is a dual-piloted, twin-engine helicopter based on the Sikorsky S-92A. The program will maintain the VH-92A Federal Aviation Administration (FAA) airworthiness certification throughout its lifecycle.
- The VH-92A aircraft will replace the current Marine Corps fleet of VH-3D and VH-60N helicopters flown by Marine Helicopter Squadron One (HMX-1) to perform the presidential airlift mission.
- The VH-92A is capable of operating worldwide in day, night, or adverse weather conditions. The VH-92A will be air-transportable to remote locations via a single Air Force C-17 cargo aircraft.
- The government-designed MCS will provide the ability to conduct simultaneous short- and long-range secure and non-secure voice and data communications. The MCS will provide situational awareness by exchanging information with outside agencies, organizations, and supporting aircraft. The MCS hardware will be installed into the VH-92A at Sikorsky Aircraft in Stratford, Connecticut. Software will then be loaded and checked out by Lockheed Martin in Owego, New York.
- Final interior finishing and aircraft painting will be done at Owego to complete the VH-92A for delivery.

Mission

- The VH-92A aircraft will enable HMX-1 to provide safe and timely transport of the President of the United States and other parties as directed by the White House Military Office.
- The VH-92A shall operate from commercial airports, military airfields, Navy ships, and austere sites throughout the world.

Major Contractor

Sikorsky Aircraft, a Lockheed Martin subsidiary company – Stratford, Connecticut

Activity

- EDM 1 achieved its first flight at the Sikorsky facility in Stratford, Connecticut, on July 28, 2017. After modifications at the Lockheed Martin facility at Owego, New York, it arrived at Patuxent River on August 2, 2018, to begin government-led, integrated developmental/operational testing.
- EDM-2 is in contractor testing at Owego after achieving its first flight at Stratford on November 16, 2017, and modifications at Owego. It is expected to deliver to Patuxent River in December 2018 to join the test program.

- NAVAIR at St. Inigoes, Maryland, is continuing development of the MCS software. Systems integration laboratories, which replicate the MCS for development, test, and training, are operational and MCS software development is on schedule.
- Sikorsky installed the MCS hardware as part of the VH-92A modifications and Lockheed Martin installed early builds of the MCS software into the EDMs at Owego.
- On September 22, 2018, aircrew from the HMX-1 VH-92A Operational Test Team conducted 14 landings on the White House South Lawn. HMX-1 will use observations from these landings to inform the OA in March 2019.
- The Navy has begun the first phase of integrated developmental/operational testing for 150 flight hours at Patuxent River, Maryland. The testing will include loading a VH-92A onto a C-17 to simulate a long-distance deployment.
- The program is preparing for the VH-92A OA, which is forecast to begin in 2QFY19 to support a Milestone C decision in 3QFY19. It includes HMX-1 aircrews, and 30 flight hours over 30 days utilizing two VH-92A EDM aircraft. This assessment will exercise all Presidential airlift missions at actual mission sites with personnel participating from all agencies that support the White House. The OA has planned scenarios that include both VH-92A cabin configurations. DOT&E approved the OA test plan on June 21, 2018.
- Due to a change in security protocols after the MCS design was finalized, the program is making changes to the MCS that will enable it to connect to the Crisis Management System (CMS). A near-term workaround is in place to support the OA, and a permanent solution is in work.
- In FY18, the VH-92 program completed the planned live fire testing in accordance with DOT&E-approved test plans.

Assessment

- The program is on track to meet program milestones. Maintenance of FAA airworthiness certification is a key emphasis area.
- The program is working to resolve a risk to meeting the Net Ready Key Performance Parameter for the MCS to connect to the CMS. Security protocol changes enacted after MCS design finalization have required development of a near-term solution to support the OA in parallel with a permanent solution to support the IOT&E.
- Live fire test data analysis is ongoing and the vulnerability evaluation of the VH-92A against operationally realistic threats is expected to be completed in FY19.

Recommendation

1. The program should continue current efforts to develop and implement solutions to enable connection to the CMS.

Air Force Programs

Air Force Programs

AC-130J Ghostrider

Executive Summary

- DOT&E published a classified IOT&E and LFT&E Report on the Block 20 AC-130J on April 25, 2018, that found the Block 20 AC-130J operationally effective and suitable for most of its Close Air Support and Air Interdiction missions. Survivability analyses did not reveal any unexpected vulnerabilities to operationally significant kinetic threats, as compared to legacy C-130 aircraft.
- The AC-130J Combined Test Force (CTF) and 18th Flight Test Squadron (FLTS) are testing an interim "Block 20+" configuration to support U.S. Special Operations Command (USSOCOM) fielding and deployment.
- Preliminary test data indicate that gun weapon system and software updates have improved gun calibration and mission effectiveness over the Block 20 configuration.
- The CTF conducted early technology demonstrations of two potential All-Weather Engagement (AWE) systems to provide the AC-130J the capability to employ its gun weapon system through cloud layers. Assessments of additional technologies for a future acquisition strategy will occur in 2QFY19. The program has not established a timeline for system selection or fielding.

System

- The AC-130J is a medium-sized, multi-engine tactical aircraft with a variety of sensors and weapons for air-to-ground attack that will replace the AC-130H/U aircraft.
- The AC-130J is operated by nine aircrew members: two pilots, one Combat System Officer (CSO), one weapons system operator, and five special mission aviators (one sensor operator, one load master, and three gunners).
- USSOCOM is developing AC-130J through the integration of modular components onto existing MC-130J aircraft. The AC-130J includes an open architecture to allow for follow-on development and future integration of block capabilities.
- The AC-130J retains all survivability enhancement features on the MC-130J aircraft.
- Block 20 consists of the following modular components:
  - A dual-console mission operator pallet (MOP) in the cargo bay that controls all subsystems with remote displays and control panels on the flight deck.
  - An interim, limited-functionality, carry-on flight deck workstation for a CSO.
  - The weapon suite consists of an internal, pallet-mounted 30 mm side-firing chain gun and 105 mm cannon; wing-mounted GBU-39/B GPS-guided Small Diameter Bombs (SDBs) and GBU-39B/B Laser SDBs; and AGM-176 Griffin laser-guided missiles mounted internally and launched through the rear cargo door.

  - Two MX-20 electro-optical/infrared sensor/laser designator pods and multiple video, data, and communication links.
  - A side-mounted heads-up display enhances pilot situational awareness.
- Post-IOT&E updates to Block 20, known as Block 20+, include:
  - Software updates to the Gun Fire Control System (GFCS) to correct performance deficiencies observed during Block 20 IOT&E.
  - Additional crashworthy seating, parachute storage, and scanner bubble windows on the right escape hatch and rear paratroop door.
  - Wing-mounted AGM-114 HELLFIRE missiles and internal GBU-69/B Small Glide Munitions (SGM).
  - A permanent CSO station on the flight deck.
  - The Defensive Systems Upgrade (DSU), Electronic Warfare (EW) bus modification, and initial Special Mission Processor (SMP) provision carried over from the baseline MC-130J aircraft, which provides the CSO with refined control of defensive equipment. SMP enables additional situational awareness by passing mission data from the MOP to cockpit displays.
- A future upgrade will equip the aircraft with an active radio-frequency countermeasures (RFCM) system, directed energy weapon, and a GPS hardened MOP.

Mission

The Joint Task Force or Combatant Commander will employ units equipped with the AC-130J to provide close air support and air interdiction using battlespace wide area surveillance, target geolocation, and precision munition employment. Additionally, the AC-130J provides time-sensitive targeting, communications, and command and control capabilities.

Major Contractor

Lockheed Martin – Bethesda, Maryland

Activity

- DOT&E published a classified IOT&E and LFT&E Report on the Block 20 AC-130J on April 25, 2018.
- The AC-130J CTF conducted ground and flight testing of the Block 20+ upgrades and other capability demonstrations throughout FY18:
  - Several captive-carry flights with HELLFIRE and SGMs, and one risk-reduction live fire of a HELLFIRE missile.
  - Initial technology demonstration of the Tactical Off-Board Sensor (TOBS) small unmanned aerial system as a potential AWE sensor.
  - Initial technology demonstration of the Thales I-Master Synthetic Aperture Radar turret as another AWE sensor, temporarily replacing the nose-mounted MX-20 sensor for the demonstration.
- Research, engineering, and risk reduction efforts to develop a high-energy laser for the AC-130J continued throughout 2018.
- The 18th FLTS conducted an operational assessment of the CSO workstation and the DSU/EW bus modification from January to February 2018 in preparation for a formal operational test of the Block 20+ configuration scheduled for 1QFY19.
- Air Force Special Operations Command (AFSOC) received 5 aircraft in FY18, bringing the total to 13 operational aircraft out of a planned fleet of 37.
- In 2018, AFSOC updated its AC-130J program strategy to field capability as soon as it is ready as opposed to comprehensive block upgrades. Block 20+ includes hardware, software, and weapon capabilities originally planned for a later Block 30 configuration.
- The separate USSOCOM program that is developing and testing the RFCM system for both AC-130J and MC-130J experienced a 6-month delay of hardware integration due to antenna design deficiencies. Developmental testing on the first aircraft is scheduled to begin in February 2019. The RFCM program conducted early hardware risk reduction testing in the Joint Preflight Integration of Munitions and Electronic Systems facility and the Integrated Defense Avionics Laboratory from May to July 2018 located at Eglin AFB, Florida.

Assessment

- The Block 20 AC-130J is effective and suitable for most of its Close Air Support and Air Interdiction missions. Training and technical documentation require improvement. Lethality data are adequate to support most mission planning requirements for intended AC-130J missions and targets.
- Survivability analyses revealed the Block 20 Precision Strike Package modifications did not result in any unexpected vulnerabilities to the AC-130J relative to legacy C-130 aircraft.
- Preliminary test results of the updated GFCS software indicate performance improvements address shortfalls observed in IOT&E. Both gun weapon systems are meeting threshold requirements across the full range of test conditions.
- A specific lot of ammunition, not the ammunition rack design, is the cause of the 105 mm ammunition rack problems from the IOT&E report.
- Inadequate training and technical documentation caused the gun calibration procedural problems documented in the IOT&E report. The 19th Special Operations Squadron training unit has rectified the issue.
- Preliminary gun precision and accuracy data indicate that AFSOC should develop quantitative criteria for the 30 mm gun barrel replacement based on round count or other measurable gun parameters in order to predict and control gun performance degradation with usage. AFSOC established standard barrel replacement interval of 15,000 rounds for the 30 mm gun to address this finding.
- The operational assessment of the new permanent CSO workstation, DSU, and EW bus indicate that the CSO workstation has high potential to improve aircrew coordination and reduce workload. DOT&E did not evaluate the performance of the SMP, DSU, and EW bus modification during the majority of the assessment because there was no cybersecurity certification to process classified information on the SMP. Technical and cybersecurity certification problems limited the ability of DOT&E to assess the DSU and EW bus modifications. DOT&E will reassess these modifications during follow-on operational testing.
- Initial demonstrations of both TOBS and I-Master were favorable. USSOCOM has not established a timeline for additional testing and final selection of an AWE system. Assessments of additional technologies for a future acquisition strategy will occur in 2QFY19.
- A fire at the McKinley Climatic Lab, Florida, in July 2017 has indefinitely delayed collection of cold weather deployability data.

Recommendation

1. The Air Force should address the recommendations from the classified DOT&E IOT&E and LFT&E report.

AIM-120 Advanced Medium-Range Air-to-Air Missile (AMRAAM)

Executive Summary

- The Air Force and Navy completed operational test activities for the Air Intercept Missile (AIM)-120D System Improvement Program 1 (SIP-1) in November 2016 and fielded in April 2017. SIP-2 OT&E began in September 2018.
- The Air Force and Navy began operational test activities for the AIM-120C7 Advanced Medium-Range Air-to-Air Missile (AMRAAM) Advanced Electronic Protection Improvement Program (AEPIP) in 2016, with testing continuing through 2018. AEPIP Tape 1 testing completed in August 2017 and fielded in March 2018. AEPIP Tape 2 is currently in OT&E and is scheduled to field in 3QFY19.
- The Air Force and Navy began combined missile cybersecurity testing of the AMRAAM missile in June 2018.

System

- AMRAAM is a radar-guided, air-to-air missile with capability in both the beyond-visual-range and within-visual-range arenas. A single aircraft can engage multiple targets with multiple missiles simultaneously when using AMRAAM.
- F-15C/D/E, F-16C/D, F/A-18C/D/E/F, EA-18G, F-22A, F-35A/B/C, and AV-8B aircraft are capable of employing the AMRAAM.
- The AMRAAM program develops and incorporates planned, periodic software upgrades. The AMRAAM AEPIP is a software upgrade to AIM-120C7. The AEPIP upgrade delivers new capability in two installments, Tape 1 and Tape 2.
- The AIM-120D is the next variant in the AMRAAM family of missiles. The newest missile includes both hardware and software improvements over the AIM-120C3-C7. Four planned follow-on SIPs provide updates to the AIM-120D to enhance missile performance and resolve previous deficiencies.

Mission

- The Air Force and Navy, as well as several foreign military forces, employ various versions of the AIM-120 AMRAAM to conduct air-to-air combat missions.
- All U.S. fighter aircraft use the AMRAAM as the primary beyond-visual-range air-to-air weapon.

Major Contractor

Raytheon Missile Systems – Tucson, Arizona

Activity

- The Air Force and Navy conducted all testing in accordance with DOT&E-approved test plans.

AIM-120D SIP

- The Air Force and Navy are conducting SIP-2 operational testing, which is scheduled to complete in 4QFY19 with fielding in 1QFY20.

AIM-120C7 AEPIP

- The Air Force and Navy are conducting operational testing for the AEPIP software upgrade to C7 missiles. Testing began in FY16 and is expected to complete in 1QFY19. AEPIP Tape 2 testing is in progress and scheduled to field in 3QFY19.

Cybersecurity

- The Air Force and Navy began combined cybersecurity testing of the AMRAAM missile in June 2018 and will complete in 2QFY19.

Assessment

- AMRAAM continues to be operationally effective and suitable.
- The AIM-120D SIP-1 missile meets performance and reliability requirements.
- The AIM-120C3-7 AEPIP Tape 1 missile meets performance and reliability requirements.

Recommendations

None.

Air Operations Center – Weapon System (AOC-WS)

Executive Summary

- The Air Force canceled the Air Operations Center – Weapon System (AOC-WS) 10.2 contract in July 2017 and program in January 2018. In July 2018, the Air Force authorized alternative approaches via National Defense Authorization Act Section 804, Middle Tier Acquisitions, to achieve faster development, testing, and fielding of AOC-WS 10.2 requirements.
- From October 2017 through July 2018, the Air Force conducted developmental and operational test of AOC-WS 10.1 Release 10.1.15, which included a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA).
- In July 2018, the Air Force authorized the use of Section 804 for Command and Control (C2) Air Operations Suite – C2 Information Services (C2AOS C2IS) to deliver a Minimum Viable Product (MVP) via the AOC-WS Modifications "Block 20" effort executed by the Air Force Kessel Run organization. The Air Force intends to transition the program to AOC-WS Modifications "Block 20" for continued modernization and sustainment.
- The AOC Configuration Review Board conducted a Full Deployment Decision of AOC-WS 10.1 Release 10.1.15 in September 2018.

System

- The AOC-WS 10.1 (AN/USQ-163 Falconer) is a system of systems that incorporates numerous third-party software applications and commercial off-the-shelf products. Each third-party system integrated into the AOC-WS provides its own programmatic documentation.
- AOC-WS capabilities include C2 of joint theater air and missile defense; pre-planned, dynamic, and time-sensitive multi-domain target engagement operations; and intelligence, surveillance, and reconnaissance operations management.
- The AOC-WS consists of:
  - Commercial off-the-shelf software and hardware for voice, digital, and data communications infrastructure.
  - Government software applications developed specifically for the AOC-WS to enable planning, monitoring, and directing the execution of air, space, and cyber operations to include:
    - Theater Battle Management Core Systems (TBMCS) – Force Level
    - Master Air Attack Plan Toolkit (MAAPTK)
  - Other government software applications used by the AOC-WS to enable joint and interagency integration include:
    - Global Command and Control System – Joint (GCCS-J)
    - Joint Automated Deep Operations Coordination System (JADOCS)

  - Additional third-party systems that accept, process, correlate, and fuse C2 data from multiple sources and share them through multiple communications systems.
- When required, the AOC-WS operates on several different networks, including the SIPRNET, Joint Worldwide Intelligence Communications System, and coalition networks. The networks connect the core operating system and primary applications to joint and coalition partners.
- The AOC-WS 10.2 requirements for a modernized, integrated, and automated approach to AOC operations remain valid.
- C2AOS C2IS is a software developmental program to upgrade critical AOC-WS mission software, including TBMCS. The Air Force intends to deliver an MVP via the AOC Modifications "Block 20."

Mission

The Commander, Air Force Forces or the Joint/Combined Forces Air Component Commander uses the AOC-WS to exercise C2 of joint (or combined) air forces, including planning, directing, and assessing air, space, and cyberspace operations; air defense; airspace control; and coordination of space and mission support not resident within theater.

Major Contractors

- AOC-WS 10.1 Production Center: Raytheon Intelligence, Information and Services – Dulles, Virginia
- AOC-WS Modifications "Block 20" (Section 804): Raytheon Intelligence, Information and Services – Dulles, Virginia; Pivotal Software, Inc. – San Francisco, California
- C2AOS-C2IS (Section 804): Leidos – Reston, Virginia; Pivotal Software, Inc. – San Francisco, California

Activity

- From October 2017 through July 2018, the Air Force conducted operational test of AOC-WS 10.1 Release 10.1.15, which included a cybersecurity CVPA. DOT&E approved the test plan submitted by the Operational Test Organization, the 605th Test and Evaluation Squadron (TES).
  - Release 10.1.15 updates software applications including GCCS-J, MAAPTK, and TBMCS – Force Level.
  - Additionally, Release 10.1.15 updates hardware and software providing core services, to include privileged SIPRNET tokens, virtualized servers, and updated server and workstation operating systems.
  - The Air Force delayed the execution of the cybersecurity Adversarial Assessment (AA) scheduled for July 2018, as described in the DOT&E-approved test plan, due to schedule conflicts with the 177th Information Aggressor Squadron. The 605 TES completed the AA in November 2018, evaluation and reporting are in progress.
- In September 2018, despite the known cybersecurity vulnerabilities and functional deficiencies, the AOC Configuration Review Board elected to field AOC-WS 10.1 Release 10.1.15.

Assessment

- The Air Force adequately tested Release 10.1.15 during integrated developmental and operational test.
- Release 10.1.15 demonstrated the required capabilities for the AOC to execute the joint air tasking order cycle and conduct operational C2 of theater air operations. AOC-WS is operationally effective.
- The 605 TES identified two new Category I functional deficiencies during test. AOC-WS is not operationally suitable, primarily because of these Category I deficiencies. Additionally, the Air Force has not developed a plan to collect and report reliability, availability, and maintainability data.
- The integrated test and CVPA of Release 10.1.15 revealed new Category I deficiencies in this update that degrade the survivability of the AOC. Details are classified.

Recommendations

The Air Force should:

1. Fix or mitigate the Category I cybersecurity and functional deficiencies in AOC-WS 10.1 Release 10.1.15.
2. Implement a solution to meet the long-standing requirement to collect and report reliability, availability, and maintainability data for the AOC-WS.

B61 Mod 12 Life Extension Program Tail Kit Assembly

Executive Summary

- The B-61 Mod 12 (B61-12) Life Extension Program (LEP) Tail Kit Assembly (TKA) completed DOD developmental testing and continues Department of Energy (DOE) system qualification testing.
- The TKA demonstrated high degrees of accuracy and reliability in testing to date with no reliability failures.
- The Air Force executed a Milestone C decision on October 26, 2018.
- Operational testing is scheduled to begin 2QFY19, contingent upon:
  - Delivering operationally representative Bomb Assemblies (BA) on time
  - Releasing updated F-15E mission planning software
  - DOT&E accepting a mix of B61-12 Weapons Control Units (WCU) using a Field Programmable Gate Array (FPGA) or Application-Specific Integrated Circuit (ASIC) chips as production representative

System

- The Nuclear Weapons Council (NWC)-directed B61-12 LEP entails the consolidation of four legacy B61 variants (Mods 3, 4, 7, and 10) into a single variant featuring a limited-life component upgrade to the BA and integration with a new TKA.
- The TKA is a subassembly of the B61-12 All-Up-Round (AUR) and will be tested in accordance with DOD Instruction (DoDI) 5000.02 requirements. The B61-12 DOE activities are led by the National Nuclear Security Administration (NNSA), and the BA subassembly will be tested and qualified per activities defined in the NWC Procedural Guideline for the Phase 6.X Process. When mated, the BA and TKA constitute an AUR, which will be qualified in accordance with the B61-12 System Qualification Plan.
- The TKA is designed to be mechanically mated and electrically connected to the nuclear BA and provides the B61-12 with a guide-to-target capability (System 2), while retaining the legacy ballistic flight capability (System 1).
- Controlled guidance is achieved via pre-programmed target location data being provided as inputs to the TKA guidance, navigation, and control (GNC) system. The TKA design does not include a GPS receiver.

Mission

The B61 thermonuclear bomb family is a key component of the current U.S. nuclear deterrence. A unit equipped with the air-delivered B61-12 nuclear weapon plays a critical role in supporting the airborne leg of the nuclear triad for the United States and allies abroad.

Major Contractor

Boeing Defense, Space & Security – St. Louis, Missouri

Activity

- The Air Force conducted developmental testing in accordance with a DOT&E-approved Test and Evaluation Master Plan (TEMP) for the B61-12 LEP TKA. DOT&E approved an updated TEMP in support of the Milestone C decision on October 26, 2018.
- The Air Force completed the developmental test phase in FY18 with the release of 16 free-flight weapons and completion of developmental cybersecurity testing. Over the past 2 years, the B61-12 LEP TKA has flown 22 free-flight weapon releases as part of TKA developmental testing.
- Reliability testing included the 22 developmental test releases and 9 additional DOE/NNSA system qualification flight tests.
- Results from the TKA developmental testing, supplemented with system qualification test results, will support an Operational Test Readiness Review (OTRR) in 2QFY19. The Air Force has scheduled B61-12 LEP TKA operational testing following the OTRR with initial events occurring in February 2019 and flight tests starting in March 2019. These dates are approximately 3 months later than previously

planned because of production delays with parts of the BA subassembly resulting in delivery slips for B61-12 AURs.
- In FY18, Sandia National Lab conducted comparison testing between two different versions of the WCU to determine if there are any performance differences between those WCUs containing an FPGA chip and those containing an Application-Specific Integrated Circuit (ASIC). This comparison testing is required for DOT&E to determine if FPGA-equipped BAs are production representative for use in IOT&E. Analysis is ongoing and expected to be complete prior to the end of CY18.

Assessment
- Air Force developmental testing of B61-12 LEP TKA is complete and system qualification testing is ongoing. Preliminary results to date indicate:
  - The TKA demonstrates high reliability, availability, and accuracy. There have been no reliability failures during flight test and all weapons have hit inside the system accuracy requirement.
  - One system component presents a cybersecurity vulnerability, but mitigation or elimination of the vulnerability appears feasible without a major investment of time or money.
- WCU comparison test data will allow DOT&E to determine if the current planned test articles with two different versions of the WCU are production representative for the purpose of IOT&E.
- While production appears to be sufficient to meet the current scheduled IOT&E completion date, delayed delivery of operational test articles will require a more aggressive test pace. A delay in the delivery of updated F-15E mission planning software to enable the planning of loft delivery missions could also affect the timely completion of operational testing.

Recommendations

The Air Force must:
1. Resolve the outstanding cybersecurity issues during the operational test period.
2. Deliver the F-15E mission planning software before the first scheduled F-15E mission.

C-130J

Executive Summary
- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted the C-130J Block Upgrade 8.1 (BU8.1) IOT&E from July through October 2018, primarily operating out of Little Rock AFB, Arkansas.
- The cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) in 2017 had technical shortfalls limiting DOT&E's ability to evaluate the cybersecurity posture of the C-130J. AFOTEC is working with the 57th Information Aggressor Squadron (IAS) to remedy those data shortfalls in preparation for the Adversarial Assessment (AA) in March 2019.

System
- The C-130J is a medium-sized four-engine turboprop tactical transport aircraft.
- The C-130J digital avionics and navigation systems enabled the Air Force to reduce the flight deck aircrew to two pilots, eliminating the navigator and flight engineer positions. Since fielding the C-130J, the Air Force has been implementing periodic Block Upgrades to improve workload and human factors for the reduced aircrew.
- BU8.1 provides navigation and communication updates to the C-130J to comply with International Civil Aviation Organization (ICAO) requirements and ensure continued access to civil airspace. It will field a Link 16 capability and deficiency corrections that were provided by the Block Upgrade 7.0, which the Air Force did not field after developmental testing.

Mission
- Combatant Commanders use the C-130J within a theater of operations for Combat Delivery missions which include:
  - Airdrop of paratroopers and cargo (palletized, containerized, bulk, and heavy equipment)
  - Airland delivery of passengers, troops, and cargo
  - Emergency aeromedical evacuations

- Combat Delivery units operate globally in civil-controlled airspace and in all weather and lighting conditions.

Major Contractor
Lockheed Martin Aeronautics Corporation – Fort Worth, Texas

Activity
- In March 2018, the C-130J BU8.1 aircraft participated in the Developmental Test Navigation Festival (DT NAVFEST) GPS denial exercise with the 746th Test Squadron at White Sands Missile Range, New Mexico.
- AFOTEC began IOT&E with two BU8.1 aircraft at Little Rock AFB on July 9, 2018. IOT&E aircrews participated in a Green Flag joint exercise and completed equatorial-, date line-, and Prime Meridian-crossing missions with oceanic and International Civil Aviation Organization (ICAO) airspace operations. IOT&E concluded in October 2018, with the exception of the cybersecurity AA, which is scheduled for March 2019.

Assessment
- The C-130J Block 8.1 does not have an operationally representative mission planning capability. In 2016, the Air Force Life Cycle Management Center (AFLCMC) mission planning office decided not to develop the C-130 legacy mission planning system for the Block 8.1 configuration. AFLCMC is working to field a C-130 Aircraft Weapons

Electronics Joint Mission Planning System (JMPS) for Block 8.1 to Air Mobility Command. In the absence of a mission planning capability, Air Force Program Office engineers are providing C-130J formatted initialization data loads to aircrews to support Link-16 operability on applicable IOT&E missions, while aircrews manually enter mission data to the aircraft for other systems.

- The 2017 CVPA limited DOT&E's ability to evaluate the cybersecurity posture of C-130J because the test team did not have access to tools for some systems within the cybersecurity test boundary. The 57th IAS conducted a system survey in advance of supporting the AA in order to address shortfalls in the data provided by the CVPA.
- Data analysis in ongoing.

Recommendations

The Air Force should.

1. Provide a operationally representative JMPS for Block 8.1
2. Complete an AA

Combat Rescue Helicopter (CRH)

Executive Summary
- The Combat Rescue Helicopter (CRH) is currently in the Engineering and Manufacturing Development (EMD) phase, with first flight of an EMD aircraft scheduled for February 2019.
- Qualification testing of many components of the aircraft have uncovered technical deficiencies that the Program Office is working to resolve. As a result, the program will begin flight test and operational assessment (OA-2) with a large number of CRH-specific systems in non-operationally representative configurations. The Program Office will be unable to provide CRH-specific information on these components to the Milestone Decision Authority in advance of the Milestone C decision, scheduled for September 2019.
- Qualification testing for components undergoing live fire testing revealed multiple design and manufacturing deficiencies for many components that may adversely affect the development schedule.

System
- The CRH (mission-design-series HH-60W) is a new-build, dual-piloted, multi-engine rotary-wing aircraft based on the in-production Army UH-60M helicopter.
- The CRH is intended to replace the aging fleet of Air Force HH-60G as its Combat Search and Rescue Aircraft.
- The CRH is intended to be able to fly a combat radius of at least 195 nautical miles (nm) without aerial refueling and conduct a hover out-of-ground effect (HOGE) at its mid-mission gross weight for its mission profile.
- The CRH will have susceptibility and vulnerability reduction features equivalent to or better than the current HH-60G aircraft:
  - Crew and cabin armor, self-sealing fuel cells that do not suffer catastrophic damage from high-explosive incendiary rounds, and crew and passenger crashworthy seating

  - CRH-unique AN/APR-52 radar warning receiver (RWR) to detect infrared (IR), radio frequency (RF), and laser threats
  - Three crew-served forward and side-firing self-protection weapons: the GAU-2, GAU-18, and the GAU-21

Mission
- Units equipped with the CRH will recover isolated personnel from hostile or denied territory, day or night, in adverse weather, and in a variety of threat spectra from terrorist attacks to chemical, biological, radiological, and nuclear threats.
- Secondary missions include humanitarian missions, civil search and rescue, disaster relief, medical evacuation, and non-combatant evacuation operations.

Major Contractor
Sikorsky Aircraft, a Lockheed Martin Company – Stratford, Connecticut

Activity
- EMD 1 and 2 aircraft are completing build at the Sikorsky facility in Stratford, Connecticut. EMD 1 is expected to be complete October 17, 2018, and EMD 2 is expected to be complete November 9, 2018. First flight is scheduled to occur with EMD 2 in February 2019.
- The 704th Test Group completed live fire testing of the flight crew armored seat in March 2018.
- Qualification testing for the fuel cell to demonstrate self-sealing capability occurred in October 2017 for Phase I article testing and September 2018 for full-scale production-representative fuel bladder testing.
- Qualification testing for the cabin and cockpit armor occurred in February and June 2018.
- Qualification testing for the primary aircrew seating occurred in May 2018 and August 2018.
- Qualification testing for the seat track pallet occurred in August 2018.
- Qualification testing for the primary rescue hoist began June 18, 2018, with 3 of 26 sub-tests complete, including a safety of flight vibration test which failed.

- Qualification testing for the gun mount began September 4, 2018; with 1 of 26 sub-tests complete, a safety of flight vibration test which failed.
- Qualification testing for the digital RWR began March 30, 2018. The software testing for qualification has not begun, although it has been successfully tested in the Integrated Demonstrations and Applications Laboratory.
- Testing has been performed in accordance with the DOT&E-approved Alternate LFT&E Strategy.
- Operational test planning for OA-2 has been in accordance with the DOT&E-approved Milestone B Test and Evaluation Master Plan (TEMP) from April 2015.

Assessment

- Due to delays in production and in acquiring necessary data to support the airworthiness technical authority review, including incomplete results stemming from qualification testing failures, first flight has slipped from October 2018 to February 2019 at the earliest.
- The current plan to begin flight testing in 2QFY19 in support of a September 2019 Milestone C decision means it is unlikely that the tactical mission kit, Link 16, digital RWR, rescue hoist, gun mount and systems, fuel cells, armor, and primary aircrew seating will be in an operationally representative configuration when testing begins. As these systems are still undergoing design changes, the Milestone Decision Authority will have limited information on HH-60W-unique components to support an informed Milestone C decision.
- Fuel cell qualification testing demonstrated several design and manufacturing deficiencies that need to be resolved:
  - The current design exceeds the weight allowance.
  - The design does not meet the Military Detail (MIL-DTL) for normal temperature, cold temperature, or self-sealing performance versus some threats. The Program Office intends to proceed with modified criteria which will allow some fuel cell leakage to be considered a pass of the specification.
  - Manufacturing control and process deficiencies have delayed and impaired testing. For example, test articles have not been manufactured to design; articles that are design compliant show significant variation from article to article, which may adversely affect the weights and vulnerabilities of the operational fuel cells.
- Phase II qualification testing significantly damaged a production-representative live fire test aircraft structural component, the repair of which may further delay live fire fuel cell testing several months or necessitate a change in the LFT&E Strategy if the article cannot be repaired.
- Cabin and cockpit armor qualification testing has failed twice, necessitating redesigns and remanufactures. The current redesign, which still requires retest, will increase armor weight by as much as 60 pounds (21 percent) beyond the expected allocation and may not be available in time for initial flight test. The Program Office is considering tailoring the qualification test pass criteria to minimize the weight impact in some areas of the aircraft.
- The primary aircrew seat qualification testing included multiple failures. The program intends to redesign the seat and use an alternate seat qualified on the HH-60G during initial flight test in order to meet the schedule.
- The seat track pallet is being redesigned based upon analysis of crash test data. This will delay live fire testing of this component by approximately 3 months and may require repeat qualification testing.
- As of October 2018, analysis is insufficient to assess success on the limited qualification testing for the primary rescue hoist.

Recommendations

The CRH Program Office should:

1. Adjust the program schedule to ensure that CRH-specific hardware is available for the upcoming operational assessment to enable an operationally meaningful and adequate system in support of the Milestone C decision.
2. Given the proposed changes to system specification requirements, determine if the CRH will be more survivable than the HH-60G, as required by the Capabilities Development Document.

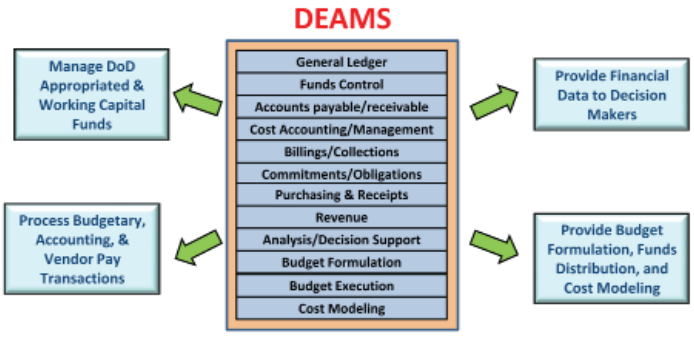
Defense Enterprise Accounting and Management System (DEAMS)

Executive Summary

- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted Operational User Evaluation (OUE) phase two from February 26 to March 16, 2018, by observing day-to-day operations at five Air Force Bases and a Defense Finance and Accounting System (DFAS) location in the Pacific Air Force (PACAF) theater of operations.
- The Defense Enterprise Accounting and Management System (DEAMS) Increment 1 demonstrated significant, sustained improvements in operational effectiveness and suitability compared to the 2015 IOT&E. Based upon the results of the OUE, DEAMS Increment 1 is operationally effective and operationally suitable.
- Based upon the 2015 IOT&E cybersecurity testing, DOT&E assessed DEAMS as not cyber secure. The DEAMS Program Manager has made significant improvements to DEAMS cybersecurity and plans to continue to conduct cybersecurity testing in CY19.

System

- DEAMS Increment 1 is a Defense Business System that uses commercial off-the-shelf enterprise resource planning software to provide accounting and management services.
- The DEAMS Increment 1 Program Management Office (PMO) is following an evolutionary acquisition strategy that adds additional capabilities and users incrementally. There are six scheduled releases. The Air Force anticipates over 16,900 users worldwide will use DEAMS by the end of the increment.
- DEAMS Increment 1 is intended to improve financial accountability by providing a single, standard, automated financial management system that is compliant with the Chief Financial Officers Act of 1990 and other mandates. DEAMS Increment 1 performs the following core accounting functions:
  - Core Financial System Management
  - General Ledger Management
  - Funds Management
  - Payment Management
  - Receivable Management
  - Cost Management
  - Reporting
- DEAMS interfaces with approximately 40 other systems that provide travel, payroll, disbursing, transportation, logistics, acquisition, and accounting support.
- DEAMS supports financial management requirements in the Federal Financial Management Improvement Act of 1996 and the DOD Business Enterprise Architecture.



Mission

Air Force financial managers and tenant organizations use DEAMS Increment 1 to do the following across the Air Force, U.S. Transportation Command, and other U.S. component 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

Major Contractors

- DSD Laboratories – Sudbury, Massachusetts
- Accenture Federal Services – Dayton, Ohio

Activity

- AFOTEC conducted phase one of the OUE in 2017, and DOT&E reported on this phase in the FY17 Annual Report. AFOTEC conducted phase two of the OUE from February 26 through March 16, 2018, in accordance with a DOT&E-approved test plan. OUE phase two testing collected day-to-day operations data at the following locations: Joint Base Pearl Harbor-Hickam, Hawaii; Kadena Air Base, Japan; Osan Air Base, Korea; Andersen Air Force Base, Guam; and Yokota Air Base, Japan. AFOTEC collected data on the adequacy of help desk support at Wright-Patterson AFB, Ohio; system maintenance at Maxwell AFB-Gunter Annex, Alabama; and a DFAS location in Japan.

- During the OUE, DEAMS Increment 1 was used by 13,800 users to conduct accounting management operations out of a total user base of 16,900 for the increment.
- As part of the OUE, the Army Research Laboratory at White Sands Missile Range, New Mexico, supported the PMO in conducting a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) August 7 – 11, 2017, at Maxwell AFB – Gunter Annex, Alabama.
- DEAMS Increment 1 plans to field a software upgrade in FY19.

Assessment

- During the 2017-18 OUE, DEAMS Increment 1 demonstrated significant improvement compared to the 2015 IOT&E and the 2016 Verification of Fixes test. Based upon the results of the OUE, DEAMS Increment 1 is operationally effective and operationally suitable. Key effectiveness findings from the OUE are:
  - DEAMS supported financial operations, and all Key Performance Parameters (KPPs) were met.
    - DEAMS met the user role requirement with 99.99 percent (103,870 out of 103,877) compliant with Comptroller guidelines for segregation of duties; requirement is 90 percent.
    - DEAMS met the Business Rules requirement with 98 percent (322 out of 328) compliant with the Standard Financial Information Structure policy and procedures; requirement is 95 percent.
    - DEAMS balanced with the United States Treasury 99.8 percent of the time (38,482,144 out of 38,566,025 line items); requirement is 95 percent.
    - One hundred percent of subsidiary accounts were successfully reconciled to their respective general ledger accounts; requirement is 95 percent.
    - One hundred percent of accounts were correctly reconciled at the end of all accounting periods observed (monthly, quarterly, and annually); no requirement specified.
  - During the OUE, the transaction backlog – which had caused major operational problems during previous tests – did not adversely affect operations.
- The DEAMS Program Office has made significant progress in the area of regression testing, which helps verify that enhancements or software defect fixes do not adversely affect overall system performance. As of August 2017, regression scripts covered 22 of the 24 critical interfaces. As DEAMS completes fielding of the software upgrade, full coverage of critical interfaces will help verify that DEAMS is sending and receiving accurate data.
- Key suitability findings from the OUE are:
  - Operational availability was 97 percent; requirement is 80 percent.
  - Eighty-four percent (208 out of 247) of respondents rated DEAMS help desk support as slightly effective or better, and comments indicated that the users perceive help desk support as continuing to improve. DEAMS Help Desk initial resolutions were successful 97 percent of the time.
  - While 77 percent (230 out of 299) of respondents rated training as slightly effective or better, users continued to comment that training does not adequately prepare them for site-specific nuances in workflow.
  - Eighty-four percent (416 out of 493) of users rated documentation as slightly effective or better, which represents an improvement from surveys in previous operational tests.
- Despite good overall performance during the OUE, DEAMS exhibited 47 defects that do not have sustainable work arounds, and System Usability Scale (SUS) results indicate operators continue to have low regard for DEAMS usability with the median SUS score of 45 (with 50 considered as the limit for marginal usability).

Recommendations

The DEAMS Program Manager should:

1. Address cybersecurity vulnerabilities that present a high risk to DEAMS missions.
2. Continue efforts to reduce severity 2 defects in DEAMS.
3. Complete development of regression scripts to cover all 24 critical interfaces for the latest release of DEAMS.
4. Continue to improve DEAMS training, with a focus on site-specific workflows.

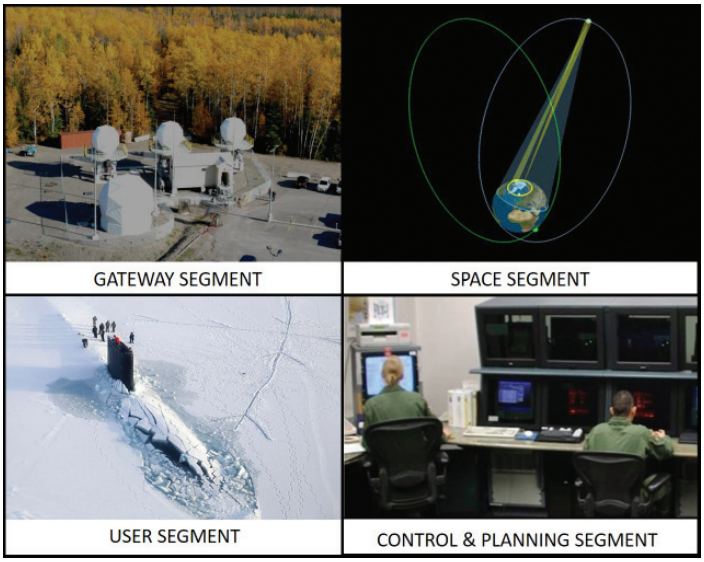
Enhanced Polar System (EPS)

Executive Summary

- The Enhanced Polar System (EPS) system is not deployed and is still being tested to resolve configuration problems prior to operational test and deployment.
- The EPS Program's Lead Developmental Tester Organization (LDTO) conducted Integrated Test #1 (IT-1) in January through February 2018 that identified problems with end-to-end system integration, operational procedures, and operator training.
- The EPS Program Office conducted a series of risk reduction and integrated test events to prove they resolved the integration problems prior to MOT&E. These developmental and integrated test events demonstrated improvements to the communication planning process, a better understanding of the end-to-end architecture, and clarified operator roles and responsibilities in resolving system problems. The Program Office subsequently resolved problems with voice communications, but problems in consistently establishing and maintaining specific end-to-end data communications remain.
- The EPS Integrated Test (IT) #4 resulted in the Navy Broadcast Control Authority (BCA) unable to transmit and receive data broadcast and data teletype messages to deployed submarines on a consistent basis.
- The Air Force Test and Evaluation Center (AFOTEC) has executed two phases of a planned three-phase MOT&E. AFOTEC collected data from the operationally realistic integrated testing and the Navy's 2018 Ice Exercise (ICEX), per the DOT&E-approved test plan. AFOTEC planned a dedicated MOT&E period from July 16 through September 14, 2018, but the Air Force postponed this phase of the MOT&E pending resolution of system-of-system integration problems and the Program Executive Officer certifying the EPS ready for operational test. The EPS MOT&E is tentatively scheduled for 2QFY2019.

System

- EPS is designed to provide secure, jam-resistant satellite communications in the North Polar Region using a subset of the Advanced Extremely High Frequency eXtended Data Rate waveform.
- EPS consists of four segments:
  - The Payload Segment consists of two payloads hosted on satellites placed in highly elliptical orbits. The EPS payloads will provide polar communications coverage for 24 hours per day.
  - The Control and Planning Segment (CAPS) is the primary means for monitoring and controlling the payloads via a ground connection to a Tracking and Commanding terminal in the polar region. The Tracking and Commanding terminal will provide radio frequency connectivity between the payload and CAPS.



  - The Gateway Segment consists of a single gateway site with three collocated gateway terminals that will provide connectivity radio frequency connectivity between the payload and the gateway ground equipment. The Gateway Segment is also designed to provide ground connectivity between north polar and mid-latitude users through the DOD Teleport System.
  - The EPS Terminal Segment consists of user terminals that are Multiband Terminal platform variants. The Navy Multiband Terminals can be deployed on ships and submarines, as well as at specific fixed ground locations. Additional terminals are currently unfunded but may be developed in the future and deployed on aircraft and ground-transportable, mobile, and fixed terrestrial platforms.

Mission

Combatant Commanders will use EPS to provide secure, jam-resistant tactical satellite communications required to support peacetime, contingency, and wartime operations at high north latitudes with command and control centers located elsewhere.

Major Contractors

- Northrop Grumman Aerospace Systems – Redondo Beach, California
- Northrop Grumman Mission Systems – Redondo Beach, California

Activity

- EPS is not deployed and is still being tested to resolve integration problems prior to operational test and deployment.
- The EPS Program Office's LDTO and AFOTEC conducted IT-1 from January 8 through February 23, 2018, using the BCA Pacific at Pearl Harbor, Hawaii, to communicate with a submarine in Groton, Connecticut, and a Navy destroyer in Everett, Washington.
- The Air Force planned and conducted, with Army Red Teams, extended, operationally realistic cyber-threat testing from January 8 through February 16, 2018, and resumed testing from July 14 – 30, 2018. An Air Force Red Team conducted further testing on August 6 – 17, 2018. The Air Force and Army conducted all testing in accordance with the DOT&E-approved cyber test plan.
- The EPS Program Office, AFOTEC, and Massachusetts Institute of Technology/Lincoln Laboratory tested the jam-resistant capabilities of EPS from February 20 – 23, 2018, in Clear, Alaska.
- The EPS Program Office participated in the Navy biennial ICEX conducted from March 7 – 18, 2018. During the ICEX, two submarines conducted polar operations. The Navy designated 2 days during the exercise for EPS testing.
- The EPS Program Office conducted a series of increasingly complex risk reduction events from March 30 through May 11, 2018, at Commander, Task Force-69 (CTF-69), U.S. 6th Fleet, and operational submarines to validate end-to-end polar communications. The EPS Program Office's LDTO conducted IT-2 from June 4 – 15, 2018, at CTF-69 and at the Naval Undersea Warfare Lab. The purpose of IT-2 was to evaluate EPS end-to-end (CTF-69 to Submarine) communication capabilities and to verify fix actions of problems discovered in IT-1 using the Undersea Warfare Lab, acting as a submarine surrogate.
- AFOTEC executed two phases of the planned three-phase MOT&E. AFOTEC collected data from the operationally realistic integrated testing and the Navy's 2 ICEX, per the DOT&E-approved test plan. AFOTEC planned a dedicated MOT&E period from July 16 through September 14, 2018, but the Air Force postponed the dedicated MOT&E pending resolution of system-of-system integration problems and the Program Executive Officer certifying the EPS ready for operational test. The EPS MOT&E is tentatively scheduled for 2QFY19.
- The EPS Program Office's LDTO conducted IT-3 from August 9 – 17, 2018, at Commander, Submarine Force Atlantic and on a submarine based in Norfolk, Virginia, to test end-to-end communication capabilities to support submarine polar operations. The LDTO also tested surface ship communications between an Everett, Washington-based Navy destroyer and NCTAMS Pacific in Hawaii.
- The program manager conducted a developmental test followed by LDTO IT-4 from September 10 – 28, 2018, to demonstrate the end-to-end submarine data communications performance.

Assessment

- The EPS Program Office, AFOTEC, and Army and Air Force Red Teams executed 9 and a half weeks of cyber-testing to more closely represent a persistent cyber threat and conduct more extensive testing than has been typically planned for programs in the past. Problems with system performance, challenges with gaining authority to connect to the system, system misconfigurations, and changes in schedules resulted in a partially completed cyber test. AFOTEC is scheduling additional Red Team testing to occur during the dedicated MOT&E period. The Program Office and AFOTEC have placed a significant focus on the cybersecurity assessment. However, additional work remains to ensure that the system provides secure communications in a cyber-contested environment.
- The IT-1 identified problems with end-to-end system integration, operational procedures, and operator training. The communication planning process required more fidelity on equipment configurations than was anticipated. The EPS operators had difficulty resolving problems when they occurred, and a lack of understanding the complete end-to-end architecture led to poor communications performance for both submarines and surface ships.
- The anti-jam test results confirmed that EPS has modulation modes on all beam coverage areas that allow communications through threat-representative jamming.
- During ICEX, the Navy was not able to consistently pass voice messages from the Arctic-deployed submarines to the Pacific BCA in Hawaii. The Navy was unable to successfully transmit and receive data messages. The Navy operators experienced configuration problems, and a general lack of knowledge about the EPS system architecture and troubleshooting procedures hampered problem resolution. The current Navy Polar Concept of Operations (CONOPS) does not discuss EPS operations and the Navy needs to update the CONOPS to include EPS. The lack of CONOPS inhibited a shared understanding of how EPS supports Navy submarine and surface combatant polar operations.
- The EPS Program Office risk reduction testing demonstrated voice communications consistent with the current satellite system but problems in consistently establishing and maintaining specific end-to-end data communications remained. The risk reduction testing also resulted in improvements to the communication planning process, a better understanding of the end-to-end architecture, and of operator roles and responsibilities in resolving problems. The testing also fostered increased efforts by the Navy to integrate EPS into the Navy communications architecture.
- The EPS IT-2 event demonstrated improved performance in communications planning and user ability to log on to the EPS payloads. However, the Navy BCA was unable to send data broadcast and teletype messages to deployed submarines on a consistent basis.
- During EPS IT-3 the Navy BCA was unable to send data teletype messages to deployed submarines. The BCA

was able to transmit broadcast messages intermittently but could not consistently maintain this capability. The short availability of the submarine to conduct testing truncated efforts at troubleshooting and finding the root-cause of the inconsistency. The NCTAMS and the Navy destroyer were also unable to communicate consistently over EPS during the test event.
- The EPS IT-4 resulted in the Navy BCA unable to transmit and receive data broadcast and data teletype messages to deployed submarines on a consistent basis.

Recommendations
- The Air Force should:
  1. Continue to work with the Navy to integrate EPS into the Navy communications architecture prior to MOT&E.
  2. Work with the Navy to formalize EPS end-user training aboard U.S. Navy vessels.
  3. Address findings from the cybersecurity assessments to ensure that EPS can fulfill its mission in a cyber-contested environment.
- The Navy should develop and publish an updated Polar CONOPS based upon the EPS.

F-22A – RAPTOR Modernization

Executive Summary

- F-22A Increment 3.2B is a Major Defense Acquisition Program modernization effort intended to integrate AIM-120D and AIM-9X missile systems; an Enhanced Stores Management System (ESMS) for weapons integration and employment improvements; Intra-Flight Data Link (IFDL) improvements and electronic protection enhancements; improved emitter geolocation capability; and a Common Weapon Employment Zone for air-to-air missile employment. IOT&E began August 21, 2017, and completed April 6, 2018, with the Air Force Full-Rate Production decision on August 10, 2018.
- Update 6 is a software-only Operational Flight Program (OFP) effort to update the aircraft cryptographic module with an F-22A cryptographic architecture change to accommodate multiple, simultaneous algorithms for Link 16 datalink interoperability and secure ultrahigh frequency radio communications. Update 6 also is intended to incorporate deferred software corrections carried over from Increment 3.2B developmental testing. Developmental testing began November 13, 2017, with an expected completion of January 7, 2019. The Air Force intends to field Update 6 in 2019.

System

- The F-22A is an air-superiority fighter that combines low observability to threat radars, sustained high speed, and integrated avionics sensors.
- Low observability reduces threat capability to engage F-22As with current adversary weapons.
- The aircraft maintains supersonic speeds without the use of an afterburner.
- Avionics fuse information from the Active Electronically Scanned Array radar, other sensors, and datalink information for the pilot to enable employment of medium- and short-range air-to-air missiles, guns, and air-to-ground munitions.
- The Air Force intended the F-22A to be more reliable and easier to maintain than legacy fighter aircraft.
- F-22A air-to-air weapons are the AIM-120C/D radar-guided missile, the AIM-9M/X infrared-guided missile, and the M61A1 20 mm gun.
- F-22A air-to-ground precision strike capability consists of the 1,000-pound Joint Direct Attack Munition and the 250-pound Small Diameter Bomb Increment 1.
- The F-22A program delivers capability in increments. Incremental Enhanced Global Strike modernization efforts include the following current and near-term modernization efforts:

- Increment 3.1 provided enhanced air-to-ground mission capability, to include geolocation of selected emitters, electronic attack, air-to-ground synthetic aperture radar mapping and designation of surface targets, and Small Diameter Bomb integration.
- Increment 3.2A was a software-only upgrade providing improved electronic protection, Link 16 Receive, and combat identification capabilities. Increment 3.2A is a modernization effort within the scope of the F-22A Advanced Tactical Fighter baseline acquisition program of record and is currently fielded in operational F-22A units.
- Update 5 combined an OFP upgrade providing software driven radar enhancements, Ground Collision Avoidance System software, and the incorporation of limited AIM-9X capabilities. The Update 5 OFP is currently fielded in operational F-22A units.
- Increment 3.2B is a separate Major Defense Acquisition Program modernization effort that integrates AIM-120D and AIM-9X missile systems; an ESMS for weapons integration and employment improvements; IFDL and electronic protection enhancements; improved emitter geolocation capability; and integration of a Common Weapon Employment Zone for air-to-air missiles employed by the F-22A. IOT&E of the 3.2B capability concluded in April 2018 and is currently projected to begin fielding mid-2019 with a compatible version of Update 6 software.
- Update 6 is a software-only OFP effort to update the aircraft KOV-20 cryptographic module with an F-22A cryptographic architecture change to accommodate multiple, simultaneous algorithms for Link 16 datalink interoperability and secure ultrahigh frequency radio communications. Update 6 is also intended to incorporate

deferred software corrections carried over from Increment 3.2B developmental testing. The software-only effort may be loaded into aircraft that are receiving Increment 3.2B capability as well as those that are not. The Air Force intends to field Update 6 in 2019.
- F-22A Tactical Link 16 (TACLink) and Tactical Mandates (TACMAN) are separate pre-Milestone B hardware and software modernization programs intended to provide Link 16 transmit capability through the Multifunctional Information Distribution System/Joint Tactical Radio System and replace the legacy Mark XVII Mode 4 Identification Friend or Foe (IFF) system with the Mode 5 IFF system. The Air Force expects to field TACLink and TACMAN capabilities in FY21 and FY22, respectively.

Mission

Commanders will use units equipped with the F-22A to:
- Provide air superiority over friendly and non-permissive, contested enemy territory
- Defend friendly forces against fighter, bomber, or cruise missile attack
- Escort friendly air forces into enemy territory
- Provide air-to-ground capability for counter-air, strategic attack, counter-land, and enemy air defense suppression missions

Major Contractor

Lockheed Martin Aeronautics Company – Fort Worth, Texas

Activity
- The Air Force conducted Increment Update 5 testing in accordance with the DOT&E-approved Test and Evaluation Master Plan in 2017, which tasked the 53rd Wing to accomplish a sufficiency of test report (SOTR) following completion of developmental test.
- The Air Force completed Increment 3.2B developmental testing in August 2017. Some of the deficiencies identified in developmental testing were carried over into IOT&E, and the Air Force deferred corrective action to a future OFP effort.
- AFOTEC conducted Increment 3.2B IOT&E from August 21, 2017, through April 6, 2018. AFOTEC designed the F-22 Increment 3.2B IOT&E to determine how well the F-22A could conduct its air-to-air and air-to-ground missions. The mission-level portion of the test consisted of 18 open-air test events at the Nevada Test and Training Range (NTTR) and 49 Pilot-in-the-Loop modeling and simulation test events at the Air Combat Simulator. The Program Office intends to fix deficiencies found during 3.2B IOT&E and re-test to validate completion of corrective actions.
- The Air Force approved the Increment 3.2B Full-Rate Production decision on July 31, 2018, with projected initial fielding in mid-2019.
- DOT&E published a classified F-22 Increment 3.2B IOT&E report in August 2018. The evaluation included results from both developmental and operational testing.

Assessment
- F-22A Increment 3.2B developmental testing experienced performance shortfalls across some of the enhancement capabilities, which led to multiple unplanned OFP revisions. The Air Force deferred corrective action for some deficiencies to future software modernization efforts.
- Increment 3.2B test of the operational effectiveness and suitability was limited by the open-air test venue types and density of ground threats; lack of real time battle shaping because the Air-to-Air Range Infrastructure (AARI) instrumentation was not accredited; and lack of surrogate adversaries that adequately emulate the modern air and ground threat.
- The capabilities introduced with Increment 3.2B were integrated effectively on the F-22A and demonstrated the reliability, availability, and maintainability to be comparable to that of the F-22A operational fleet.
- The Increment 3.2B IOT&E revealed classified cyber deficiencies. Details are in the August 2018 DOT&E IOT&E report.

Recommendations

The Air Force should:
1. Provide the test infrastructure, instrumentation, and surrogate threats to conduct F-22A operational testing against an operationally realistic array of threats to fully vet F-22A and fifth generation capabilities on an appropriate open-air test range.
2. Resolve AARI sustainment, test readiness, and modernization shortfalls to support simultaneous advanced aircraft open-air mission testing on an appropriate open-air test range.
3. Accomplish additional testing and follow up as provided in the DOT&E Increment 3.2B IOT&E report.

Global Positioning System (GPS) Enterprise

Executive Summary

- The Air Force conducted developmental test and evaluation (DT&E) for all three GPS enterprise segments (space, control, and user) in 2018. DT&E included the GPS III Satellite Vehicle (SV) 01 Mission Readiness Test, Next Generation Operational Control System (OCX) Launch and Control/ Checkout System (or Block 0) testing, and Military GPS User Equipment (MGUE) Increment 1 circuit card testing.
- The Lead Developmental Test and Evaluation Organization (LDTO) has done commendable work managing the breadth of developmental testing activities, emerging test requirements (such as the OCX Block 0 cyber test), and significant changes to test plans.
- The Program Office conducted a cybersecurity test, including developmental and operational test objectives, of the OCX Block 0 baseline with a National Security Agency-certified Red Team.
- Schedule slips have caused operational testing delays for all GPS segments from dates listed in prior DOT&E Annual Reports.
- The Program Office updated the Enterprise Test and Evaluation Master Plan (ETEMP) Revision B to reflect acquisition strategy changes, capture schedule and resource changes due to segment delays, and define the initial strategy for contested space testing. DOT&E approved the ETEMP in September 2018.
- While the Air Force has made progress across the segments, significant GPS Enterprise operational risks remain:
  - Ground control delays will limit adequate and timely operational testing for the full capabilities of GPS III satellites prior to extensive procurement and incorporation of the satellites into the operational constellation.
  - GPS III lacks sufficient test resources for realistic operational space segment threat testing.
  - The MGUE program continues to face challenges implementing the new technology, resulting in repeated delays to development of final software and hardware builds by all three MGUE vendors.
  - Ongoing MGUE Lead Platform test schedule slips increase integration risks for platforms seeking to implement MGUE before Lead Platform testing is complete.

System

- The GPS enterprise is an Air Force-managed, satellite-based radio navigation system of systems that provides military and civil users accurate position, velocity, and time within the near-Earth space, Earth atmosphere, and worldwide Earth surface areas.
- The current GPS enterprise consists of three operational segments:

AFSCN – Air Force Satellite Control Network
GPS IIR – Global Positioning System (GPS) Block II "Replenishment" Satellites
GPS IIR-M – GPS Block II "Replenishment – Modernized" Satellites
GPS IIF – GPS Block II "Follow-On" Satellites
GPS III – GPS Block III Satellites

  - Space Segment – The GPS spacecraft constellation consists of satellites in semi-synchronous orbit. The Air Force has successfully launched 70 GPS satellites and currently operates 31 operational GPS satellites. The operational constellation is comprised of Block IIA (1990-1997), Block IIR (1997 2004), Block IIR-M (2005-2009), and Block IIF (2010-2016).
  - Control Segment – The GPS control segment consists of primary and backup GPS master control stations, satellite ground antennas, a pre-launch satellite compatibility station, and geographically distributed monitoring/ tracking stations. The GPS control segment includes: the Operational Control System (OCS)/Architecture Evolution Plan (AEP), which supports operations of the current satellite constellation; the Launch/Early Orbit, Anomaly Resolution and Disposal Operations (LADO) system; the Selective Availability/Anti-Spoof Module (SAASM) Mission Planning System (SMPS); and OCX Block 0, which will launch and initialize GPS III satellites.
  - User Segment – There are many versions of military GPS mission receivers fielded on a multitude of operational systems and combat platforms, including the Defense Advanced GPS Receivers and embedded Ground-Based GPS Receiver Application Modules (GB GRAM), numbering in the hundreds of thousands.
- In 2000, the Air Force initiated a GPS enterprise modernization effort to include upgrades to all three segments, along with new civil and military signals (M-code). In addition to replenishment of the satellite constellation, this modernization will improve both military and civil signal

integrity and service quality. Modernized GPS enterprise improvements include:

- Space Segment – The Air Force intends for the GPS III satellites, an Acquisition Category (ACAT) 1C program, to be capable of transmitting a fourth civil signal and higher powered M-code, as well as all legacy military and civil navigation signals of previous satellite blocks. The Air Forces plans for 10 GPS III satellites and subsequently 22 GPS III Follow-On Production (GPS IIIF) satellites, which will have enhancements such as regional military protection, laser retro-reflector arrays for better on-orbit position determination, and a redesigned nuclear detonation detection system.
- Control Segment – The Air Force plans to deliver OCX, an ACAT 1D program, in three blocks. OCX will replace OCS and LADO, be backward compatible with legacy/modernized satellites, and interface with updated SMPS versions. OCX Block 0 will launch and initialize GPS III satellites, while OCX Block 1 will command and control GPS Block II and III satellites. OCX Block 2 (now merged and scheduled concurrently with the OCX Block 1 delivery) will provide full control of modernized civil and M-code signals and navigation warfare functions. OCX is intended to provide significant cybersecurity improvements over OCS.
- User Segment – MGUE Increment 1 is an ACAT IC program and, currently, Increment 2 is a pre-Major Defense Acquisition Program. MGUE Increment 1 includes the GB-GRAM-Modernized form factor for ground and low-dynamic platforms and the GRAM Standard Electronic Module-E/Modernized for maritime and aviation applications.

• Due to delays in OCX Block 1 delivery, the Air Force initiated the GPS III Contingency Operations (COps) program as a "bridge capability" or risk mitigation effort to enable employment of GPS III satellites using legacy (pre-M-Code) signals for operational constellation sustainment until OCX is delivered. Additionally, M-Code Early Use (MCEU) will deliver early operational use of core M-Code, with full M-Code functionality delivered in OCX Block 1 and 2.

Mission

Combatant Commanders of U.S. and allied military forces use GPS to provide accurate, position, navigation, and time information to operational users worldwide. GPS also supports myriad non-military users worldwide.

Major Contractors

- Space Segment
  - Block IIR/IIR-M/III satellites: Lockheed Martin Space Systems – Denver, Colorado
  - Block IIF satellites: Boeing, Network and Space Systems – El Segundo, California
  - Block IIIF satellites: Lockheed Martin – Denver, Colorado
- Control Segment
  - OCS, COps, and MCEU: Lockheed Martin, Space Systems Division – Colorado Springs, Colorado
  - OCX: Raytheon Company, Intelligence, Information, and Services – Aurora, Colorado
- User Segment (MGUE Increment 1)
  - L3 Technologies/Interstate Electronics Corporation – Anaheim, California
  - Raytheon Company, Space and Airborne Systems – El Segundo, California
  - Rockwell Collins – Cedar Rapids, Iowa

Activity

- The Air Force conducted DT&E for all three GPS enterprise segments (space, control, and user), but did not conduct operational testing in 2018. Testing included the GPS III SV01 Mission Readiness Test, OCX Block 0 testing, and MGUE Increment 1 card testing.
- Schedule slips have caused operational testing delays for all GPS segments from dates listed in prior DOT&E Annual Reports. The Air Force plans to begin operational testing of the space, ground, and user segments in 2019.
- The Program Office updated the ETEMP Revision B to reflect acquisition strategy changes, incorporate the GPS III COps and MCEU test strategies, capture schedule and resource changes due to segment delays, and define the initial strategy for contested space testing. DOT&E approved ETEMP Revision B in September 2018.
- GPS Enterprise segment activity includes:

OCX

- The Program Office conducted a cybersecurity test, including DOT&E-approved operational cyber test objectives, of the OCX Block 0 baseline with a National Security Agency-certified Red Team. The cybersecurity test combined elements of developmental and operational cybersecurity test objectives.
- The Milestone Decision Authority approved the OCX Milestone B in September 2018.
- The Air Force Operational Test and Evaluation Center (AFOTEC) will conduct OT&E of OCX in 2023 as part of a GPS Enterprise Multi-Service OT&E (MOT&E) that will include OCX, GPS III, and MGUE. This will inform both the Positioning, Navigation, and Timing (PNT) Initial Operating Capability (IOC) as well as the Constellation Management IOC.

GPS III COps
- AFOTEC is planning operational testing of COps in October 2019, concurrent with GPS III SV01 operational tests.

MCEU
- Shortly after contract approval, the Air Force modified the contract to address M-Code "hot start" requirements for GPS receivers. Hot start is the capability of M-Code receivers to initialize legacy GPS receivers with data derived from a modernized navigation signal. Initial hot start capability only requires changes to the MGUE cards. The Program Office intends to implement an enterprise hot start capability with a more enduring, coded solution in the ground, space, and user segments.
- AFOTEC plans to conduct operational testing of MCEU in 2020.

GPS III and GPS III Follow-On Production
- The first of 10 GPS III satellites is scheduled to launch in December 2018. In August 2018, the Air Force declared the second GPS III satellite fully tested and available for launch.
- In February 2018, the Air Force released its request for proposals to acquire 22 GPS IIIF satellites. The contract was awarded to Lockheed Martin in September 2018.

MGUE
- In order to begin platform integration testing with the MGUE receiver cards, the Services have been conducting bench and chamber developmental testing activities to understand how the host applications perform under various environmental and electromagnetic conditions.
- The Program Office conducted a developmental field test of MGUE card maturity in July 2018. Test findings will inform MGUE card development and support preparations for MGUE Lead Platform developmental field testing scheduled to begin in 2019.
- MGUE Lead Platform OT&E will include data collection from separate MGUE Increment 1 Operational Utility Evaluations on the four designated Service Lead Platforms. MGUE OT&E will be followed by the GPS Enterprise MOT&E in 2023 and will include OCX, GPS III, and MGUE.
- The MGUE Increment 1 Acquisition Decision Memorandum directed the Air Force to provide the MGUE Increment 2 Acquisition Strategy, and the Air Force submitted the Increment 2 Acquisition Strategy to the Milestone Decision Authority in November 2018.

Assessment
- The Air Force has improved the GPS enterprise schedule by addressing schedule and performance risks; however, articulation of program risks with stakeholders continues to be incomplete, increasing the probability of unmitigated risks causing further program problems and delays.
- The Air Force made efforts to integrate the GPS space, ground, and user segments; however, there are still major disconnects in the synchronization of the enterprise segments due to technical problems, development delays, and a lack of integrated strategies.
- The LDTO developed an initial outline of the test strategy for contested space in the recently signed ETEMP Revision B; however, significant work needs to take place to identify specific strategies to address space threats. AFOTEC needs to develop test methodologies, operational threat scenarios, and measures for operational testing of threats against the GPS space segment.
- The LDTO managed the breadth of developmental testing activities, emerging test requirements (such as the OCX Block 0 cyber test), and significant changes to test plans.
- Assessment of the GPS Enterprise segments follows:

OCX and COps/MCEU
- Ground control delays will limit adequate and timely operational testing for the full capabilities of GPS III satellites prior to extensive procurement and incorporation of the GPS III satellites into the operational constellation.
- The OCX Program Office and LDTO leaned forward to conduct cybersecurity testing of the OCX Block 0 system. Additionally, the combined effort between developmental and operational testers provided beneficial lessons on agile, efficient testing. The testing suggested areas for needed cybersecurity hardening and the necessity to better characterize the defense posture of the full system.
- Since the 2016 Nunn-McCurdy OCX review, the Program Office has attempted to reduce future schedule risk by increasing manpower, improving system engineering and configuration management processes, and evolving its testing approach. While there has been improvement, it is unclear the Air Force has enough satellite simulator test resources to conduct developmental testing on GPS III COps and OCX in parallel, which is required to keep these programs on the current schedule.

GPS III and GPS IIIF
- GPS III lacks sufficient test resources for realistic operational space segment threat testing.
- The Program Office is planning for the GPS IIIF Non-flight Satellite Testbed (GNST+) in the GPS IIIF program; however, GNST+ will not provide full capability for realistic threat testing. The program plans to conduct environmental testing; but, it is not currently planning for sufficient test articles to support full characterization of adversary threats against the system.
- The Air Force has proposed a Milestone C decision in 2020, before any GPS IIIF satellites will be developed or tested. Additionally, the delay in publishing an enterprise strategy makes it difficult to plan for upgrades of GPS capability.

MGUE
- The MGUE program continues to face challenges implementing the new technology, resulting in repeated delays to development of final software and hardware builds by all three MGUE vendors.
- Development of "hot start" capabilities will add to MGUE cost and schedule, with each Service having differing

operational requirements that could result in varying implementation needs across the DOD.

- Due to thermal performance problems with one MGUE vendor circuit card, the Army and Marines are not planning to test that vendor card in their respective MGUE GPS Lead Platforms. This leaves only two vendor cards for testing in the ground lead weapons platforms, reducing the available comparison data from vendor card performance that the LDTO and AFOTEC will be able to provide for other DOD weapons platform integration decisions.
- Ongoing MGUE Lead Platform test schedule slips increase integration risks for platforms seeking to implement MGUE before Lead Platform testing is complete. The utility of the Lead Platforms to act as pathfinders will also diminish due to these delays. The U.S. Strategic Command (USSTRATCOM) Joint Navigation Warfare Center's expertise and assessments are an important resource for navigation warfare testing and to more broadly assess MGUE integration across the DOD operational envelope.

Recommendations

The Air Force should:

1. Comprehensively test the GPS III satellite against on-orbit threats with operationally representative test articles and simulators.
2. Leverage the USSTRATCOM Joint Navigation Warfare Center's expertise and assessments to more broadly assess MGUE integration across the DOD operational envelope.

Joint Space Operations Center (JSpOC) Mission System (JMS)

Executive Summary

- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted operational testing on the Joint Space Operations Center (JSpOC) Mission System (JMS) Increment 2, Service Pack (SP)-9 from March to May 2018.
- JMS SP-9 is not operationally effective or suitable for its Space Situational Awareness (SSA) mission.
- The JMS Program Office, developers, operators, and testers could have prevented many of the problems identified during operational testing if they better synchronized their efforts from requirements creation through system development and all stages of testing.
- The JMS Program Office placed the JMS Test and Evaluation Master Plan update for SP-11 on hold while the Air Force determines the way forward for the JMS program.
- The current SP-11 schedule is not executable because it does not incorporate time to fix SP-9 deficiencies, account for the continued resource constraints related to SP-9 and SP-11 concurrency, or address lessons from SP-9 development and testing.
- JMS will not be ready to support Space Fence operational testing or operations.

System

- The Air Force is developing JMS to process, integrate, store, and present SSA sensor data in a net-centric, service-oriented architecture of hardware, software, and network connectivity. JMS data and analysis is intended to support command and control tasking and battle-management decisions for space forces.
- The Air Force installed operational JMS hardware and infrastructure at Vandenberg AFB, California. Additional non-operational instances of JMS are installed for development and developmental testing purposes at other sites, including Vandenberg AFB, California, and Space and Naval Warfare Systems Center Pacific at the Point Loma Annex of Naval Support Center San Diego, California.
- JMS net-centric enterprise services, including data visualization, mission applications, and functional queries, are intended to be accessible to worldwide users. Users can run JMS client software on non-JMS workstations connected through the SIPRNET and the Joint Worldwide Intelligence Communication System.
- JMS is intended to replace Space Defense Operations Center (SPADOC) and space-specific portions of the Astrodynamic Support Workstation (ASW).
- The Air Force is currently developing JMS in two increments:
  - Increment 1 delivered an initial service-oriented architecture infrastructure and user tools. Tools included a User Defined Operational Picture, accessible through the client workstation, which allows analysis of data from legacy systems, integrated collaboration and data sharing tools, and space order of battle processing.
  - Increment 2 is being developed to deliver mission functionality in three Service Packs.
    - SP-7 delivered updates and additions to Increment 1-delivered hardware and software infrastructure, including servers, space surveillance network (SSN) communications services connectivity, system security and message processing capabilities, and limited space surveillance data processing and visualization tools. The Air Force operationally accepted SP-7 in 2014, but did not operationally test SP-7 because it did not replace legacy systems and was not used for mission critical functions.
    - SP-9 was intended to update and expand JMS hardware and software to perform functions currently performed by SPADOC and ASW, with improved accuracy, efficiency, and responsiveness. Those functions include administration and maintenance of the space catalog, orbit determination for resident space objects, and high-accuracy tasking of sensors for orbital safety, threat modeling, and operational decisions. However, the SP-9 Operational Utility Evaluation (OUE) was descoped twice due to capability limitations identified during developmental and operational testing. Critical issues identified during the OUE led to the test's premature conclusion in May 2018.
    - SP-11 is intended to complete Increment 2 functionality on the Secret and Top Secret enclaves. It is designed to support space object identification tasking and processing for critical events such as closely spaced satellite operations; breakups, re-entries and de-orbits; launch processing; and processing of uncorrelated tracks.

The Air Force transferred content from SP-9 and SP-13 to SP-11, adding risk to this delivery. During the JMS Critical Change in 2016, the Air Force canceled SP-13. The Key Performance Parameter requirements for SP-13 were moved to SP-11, while most of the remaining SP-13 content was deferred.

Mission

The Joint Force Space Component Commander intends to use JMS to enable the coordination, planning, synchronization, and execution of continuous, integrated space operations in support of national and Combatant Commander objectives.

Major Contractors

- Government prime contractor:
  - Air Force Space and Missile Systems Center – Los Angeles AFB, California
- System Integrator, Increments 1 and 2:
  - Space and Naval Warfare Systems Command (SPAWAR) – San Diego, California
- Increment 1 sub-contractors:
  - Polaris Alpha – Colorado Springs, Colorado
  - The Design Knowledge Company – Fairborn, Ohio
- Increment 2 sub-contractors:
  - Analytical Graphics Incorporated – Exton, Pennsylvania
  - Artificial Intelligence Solutions – Lanham, Maryland
  - Omitron – Beltsville, Maryland

Activity

- AFOTEC conducted SP-9 operational testing from March to May 2018. The Air Force ended the test earlier than planned due to significant performance problems.
- AFOTEC and the Army Research Laboratory conducted a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) from March to April 2018.
- The Air Force canceled the SP-9 cybersecurity Adversarial Assessment, originally scheduled for August 2018.
- The Program Office placed the JMS TEMP update for SP-11 on hold while the Air Force determines the way forward for the JMS program.
- It is unclear if the Air Force intends to continue with JMS development, modernize existing capabilities for extended operations, or merge SSA and command and control development into an undefined program.

Assessment

- The SP-9 OUE was adequate to determine effectiveness and suitability; however, underperforming mission functions, system instability, and poorly defined or missing requirements caused the Air Force to reduce the scope of testing twice. The system suffered from poor pre-test set-up, configuration problems, and maturity problems that reduced system performance during the test and produced invalid operational test data.
- SP-9 is not operationally effective. SP-9 cannot consistently perform basic SSA mission functions in a correct, consistent, or timely manner.
- SP-9 is not operationally suitable. SP-9 operator training and documentation are not relevant to operational tasks and workflows.
- The JMS Program Office, developers, operators, and testers could have prevented many of the problems identified during operational testing if they better synchronized their efforts from requirements creation through system development and all stages of testing. The operational units are not currently staffed to support both current operations and sustained engagement with the acquirers and developers.
- The current SP-11 schedule is not executable because it does not incorporate time to fix SP-9 deficiencies, account for the continued resource constraints related to SP-9 and SP-11 concurrency, or address lessons from SP-9 development and testing.
- JMS will not be ready to support Space Fence Increment 1 operational testing or initial operations.

Recommendations

- The Air Force should synchronize the effects of the JMS Program Office, developers, operators, and testers through all stages of system development and developmental testing to increase problem discovery before operational testing.
- If the Air Force goes forward with SP-11, it should provide additional staffing to the operational units so they can support both SP-11 development and testing while executing their operational mission. If the Air Force moves forward with another program instead of JMS or changes the JMS acquisition approach, it should still properly staff the operational units to support continued engagement between operators and acquirers.
- The Air Force should identify lessons learned and develop courses of action to avoid repeating the mistakes of SP-9 development and testing in SP-11 (or other future development).
- If the Air Force decides to go forward with SP-9, it should ensure SP-9 mission functions perform correctly, consistently, and timely, and verify the fixes with testing.
- The Program Office, in coordination with the operational units, should develop operator training and system documentation relevant to operational tasks and workflows for any delivery to operations.
- The Air Force should operationally test Space Fence, SPADOC, and ASW together to ensure the existing SSA systems and their operators can process Space Fence data correctly, consistently, and in a timely manner.

KC-46A

Executive Summary

- The KC-46 program completed flight test requirements for first aircraft delivery in June 2018. The Federal Aviation Administration (FAA) awarded the aircraft's Supplemental Type Certification in early September 2018. The Military Type Certification is still pending additional test results. Both the FAA and military certifications are required before operational crews can fly the KC-46A.
- Flight testing to certify the KC-46A aerial refueling (AR) system and the first eight aircraft for receiver operations with the KC-46A began in October 2017 and will continue into FY19.
- IOT&E is likely to start in March 2019 or later. Schedule analysis identified two key milestones affecting IOT&E start and completion: (1) completion of AR certification of the initial group of 3 to 8 receivers before the beginning of IOT&E and (2) certification of all 18 receivers planned to participate in the IOT&E.
- Air refueling operators continue to inadvertently contact receiver aircraft outside the refueling receptacle with the boom nozzle. Boeing identified the root cause as reduced visual acuity in the Remote Vision System (RVS) and implemented a software-only fix. Evaluators reviewed the effectiveness of this solution, and although the software improved a few display deficiencies, it did not provide an overall adequate solution. The potential boom strikes will likely have adverse operational affects primarily on low observable receivers.

System

- The KC-46A AR aircraft is the first increment of replacement tankers (179) for the Air Force fleet of more than 400 KC-135 and KC-10 tankers.
- The KC-46A design uses a modified Boeing 767-200ER commercial airframe with numerous military and technological upgrades, such as the fly-by-wire refueling boom, the remote air refueling operator's station, 787 cockpit displays, additional fuel tanks in the body, and defensive systems.
- The KC-46A will provide both a boom and probe-drogue refueling capabilities. The KC-46A is equipped with an AR receptacle so that it can also receive fuel from other tankers, including legacy aircraft.
- The KC-46A is designed to have significant palletized cargo and aeromedical capacities; chemical, biological, radiological, and nuclear survivability; and the ability to host communications gateway payloads.
- Survivability enhancement features are incorporated into the KC-46A design.
  - Susceptibility is reduced with an Aircraft Survivability Equipment suite consisting of Large Aircraft Infrared Countermeasures (LAIRCM), a modified version of the ALR-69A Radar Warning Receiver (RWR), and a Tactical Situational Awareness System. The suite is intended to correlate threat information from pre-flight planning, the RWR, and other on- and off-board sources, and to prompt the crew with an automatic re-routing suggestion in the event of an unexpected threat.
  - Vulnerability is reduced by adding a fuel tank inerting system and integral armor to provide some protection to the crew and critical systems.

Mission

Commanders will use units equipped with the KC-46A to perform AR to accomplish six primary missions to include nuclear operations support, global strike support, air bridge support, aircraft deployment support, theater support, and special operations support. Secondary missions will include airlift, aeromedical evacuation, emergency AR, air sampling, and support of combat search and rescue.

Major Contractor

The Boeing Company, Commercial Aircraft in conjunction with Defense, Space & Security – Seattle, Washington

Activity

- In June 2018, the KC-46 program completed flight test requirements for the first KC-46A aircraft delivery by finishing test events for the RVS and the F-16, C-17, and A-10 receivers, and KC-135 refueling the KC-46A as a receiver.

- Flight tests completed for FAA Supplemental Type Certification in September 2018 and continue for Military Type Certification, both of which are required for operational crews to fly and employ the KC-46A.
- Flight testing to certify the KC-46A AR system and the first eight aircraft for receiver operations with the KC-46A began in October 2017 and will continue into FY19.
- The KC-46A program tested the aircraft in extreme humid, cold, and hot environments with a December 2017 deployment to Guam for humid; a January 2018 deployment to Fairbanks, Alaska, for cold; and a July 2018 deployment to Yuma, Arizona, for hot.
- Boeing completed Block 30 LAIRCM flight testing at Moses Lake, Washington, in June 2018 to confirm installed system performance.
- The KC-46A program completed one test in FY18 and has planned two more tests in FY19 to assess thermal curtains for crew survivability to nuclear threats against the KC-46A.
- Air Force analyses are ongoing for the KC-46A inherent nuclear hardness to blast, radiation, flash, thermal, and electromagnetic pulse effects and to assess the ability to launch and fly a safe distance from a simulated nuclear attack.
- The Air Force completed Joint Interoperability Testing of the KC-46A communicating over Link 16 with other material assets in April 2018.
- The Air Force completed its LFT&E Consolidated report.
- Analysis of Block 30 LAIRCM testing and nuclear survivability assessment of thermal curtains is ongoing.
- The KC-46A program completed follow-on developmental testing of an RVS software-only fix in June 2018.
- Initial centerline drogue system (CDS) testing revealed deficiencies in software and hardware that resulted in unexpected disconnects during AR operations. Boeing identified the root cause and implemented new coupler tolerances and updated control software logic.

Assessment

- IOT&E is likely to start in March 2019 at the earliest. Schedule analysis identified two key milestones affecting IOT&E start and completion: (1) completion of AR certification of the initial group of 3 to 8 receiver aircraft before the beginning of IOT&E and (2) certification of all 18 receiver aircraft planned to participate in IOT&E.
- Air refueling operators continue to inadvertently contact receiver aircraft outside the refueling receptacle with the boom nozzle. Boeing identified the root cause as reduced visual acuity in the RVS and implemented a software-only fix. Evaluators reviewed the effectiveness of this solution, and although the software improved a few display deficiencies, it did not provide an overall adequate solution. The potential boom strikes will likely have adverse operational affects primarily on low observable receivers.
- After the program incorporated modifications to the CDS, testing showed improved system performance and enabled probe-equipped receiver certification testing to continue. However, the modifications did not resolve all of the problems and therefore, additional data collection and analysis are required to determine the appropriate action for problem resolution.
- Joint Interoperability Testing was successful. The KC-46A was able to communicate via Link 16 with other military assets.

Recommendation

1. The KC-46A program should consider hardware changes for the RVS to improve system visual acuity and depth perception for the air refueling operators.

Light Attack Aircraft (LAA) Program

Executive Summary
- The Air Force is leveraging the rapid acquisition authorities granted by Section 804 of the FY16 National Defense Authorization Act (NDAA) to fill the need for a low-cost, multirole aircraft in its future fleet of attack aircraft. It is evaluating non-developmental aircraft candidates to provide a cost effective Light Attack Aircraft (LAA) requiring minimal design modification.
- The Air Force intends to procure 359 aircraft for 8 operational squadrons and 3 Flying Training Units (FTUs).
- Informed by Phase I of the Light Attack Experiment (LAE) completed in August 2017, the A-29 Super Tucano and the AT-6 Wolverine were further evaluated in Phase II.
- The Air Force completed Phase II of the LAE in August 2018 after ending the flight portion in June due to an aircraft mishap.

System
- Both the A-29 Super Tucano and the AT-6 Wolverine LAA candidates are single-engine turboprop aircraft, with armaments including free-fall and laser-guided weapons, machine guns, and an electro-optical/infrared sensor operated by two aircrew members.
- The Air Force intends to procure 359 aircraft for 8 operational squadrons, and 3 FTUs using the rapid acquisition authorities granted by Section 804 of the FY16 National Defense Authorization Act (NDAA).

Mission
- Commanders intend to employ units equipped with the LAA to provide close air support, strike coordination and reconnaissance, armed reconnaissance, forward air controller airborne, and air interdiction in a permissive threat environment thereby reducing the demand for 4th and 5th generation fighters. The Air Force also expects the LAA to be used for combat search and rescue and maritime air support.
- The LAA is intended to provide a survivable, sustainable platform capable of operating with light logistical support and will be interoperable with partner nations.

Major Contractors
- Sierra Nevada Corporation and Embraer Defense and Security (A-29 Super Tucano) – Jacksonville, Florida
- Textron Aviation Defense LLC (AT-6 Wolverine) – Wichita, Kansas

Activity
- The Air Force is leveraging the rapid acquisition authorities granted by Section 804 of the FY16 NDAA to fill the need for a low-cost, multirole aircraft in its future fleet of attack aircraft. Program of Record declaration under Section 804 occurred on June 23, 2018.
- The Office of Strategic Development Planning and Experimentation (SDPE), Air Force Materiel Command, Wright Patterson AFB, Ohio, developed and conducted Phase I of an LAE campaign during August 2017. LAE Phase I included four LAA candidates.
- After Phase I of the LAE was complete, DOT&E assigned the LAA program to oversight in April 2018.
- The Air Force further evaluated the A-29 Super Tucano and the AT-6 Wolverine informed by Phase I of the two-phased LAE. LAE Phase II was a repurposed combat demonstration of suitable LAA that completed in August 2018. The operational flying portion of the LAE Phase II was terminated in June due to an aircraft mishap. Most critical objectives had been met by that time.
- As a limited participating test organization, the Air Force Operational Test and Evaluation Center developed measures of suitability, assisted in writing measures of effectiveness, created an integrated maintenance database system, trained data collectors, provided data management, collected data, made suitability observations, and computed metrics from collected data.
- The Air Force is pursuing an LFT&E waiver to full-up, system-level testing in accordance with section 2366,

title 10, U.S. Code. The Air Force proposed a series of component-level live fire testing, combined with modeling and simulation, and design analyses of both candidate aircraft as the Alternative LFT&E Strategy. The test results will inform the future contract award scheduled for September 2019.
- The Air Force has a plan and resourcing to perform the initial analysis for developmental cybersecurity test and evaluation of both aircraft in accordance with DOD policy in 2019 before contract award.
- The Air Force is planning operational cybersecurity test and evaluation in accordance with DOD policy to occur after the contract award decision in 2020 on the selected aircraft.

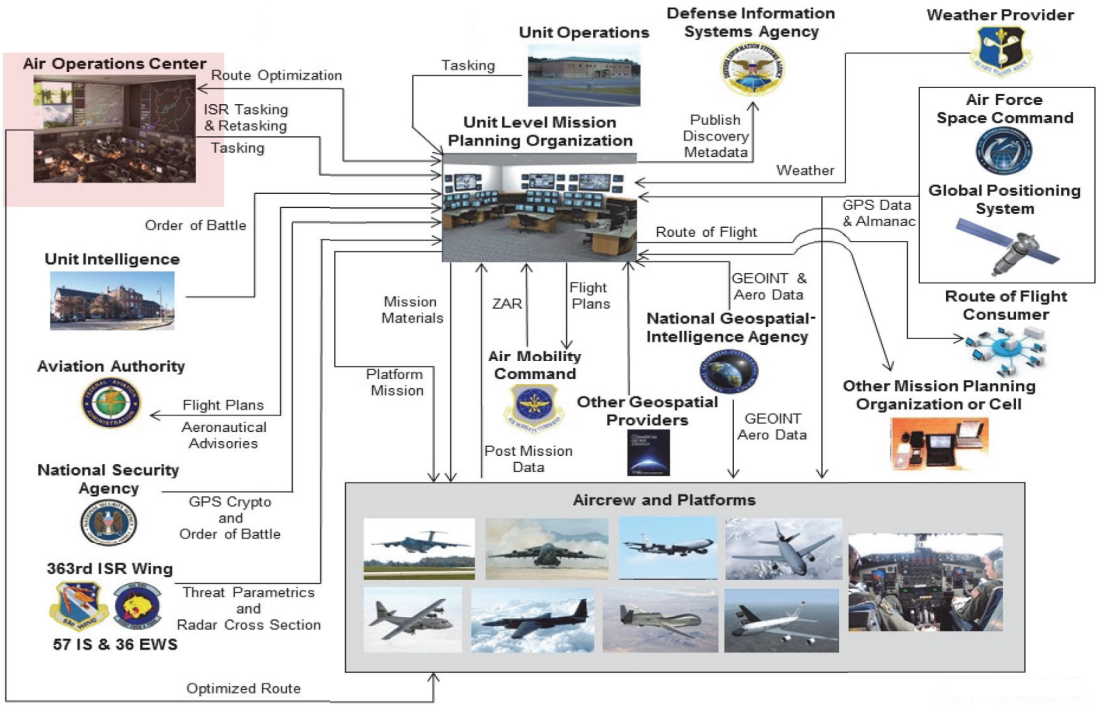
Assessment
- SDPE provided the LAE Phase I and II reports for each candidate aircraft and analysis is ongoing.
- Source selection to a single contractor is expected by September 2019.
- The Air Force has required funding in place for Program Office stand up, risk reduction activities, and other efforts leading to contract award in FY19.
- DOT&E will release an Early Fielding Report in summer 2019, which will provide an independent appraisal of capabilities, limitations, program risks, and recommendations. The nature of the LAE precludes DOT&E from formally assessing effectiveness and suitability due to the data limitations.

Recommendations
None.

Mission Planning System (MPS) / Joint Mission Planning System – Air Force (JMPS-AF)

Executive Summary

- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted the Mobility Air Forces Automated Flight Planning Service (MAFPS) IOT&E in 1QFY18. The MAFPS IOT&E exposed numerous deficiencies inherited from developmental testing that indicate system immaturity.
- The classified MAFPS functions were ready for test during the IOT&E period; however, its enclave-dependent environment and the interfaces required to implement the SIPRNET concept of operations were not ready. Therefore, additional post-IOT&E operational test and evaluation will be required to assess MAFPS classified capabilities.



Aero - Aeronautical
Crypto - Cryptology Keys
EWS - Electronic Warfare Squadron
GEOINT - Geospatial Intelligence
IS - Intelligence Squadron
ISR - Intelligence, Surveillance, and Reconnaissance
ZAR - Zone Availability Report

System

- The mission planning system (MPS) Increment (Inc) 5 is a software-only acquisition category III program consisting of common mission planning software modules for unit-level aircraft platform mission planning and centralized Air Force Mobility Air Operations Center global mobility planning and dispatching.
- MPS Inc 5 migrates Air Force airlift, tanker, airdrop, and combat search and rescue legacy mission planning platforms to the Joint Mission Planning System (JMPS).
  - JMPS software installs on standard Air Force computers with aircraft-specific Mission Planning Environments which can operate as classified or unclassified systems.
- MAFPS is one of three efforts in the MPS Inc 5 program. It replaces the legacy Advanced Computer Flight Plan (ACFP) software used by the Air Force Air Mobility Command (AMC) 618th Air Operations Center (AOC), also known as Tanker Airlift Control Center (TACC).
  - MAFPS software supports AOC-level global mission planning and route optimization for strategic airlift, aerial refueling, and tactical airlift missions.
  - MAFPS is designed to automate global mobility planning processes by integrating aircraft performance data, weather, global airspace restrictions and aeronautical charts, and geopolitical boundaries into one planning tool. MAFPS is also designed to provide optimized flight paths based on time and fuel requirements.

Mission

- AMC MAFPS force-level global mobility planning occurs worldwide at AMC-specific AOCs. For example, U.S. Transportation Command planners use MAFPS in the AOC environment then pass products to units for execution.
- At the aircraft unit level, individual aircrews or mission planning cells use MAFPS Inc 5 JMPS to optimize flight missions across the full spectrum of air missions ranging from peacetime training missions to complex combat missions.

Major Contractor

BAE Systems – San Diego, California

Activity

- AFOTEC conducted the MAFPS IOT&E from August 2017 through November 2017 in accordance with the DOT&E-approved Test and Evaluation Master Plan and the DOT&E-approved IOT&E plans.
- The classified MAFPS functions were ready for test during the IOT&E period; however, its enclave-dependent environment and the interfaces required to implement the SIPRNET concept of operations were not ready. Post IOT&E testing is required to evaluate these capabilities.
- The Air Force fielded the overall system in March 2018. The Air Force generated and fielded three continuous agile software releases since December 2017.

Assessment

- DOT&E analysis indicated numerous problems hampering effectiveness, suitability, and cybersecurity, many of which were previously documented in numerous unresolved deficiencies carried over from developmental test.
- MAFPS classified capabilities will require additional testing once these systems are ready for operation. The Air Force anticipates these capabilities will be ready for operational use in FY19.

Recommendations

The Air Force should:

1. Plan on conducting formal operational test and evaluation of MAFPS classified capabilities as soon as system readiness allows.
2. Resolve open deficiencies in MAFPS by further system development, followed by regression testing.

RQ-4B Global Hawk High-Altitude Long-Endurance Unmanned Aerial System (UAS)

Executive Summary
The Air Force Operational Test and Evaluation Center (AFOTEC) originally planned to execute an Operational Utility Evaluation (OUE) on the RQ-4B Block 30 Global Hawk Multi-Spectral (MS) – 177 system in mid-2017. However, delays to the start of the OUE occurred due to problems with weather radar testing, technical order development, and a software deficiency on a new software build that had the potential to result in loss of RQ-4B Global Hawk aircraft control while in flight. The program resolved the weather radar testing problems and completed technical order development in September 2018. Northrop Grumman modified software code to address the software deficiency and completed testing in October 2018. The OUE is planned to begin March 2019 and conclude in spring 2019.

System
- The RQ-4B Global Hawk is a remotely piloted, high-altitude, long-endurance airborne intelligence, surveillance, and reconnaissance (ISR) system that includes the Global Hawk unmanned air vehicle, various intelligence and communications relay mission payloads, and supporting command and control ground stations.
- The RQ-4B Global Hawk Block 30 system is equipped with a multi-intelligence payload that includes both the Enhanced Integrated Sensor Suite imagery intelligence payload and Airborne Signals Intelligence Payload sensor. The Air Force has retrofitted two Block 30 aircraft with the MS-177 sensor to provide high resolution MS imaging capability with accurate and automatic geolocation capabilities at high stand-off ranges.
- All RQ-4B systems use line-of-sight and beyond line-of-sight communication systems to provide air vehicle command and control and to transfer collected intelligence data to ground stations for exploitation and dissemination.
- The Air Force Distributed Common Ground System (AF-DCGS) supports ISR collection, processing, exploitation, analysis, and dissemination for the Block 30 Global Hawk system. The AF DCGS employs global communications architecture to connect multiple intelligence platforms and sensors to numerous DCGS installations where intelligence analysts produce and disseminate intelligence products.
- The Air Force has taken delivery of all 21 RQ-4B Block 30 air vehicles along with 9 Mission Control and 10 Launch and Recovery ground stations. Each Launch and Recovery ground station controls one air vehicle. The Air Force does not intend to procure any additional Mission Control or Launch and Recovery ground stations.

Mission
Commanders use RQ-4B Global Hawk reconnaissance units to provide high-altitude, long-endurance intelligence collection capabilities to support theater operations.

Major Contractor
Northrop Grumman Aerospace Systems, Strike and Surveillance Systems Division – San Diego, California

Activity
- AFOTEC originally planned to execute an OUE on the RQ-4B Block 30 Global Hawk MS-177 system in mid-2017. However, delays to the start of the OUE occurred due to problems with weather radar testing, technical order development, and a software deficiency on a new software build that occurred during ground testing of the RQ-4B Global Hawk Battlefield Airborne Control Network (BACN) aircraft. The software deficiency could result in loss of RQ-4B Global Hawk aircraft control while in flight. This same software is utilized for the RQ-4B Global Hawk MS-177 aircraft. The program completed technical order development in September 2018.
- Northrop Grumman modified the software code to address the software deficiency. The 53rd Test and Evaluation Group,

Detachment 2 observed system integration laboratory testing and developmental ground and flight tests in October 2018, and witnessed that the software deficiency, which could cause loss of aircraft control, was mitigated by the new software code.

- The program addressed three weather radar deficiencies associated with the KVM switch that were identified by the 53rd Test and Evaluation Group, Detachment 2 while conducting a Force Development Evaluation from July through August 2017. The program accomplished the following:
  - Relocated the switch to facilitate pilot access.
  - Modified the switch button logic, due to the need for pilots to display the weather radar information while manipulating the SIPRNET functions simultaneously.
  - Moved switch power access to reduce time required for operators and maintenance to recycle power when necessary.
- The OUE is planned to begin in March 2019 and conclude in spring 2019.

Assessment

- The 53rd Test and Evaluation Group, Detachment 2 validated the KVM switch modifications as adequate in March 2018. DOT&E concurs with this assessment.
- The 53rd Test and Evaluation Group, Detachment 2 validated the adequacy of the software modification addressing the potential loss of aircraft control deficiency as adequate in October 2018. DOT&E concurs with this assessment.

Recommendation

1. The Air Force should conduct operational testing of the MS-177 system to evaluate operational effectiveness, suitability, and mission capability

Small Diameter Bomb (SDB) II

Executive Summary

- The Small Diameter Bomb (SDB) II developmental testing is complete. Operational and live fire testing is ongoing. The Air Force completed Government Confidence Testing (GCT) in May 2018. The Air Force awarded the Low-Rate Initial Production Lot 4 contract for 660 weapons (570 Air Force, 90 Navy) in January 2018.
- The SDB II has demonstrated the Normal Attack (NA) mode, the primary employment method for the SDB II, against moving targets, but has had difficulty hitting static targets. Software changes have shown improvements against static targets, but are not fully validated. The Air Force successfully demonstrated Coordinate Attack (CA) and Laser Illuminated Attack (LIA) in 2017, and verified CA and LIA enhancements and corrections during GCT in 2018.
- The program implemented corrective actions and fixes for all failure modes discovered in developmental test and GCT. The program discovered six anomalies in GCT, identified and implemented a fix for five, and awaits the opportunity to test new software to address the sixth during operational test.
- The Air Force began IOT&E in June 2018 with an adequately resourced test program.

System

- The SDB II is a 250-pound, air-launched, precision-glide weapon that uses deployable wings to achieve standoff range. F-15E aircraft employ SDB IIs from the BRU-61/A four weapon carriage assembly.
- The Air Force directed design of the SDB II to provide the capabilities deferred from SDB I. It includes a weapon datalink allowing for post-launch tracking and control of the weapon, as well as a multi-mode seeker to provide the ability to strike mobile targets in adverse weather.
- The SDB II combines Millimeter-Wave radar, imaging infrared, and laser-guidance sensors in a terminal seeker, in addition to a GPS and an Inertial Navigation System, to achieve precise guidance accuracy in adverse weather.
- It incorporates a multi-function warhead (blast, fragmentation, and shaped charge jet) designed to defeat armored and non-armored targets. The weapon can be set to initiate on impact, at a preset height above the intended target, or in a delayed mode.
- There are three principal attack modes: NA, LIA, and CA. The SDB II is used against moving or stationary targets using its NA (radar/infrared sensors) or LIA modes, and stationary targets with its CA mode.
- The SDB II is designed to provide increased weapons load per aircraft and reduce collateral damage while achieving kills across a broad range of target sets by precise accuracy, small warhead design, and focused warhead effects.
- An SDB II-equipped unit or Joint Terminal Attack Controller (JTAC) will engage targets in dynamic situations and use a weapon datalink network to provide in-flight target updates, in-flight retargeting, weapon in-flight tracking, and, if required, weapon abort.

Mission

Combatant Commanders will use units equipped with the SDB II to attack stationary and moving ground and littoral targets in adverse weather conditions at standoff ranges.

Major Contractor

Raytheon Missile Systems – Tucson, Arizona

Activity

- As of May 2018, the Air Force completed 19 NA, 3 CA, 4 LIA Guided Test Vehicles (GTV) (including 4 repeats) and 9 NA, 3 CA, and 2 LIA Live Fire (LF) tests (including 4 repeats) against moving and stationary targets as part of contractor-led developmental testing. Of those events, the Air Force conducted 7 GTV and 6 LF tests with ultrahigh frequency (UHF) weapon data link (WDL) updates, and 12 GTV and 7 LF test shots were conducted with Link 16 WDL updates. NA is the primary employment method for the SDB II.
- The Air Force completed a government-managed 28-shot NA mode GCT program in May 2018, which tested the weapon in more operationally realistic environments with more operationally representative hardware and software. During GCT, the Air Force dropped all 31 available weapons

(28 planned plus 3 spare weapons); 29 were NA, and 1 each were CA and LIA. Results were 25 successes and 6 failures.
- The GCT events incorporated more operationally realistic employment challenges, to include:
  - GPS degradation and denial
  - JTAC controlled weapons
  - Various on- and off-board airborne targeting systems
  - Simple denial and deception measures
  - In-flight retargeting
  - Maneuvering and stop/start motion by targets
  - Higher clutter environments, including more decoy or confuser targets to stress the classification feature
- During GCT, the Air Force accomplished one successful employment against a maritime target and two successful ripple releases (dropping two bombs in rapid succession against different targets).
- The Program Office completed 20 rounds of seeker Captive Flight Tests (CFTs), resulting in over 2,260 target runs in a wide variety of terrain and environmental conditions. These tests logged over 483 hours of seeker operation without a single failure.
- The program has augmented and refined the Integrated Flight System (IFS) model by incorporating the results of the 2,260 CFT runs as well as weapon flight tests. Raytheon released its IFS model verification and validation report in July 2017, and the Air Force Operational Test and Evaluation Center expects to give initial accreditation prior to completion of operational testing.
- The Program Office completed over 2,000 hours of ground reliability testing and over 2,320 hours of in-flight captive carry reliability testing (CCRT). The CCRT program is complete; however, captive hours will continue to be collected during the Production Reliability Incentive Program (PRIDE) beginning with Lot 2 production-representative assets.
- The program redesigned the Air Turbine Alternator (ATA), which provides power to the SDB II fuse, to address a deficiency identified during a captive flight test failure. Regression testing is nearing completion. At least 10 weapons incorporating the new ATA will be available and employed during IOT&E.
- The Air Force commenced operational test flights on June 4, 2018. It has released 31 weapons to date including 21 NA, 3 CA, and 7 LIA missions. Six NA missions and one CA mission were unsuccessful in hitting the intended target as planned. All other NA and CA missions resulted in direct hits on their targets and the LIA missions all resulted in weapons hitting the weapon controller's laser spot. The causes of the six NA and one CA unsuccessful missions were:
  - A mission planning error preventing the weapon from receiving inflight target updates
  - Incorrect WDL keys preventing the weapon from receiving IFTUs and having the target in the seeker field of view
  - An electrical transient resulting in uncontrolled flight of the weapon
  - Corrupted IFTUs resulting in the target being outside of the seeker field of view
  - On the CA mission, the Height of Burst (HOB) sensor did not function because the seeker dome cover is believed to have contacted the dome after jettison causing damage and preventing the seeker from functioning properly
  - Two NA missions remain under review
- The Air Force awarded the Low-Rate Initial Production Lot 4 contract in January 2018 for 660 weapons (570 Air Force, 90 Navy).
- The Air Force conducted all testing in accordance with the DOT&E-approved Milestone C Test and Evaluation Master Plan.

Assessment
- In the NA mode, the SDB II successfully engaged both moving and stationary targets, including proper classification of target type (wheeled versus tracked) on 19 of 22 GTV flight tests (including GCT); 3 events had failures. The program has implemented corrective actions and fixes for all failure modes discovered in test.
- In the CA and LIA modes, the program adequately addressed the two failure types found in the CA mode, as demonstrated in test. During GCT, the program conducted two successful LIA tests against moving targets with new weapon software and successfully tested new capability in a CA test and a LIA test using a ground-based laser against a fixed target.
- Early phases of operational testing have been largely successful, with one mission failure prompted by a mission planning error and two possible reliability failures, which are under technical review. The challenges with mission planning appeared during developmental test and became manageable with time and experience, but with one attributable failure already in operational test, mission planning will remain an emphasis item.
- The Air Force has employed a total of 101 SDB IIs during testing to date. Seventy-one weapons have been successful in terms of Free Flight Reliability, with 19 failures and one no test. Ten weapons have not yet been formally adjudicated. The resulting reliability level of 0.79 is slightly below the 0.80 level required by the end of IOT&E, and is moderately below the 0.85 level required by the end of Lot 2 in September 2018. Delays in entering IOT&E are due to the steady rate of discovering new failure modes in GCT, which resulted in the lower than required reliability rates and implies the weapon was not yet fully mature.
- The program has thoroughly implemented corrective actions and fixes for all failure modes discovered in developmental test. A fix implemented after a failure in October 2014 may have failed to correct the root cause because a recent operational test failure appears to have the same failure mode. Otherwise, there have been no failures to date of components or software for which a fix has already been implemented. Reliability improved modestly from developmental test which produced a figure of 0.74 (28/38) compared to GCT which demonstrated 0.81 (26/32). Initial operational test results show 17 free flight reliability successes in 20 attempts (0.85), providing an acceptable point estimate for reliability, but

this current figure is insufficient to state with confidence that reliability will meet final requirements.

- The Air Force discovered six anomalies during GCT. These include: a software coding error that has been fixed and tested; a maritime target problem; three anomalies related to employment against static targets, which were successfully addressed in a final weapon software version tested prior to IOT&E; and a cracked seeker dome that prevented the seeker from operating properly. The seeker dome cover appears to have contacted the seeker dome after jettison, resulting in damage to the dome.
- The SDB II continues to perform well against moving targets in the NA mode. Difficulties against static targets in some conditions have been addressed with a combination of software improvements and modified employment procedures first implemented at the end of GCT. Initial results are promising but require further testing in operational test to confirm.
- Continued comparisons of the IFS model pre- and post-flight predictions indicate the model is adequate for the kinematics flown in flight test to date. Raytheon Missile Systems continues to develop and update the IFS model, which will be essential to the assessment of the results of live fire and operational testing. IFS, in combination with lethality and free flight reliability data, will produce single shot kill probability values needed to assess end-to-end weapon effectiveness against a range of operationally relevant targets.

Recommendations

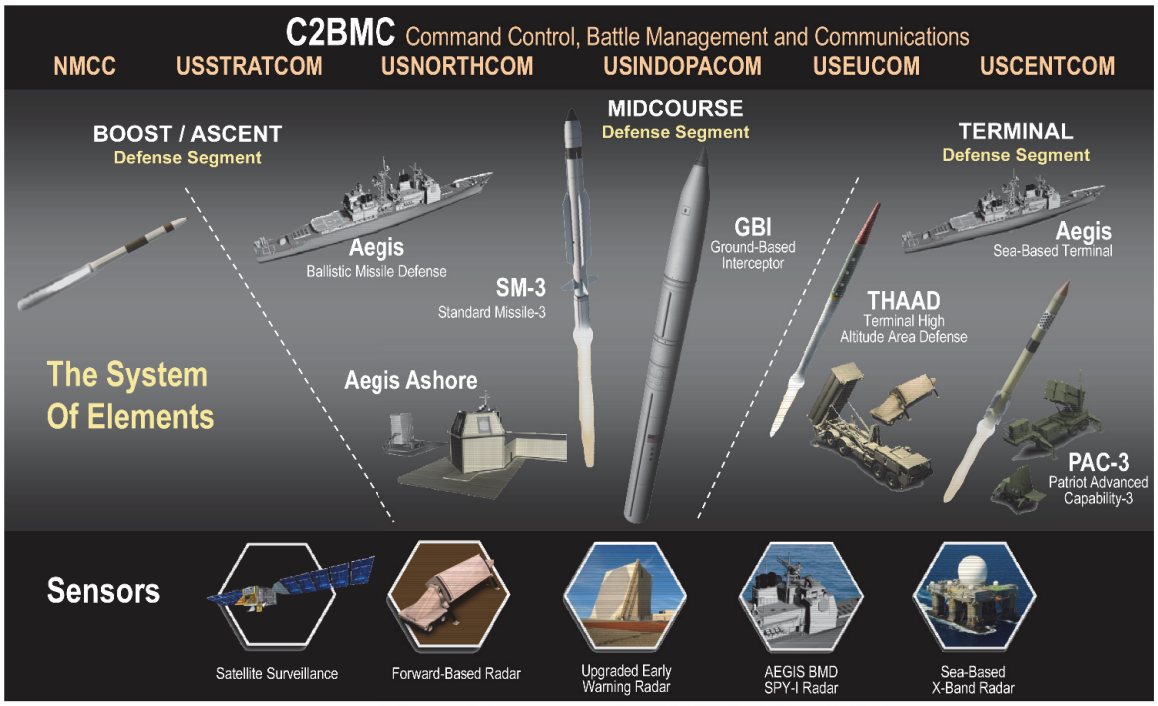
The Air Force should:

1. Re-fly the two failed GCT maritime missions during the operational test period to better characterize weapon performance against the maritime target category.
2. Examine opportunities during operational testing to eliminate possible redundancy with tests successfully completed in GCT.
3. Maximize the number of GCT and operational test shots used to validate the IFS in order to improve its overall performance.

Ballistic Missile Defense Systems

Ballistic Missile Defense Systems

Ballistic Missile Defense System (BMDS)



NMCC – National Military Command Center
USSTRATCOM – U.S. Strategic Command
USNORTHCOM – U.S. Northern Command
USINDOPACOM – U.S. Indo-Pacific Command
USEUCOM – U.S. European Command
USCENTCOM – U.S. Central Command

Executive Summary

- The Ground-based Midcourse Defense (GMD) element has demonstrated capability to defend the U.S. Homeland from a small number of intermediate-range ballistic missile (IRBM) and intercontinental ballistic missile (ICBM) threats with simple countermeasures when the Homeland Defense Ballistic Missile Defense System (BMDS) employs its full architecture of sensors and command and control.
- The Regional/Theater BMDS demonstrated a capability to defend the U.S Indo-Pacific Command (USINDOPACOM), U.S. European Command (USEUCOM), and U.S. Central Command (USCENTCOM) areas of responsibility for small numbers of medium-range ballistic missile and IRBM threats (1,000 to 4,000 km), and a capability for short-range ballistic missile threats (less than 1,000 km range).
- The Missile Defense Agency (MDA) has improved its modeling and simulation (M&S) capability over the last 2 years; however, the MDA currently does not have sufficient independently accredited M&S to enable a quantitative evaluation of BMDS operational effectiveness and interoperability.
- Over FY18, the MDA Director emphasized three guiding principles to the agency, enabling significant progress across multiple fronts:
  - Transparency and inclusion of DOT&E, and other interested organizations, in all test meetings from preliminary concept to execution, and at all levels of the MDA.
  - Importance of verification, validation, and independent accreditation of M&S.
  - Improving the cybersecurity posture of BMDS assets by conducting comprehensive, robust cybersecurity assessments and remediation of deficiencies identified in test.

System

The BMDS is a geographically distributed system of systems that relies on element interoperability and warfighter integration for operational capability and efficient use of guided missile/interceptor inventory. The BMDS includes five elements: four combat systems and one sensor/command and control architecture.

- Combat systems – GMD, Aegis Ballistic Missile Defense (BMD)/Aegis Ashore Missile Defense System (AAMDS), Terminal High Altitude Area Defense (THAAD), and Patriot.
- Sensor/command and control architecture.
  - Sensors – COBRA DANE radar, Upgraded Early Warning Radars (UEWRs), Sea-Based X-band (SBX) radar, AN/TPY-2 radars (Forward-Based Mode (FBM) and THAAD Mode (TM)), Aegis AN/SPY-1 radar aboard Aegis BMD ships, and the Space Based Infrared System (SBIRS).
  - Command and control – Command and Control, Battle Management, and Communications (C2BMC), including the BMDS Overhead Persistent Infrared Architecture (BOA).

FY18 BALLISTIC MISSILE DEFENSE SYSTEMS

Mission
- U.S. Northern Command (USNORTHCOM), USINDOPACOM, USEUCOM, and USCENTCOM employ the assets of the BMDS to defend the United States, deployed forces, and allies against ballistic missile threats of all ranges.
- The U.S. Strategic Command (USSTRATCOM) synchronizes operational-level global missile defense planning and operations support for the DOD.

Major Contractors
- The Boeing Company
  - GMD Integration: Huntsville, Alabama
- Lockheed Martin Corporation
  - Aegis BMD, AAMDS, and AN/SPY-1 radar: Moorestown, New Jersey
  - C2BMC: Huntsville, Alabama, and Colorado Springs, Colorado
  - SBIRS: Sunnyvale, California
  - THAAD Weapon System and Patriot Advanced Capability-3 Interceptors: Dallas, Texas
  - THAAD Interceptors: Troy, Alabama
  - Patriot Missile Enhancement Segment Interceptors: Dallas, Texas
- Northrop Grumman Corporation
  - GMD Booster Vehicles: Chandler, Arizona
  - GMD Fire Control and Communications: Huntsville, Alabama
  - BOA: Boulder, Colorado; Colorado Springs, Colorado; and Azusa, California
- Raytheon Company
  - GMD Exo-atmospheric Kill Vehicle and Standard Missile-3/6 Interceptors: Tucson, Arizona
  - Patriot Weapon System including Guidance Enhanced Missile-Tactical interceptors, AN/TPY-2 radar, COBRA DANE radar, SBX radar, and UEWRs: Tewksbury, Massachusetts

---

Activity
- The MDA conducted a yearlong test program review resulting in an updated Integrated Master Test Plan (IMTP). DOT&E was included in all planning events and approved the final product.
- During FY18, the MDA did not conduct BMDS-level intercept flight tests, but did execute five element-level intercept flight tests, five ground tests, five cybersecurity Cooperative Vulnerability and Penetration Assessments (CVPAs), three cybersecurity Adversarial Assessments (AAs), two Air Force ICBM reliability and sustainment flight tests, and three individual element data collection flight tests. See the BMDS element articles (pages 205 through 220) for reporting on these tests.
- The MDA conducted numerous wargames and exercises designed to enhance Combatant Command BMD readiness and increase Service member confidence in the deployed elements of the BMDS.
- The MDA initiated development of a BMDS-wide Hypersonic Defense program, which includes near-term capability upgrades, technology development, test planning, and demonstrations over the next several years.
- The MDA conducted CVPAs for the following BMDS assets:
  - X-band radar (XBR) portion of the SBX sensor in October 2017 (limited CVPA).
  - USCENTCOM AN/TPY-2 (FBM) in January 2018.
  - THAAD 3.0 (including the AN/TPY-2 (TM) radar) in March 2018.
  - USEUCOM C2BMC S8.2-3 and BOA 6.1 in July 2018.
  - USEUCOM AN/TPY-2 (FBM) radar in September 2018.
- The MDA conducted the agency's first AAs in FY18: USEUCOM C2BMC S6.4 in March 2018, THAAD 3.0 (including the AN/TPY-2 (TM) radar) at White Sands Missile Range, New Mexico, in April 2018, USEUCOM C2BMC S8.2-3 in September 2018, BOA 6.1 in September 2018, and USEUCOM AN/TPY-2 (FBM) in September 2018.
- In FY18, the MDA established standing ground rules to enable future Persistent Cyber Operations.
- The MDA continues to pursue and resource efforts to resolve major limitations that have prohibited independent M&S accreditation in the past.

Assessment
- Previous BMDS-level assessments for Homeland and Regional/Theater Defense remain unchanged:
  - GMD has demonstrated capability to defend the U.S. Homeland from a small number of IRBM or ICBM threats with simple countermeasures when the Homeland Defense BMDS employs its full architecture of sensors and command and control.
  - The Regional/Theater BMDS demonstrated a capability to defend the USINDOPACOM, USEUCOM, and USCENTCOM areas of responsibility for small numbers of MRBM and IRBM threats (1,000 to 4,000 km), and a capability for short-range ballistic missile threats (less than 1,000 km range).
- The process used by the MDA to update the IMTP during FY18 was rigorous, transparent, and inclusive of all MDA-internal and DOD-external stakeholders. It produced the most technically comprehensive and DOD-wide coordinated IMTP to date. It is traceable to MDA program priorities, which are:
  - Focus on increasing system reliability to build warfighter confidence.

  - Increase engagement capability and capacity.
  - Rapidly address the advanced threat.
- The MDA continues to make progress characterizing the cybersecurity posture of fielded and soon-to-be fielded BMDS Increment 4 and 5 capabilities. Additional CVPAs and AAs are required to support a comprehensive cybersecurity assessment of BMDS network and system cybersecurity and to inform future increment deliveries.
  - All cybersecurity assessments in FY18 identified cybersecurity findings (see the classified DOT&E "FY18 Assessment of the BMDS," to be published in February 2019). The MDA began to implement more structured cybersecurity test planning activities, and addressed some of the FY17 assessment shortfalls. More deliberate and detailed planning per element is needed to enable strategic cybersecurity assessments across both developmental and operational testing and to ensure findings are applied to future engineering cycles.
  - AAs in FY18 identified ways to improve THAAD, C2BMC, BOA, and AN/TPY-2 (FBM) network defense operations and capabilities in a cyber-contested environment. The GMD program has not yet conducted an AA.
  - The MDA improved upon identifying limitations in advance of testing and should work to implement mitigation strategies for deficiencies identified in FY18 assessments.
- The number of M&S accredited has steadily risen over the last 2 years. While full performance assessments are still not possible, the functional aspects of BMDS performance that can be assessed with independently accredited M&S continue to grow. Concurrently, the MDA is redesigning the process for conducting ground tests with the intent to respond more quickly to Combatant Command needs and evolving threats. While the traditional process does not ensure adequate time for independent M&S verification, validation, and accreditation (VV&A), the MDA is working with OTA to develop VV&A methodologies and data sources to support accreditation.

Recommendations

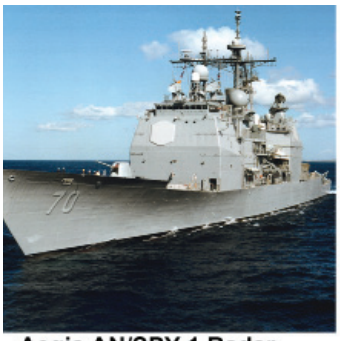
The MDA should:

1. Continue to use the IMTP update process initiated during FY18.
2. Address findings from cybersecurity assessments.
3. Enable Persistent Cyber Operation assessments of BMDS assets in each Combatant Command and of MDA networks and systems.
4. Integrate DT&E into all cybersecurity assessment planning, to enable discovery and remediation of cybersecurity findings prior to OT&E.
5. Design ground test schedules to account for accreditation timelines. If the ground test results are critical to making technical baseline and fielding decisions, the selection of such decision dates should also consider the availability of accredited models to perform the assessment.

Sensors / Command and Control Architecture

Executive Summary

- The Missile Defense Agency (MDA) continued to mature the Ballistic Missile Defense System (BMDS) sensors/ command and control architecture during 23 flight tests, ground tests, and cybersecurity assessments.
- The MDA delivered the first instantiation of the BMDS Overhead Persistent Infrared Architecture (BOA) and tested an updated version of the BMDS mission planner.
- The MDA completed the final design of the Long-Range Discrimination Radar and initiated the Homeland Defense Radar – Hawaii program.
- The MDA conducted threat-realistic cybersecurity testing on Command and Control, Battle Management, and Communications (C2BMC), AN/TPY-2 radar, and Sea-Based X-band (SBX) radar, improving the ability of these systems to withstand cybersecurity attacks.


Aegis AN/SPY-1 Radar


AN/TPY-2


Cobra Dane


C2BMC


UEWR


SBIRS


Sea-Based X-band Radar

C2BMC - Command and Control, Battle Management and Communications
SBIRS - Space-Based Infrared System
UEWR - Upgraded Early Warning Radars

System

- The BMDS sensors are systems that provide real-time ballistic missile threat data to the BMDS. The Services use the data to counter ballistic missile attacks. The Army, Navy, Air Force, and the MDA operate the sensor systems.
  - The COBRA DANE radar is a fixed site, L-band phased array radar operated by the Air Force and located at Eareckson Air Station (Shemya Island), Alaska.
  - The Upgraded Early Warning Radars (UEWRs) are fixed site, ultrahigh frequency radars, operated by the Air Force located at Beale AFB, California, and Thule Air Base, Greenland. A third radar is operated by the Royal Air Force (RAF) with Air Force liaisons on site at RAF Fylingdales in the United Kingdom. The MDA and Air Force Space Command are also upgrading the Clear Air Force Station, Alaska, Early Warning Radar and the east coast Early Warning Radar at Cape Cod Air Force Station, Massachusetts.
  - The SBX radar is a mobile, phased array radar operated by the MDA and located aboard a twin-hulled, semi-submersible, self-propelled, ocean-going platform.
  - The AN/TPY-2 Forward-Based Mode (FBM) radar is a transportable, single-face, X-band phased array radar commanded and tasked by the C2BMC, and located at sites in Japan, Israel, Turkey, and the U.S. Central Command (USCENTCOM) area of responsibility.
  - The Space-Based Infrared System (SBIRS) is a satellite constellation of infrared sensors operated by the Air Force with external interfaces to the BMDS located at Buckley AFB, Colorado, and Schriever AFB, Colorado.
  - The list of BMDS sensors also includes the Aegis AN/SPY 1 radar. See the Aegis Ballistic Missile Defense (BMD) article (page 215) for reporting on this sensor.
- The C2BMC system is a Combatant Command interface to the BMDS and the integrating element within the BMDS. C2BMC workstations are fielded at U.S. Strategic Command, U.S. Northern Command (USNORTHCOM), U.S. European Command (USEUCOM), U.S. Indo-Pacific Command (USINDOPACOM), and USCENTCOM; numerous Army Air and Missile Defense Commands; Air and Space Operations Centers; Maritime Operation Centers; and other supporting warfighter organizations.
  - The current C2BMC provides Combatant Commands and other senior national leaders with situational awareness of BMDS status, system coverage, and ballistic missile tracks.

- The C2BMC also provides a consolidated upper echelon BMD mission plan at the Combatant Command and component level.
- The C2BMC suite provides command and control for the AN/TPY-2 (FBM) radar as well as track reporting to support weapon system cueing and engagement operations.
- BOA is a system within the C2BMC enterprise that receives raw infrared sensor information on boosting and midcourse ballistic objects and feeds that track data to C2BMC (S8.2-1 and beyond) for use in cueing BMDS sensors and weapon systems, and for situational awareness.
- Using the BMDS Communications Network, the C2BMC forwards AN/TPY-2 (FBM) and AN/SPY-1 tracks to Ground-based Midcourse Defense (GMD). C2BMC uses the Tactical Digital Information Link-Joint message formats to send C2BMC system track data to Aegis BMD, Terminal High-Altitude Area Defense (THAAD), Patriot, and coalition systems for sensor cueing and engagement support.

Mission

- Combatant Commands integrate the BMDS sensors and C2BMC with other BMDS elements to intercept ballistic missile threats that target the United States and U.S. allies.
  - Combatant Commands use the BMDS sensors to detect, track, and classify/discriminate ballistic missile threats.
  - Combatant Commands use C2BMC for deliberate and dynamic planning; situational awareness; track management; AN/TPY-2 (FBM) sensor management and control; engagement support and monitoring; data exchange between C2BMC and BMDS elements; and network management.

Major Contractors

- COBRA DANE Radar
  - Raytheon Company, Intelligence, Information, and Services – Dulles, Virginia
- UEWRs
  - Raytheon Company (Prime), Integrated Defense Systems – Tewksbury, Massachusetts
  - Harris Corporation/Exelis (Sustainment) – Colorado Springs, Colorado
- SBX and AN/TPY-2 (FBM) Radars
  - Raytheon Company, Integrated Defense Systems – Tewksbury, Massachusetts
- SBIRS
  - Lockheed Martin Corporation, Space Systems – Sunnyvale, California
- C2BMC
  - Lockheed Martin Corporation, Rotary and Mission Systems – Huntsville, Alabama, and Colorado Springs, Colorado
- BOA
  - Northrop Grumman Corporation – Boulder, Colorado; Colorado Springs, Colorado; and Azusa, California

---

Activity

- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- The MDA fielded BOA 5.1 in January 2018 and SBX X-band Radar (XBR) 3.3.4 in July 2018.
- The MDA completed the Final Design Review for the Long-Range Discrimination Radar in September 2018.
- During FY18, the MDA used the sensors and the command and control architecture in five intercept flight tests, five ground tests, five cybersecurity Cooperative Vulnerability and Penetration Assessments (CVPAs), three cybersecurity Adversarial Assessments (AAs), two Air Force intercontinental ballistic missile (ICBM) reliability and sustainment flight tests, and three individual element data collection flight tests.

Intercept Flight Tests

- The MDA and Navy conducted:
  - Navy fleet exercise Formidable Shield 17 (FS-17) in October 2017. FS-17 included an Aegis BMD intercept of a ballistic missile target as well as simulated intercepts.
  - Flight Test, Standard Missile-29 (FTM-29) in January 2018. The Aegis Ashore Missile Defense Test Facility attempted an engage-on-remote intercept using data from the AN/TPY-2 (FBM) CX3.0.0 Early Release (ER) radar. A Standard Missile-3 (SM-3) Block IIA guided missile failure precluded an intercept.
  - Navy fleet exercise Pacific Dragon 18 in August 2018.
  - Japanese Flight Test Mission-05 (JFTM-05) Event 1 and 2 in September 2018. A Japanese destroyer using a SM-3 Block IB guided missile intercepted a short-range ballistic missile target during Event 2; the destroyer conducted a simulated engagement of a short-range ballistic missile target during Event 1.
  - Software configurations for these tests were:

FLIGHT TEST	C2BMC	BOA	SBIRS	UEWR	AN/TPY-2 (FBM)
FS-17	S6.4-3		17-1	8.4.2	
FTM-29	S8.2-1	5.1	17-1		CX-3.0.0 ER
Pac Dragon 18	S8.2-1	5.1	17-1		
JFTM-5 Event 1	S8.2-1	5.1	17-1		
JFTM-05 Event 2	S8.2-1	5.1	17-1		

ER – Early Release

Ground Tests

- The MDA conducted:
  - Hardware-in-the-Loop GT in November 2017. The ground test assessed BMDS Capability Increment 4 functionality against ICBM threats and aided USNORTHCOM doctrine development.
  - Ground Test, Integrated-07b (GTI-07b) USEUCOM/USCENTCOM in April and May 2018. The ground test assessed European Phased, Adaptive Approach Phase 3 and BMDS Capability Increment 5 functionality in USEUCOM and USCENTCOM regional/theater scenarios.
  - GTI-18 Sprint 1 in April 2018. The ground test assessed the functionality of the U.S. Forces, Korea (USFK) Joint Emergent Operational Need (JEON) Phase 2 architecture.
  - GTI-18 Sprint 2 in July 2018. The ground test supported Aegis Baseline 9.C2 testing for modeling and simulation verification, validation, and accreditation prior to its Operational Capacity Baseline decision as well as system assessment for GMD Ground Systems 7A.0.1.1.
  - Ground Test, Distributed-07b (GTD-07b) USEUCOM/USCENTCOM in August and September 2018. The test used a distributed environment to assess BMDS performance in USEUCOM and USCENTCOM regional/theater defense, and to support deployment of the BMDS Capability Increment 5 functionality.
  - Software configurations for these tests were:

GROUND TEST	C2BMC	BOA	SBIRS	CD	UEWR	SBX XBR	AN/TPY-2 (FBM)
HWIL GT	S8.2-1		17-1	2.7.1.2	9.0.7/8.4.2	3.3.3	CX-2.1.1
GTI-07b (E/C)	S8.2-3 ER	6.1 ER	17-1				CX-3.0.0 ER
GTI-18 Sprint 1	S8.2-1	5.1/6.1 ER	17-1				CX-2.1.1
GTI-18 Sprint 2	S8.2-3 ER	6.1 ER	17-1	2.7.1.2	9.0.7	3.3.5 ER	CX-3.0.0
GTD-07b (E/C)	S8.2-3 ER	6.1 ER	17-1				CX-3.0.0

CD – Cobra Dane; E/C – U.S. European Command/U.S Central Command; ER –Early Release

CVPAs

- The Research Development and Engineering Command (RDECOM) Survivability/Lethality Analysis Directorate (SLAD), in support of the MDA, conducted:
  - XBR 3.3.x portion on the SBX in October 2017 (limited CVPA).
  - AN/TPY-2 (FBM) CX 2.1 radar in January 2018.
  - AN/TPY-2 (Terminal Mode (TM)) CX 2.1 radar in March 2018.
  - C2BMC S8.2-3 ER and BOA 6.1 ER in July 2018.
  - AN/TPY-2 (FBM) CX 3.0 ER in September 2018.

Adversarial Assessments (AAs)

- The Army Threat Systems Management Office, in support of the MDA, conducted:
  - C2BMC S6.4 (USEUCOM) in March 2018.
  - AN/TPY-2 (TM) CX 2.1 in April 2018.
  - C2BMC S8.2-3 ER, BOA 6.1 ER, and AN/TPY-2 (FBM) CX 3.0 ER in September 2018.

Air Force ICBM Reliability and Sustainment Flight Tests

- The Air Force conducted:
  - Glory Trip-226 (GT-226) in April 2018 and GT-224 in May 2018, using the SBX radar and overhead sensors. The Air Force was unable to complete GT-225 in July 2018 due to a missile failure.

Data Collection Flight Tests

- The MDA conducted:
  - A classified Cobra Dane/UEWR data collection event.
  - Flight Test, Other-33 (FTX-33) in March 2018. The test was an AN/SPY-6 developmental radar test, which included participation by SBIRS and overhead sensors.
  - Sensors-18 (SN-18) element test of the AN/TPY-2 (FBM) radar in May 2018 with a follow-on hardware-in-the-loop portion in August 2018. The test assessed electronic protection capabilities and supported further electronic protection development.
- In August 2018, the MDA tested the C2BMC S8.2-3 BMDS Planner in an USEUCOM planning exercise.
- The Army completed an urgent materiel release (conditional) in August 2018 for the AN/TPY-2 (FBM) CX 3.0 radar. The MDA and Army intend to close all remaining materiel release conditions for software version CX 2.1.0 and the electronic equipment unit x86 computer processor in 2019, and all conditions for software version CX 3.0 in 2020.

Assessment

- During FY18 testing, extensive sensor and command and control data were collected supporting development and fielding of new capabilities associated with European Phased, Adaptive Approach Phase 3, BMDS Capability Increment 5, and USFK JEON Phase 2 functionalities:
  - Sensor improvements on tactics, techniques, and procedures for engagement of new ICBM threats.
  - Aegis BMD engage-on remote capabilities interoperating with C2BMC, BOA, and the AN/TPY-2 (FBM) radar.
  - BOA data on threat acquisition and tracking.
  - AN/TPY-2 (FBM) search plan selection.
  - New SBX discrimination databases.
  - USFK JEON Phase 2 architecture.
- Further, FY18 cybersecurity assessments informed the network defense posture of parts of the BMDS in USEUCOM and provided data on how to reduce mission risk for these elements operating in a cyber-contested environment. Specific test data and resulting assessments are classified (see the classified DOT&E "FY18 Assessment of the BMDS," to be published in February 2019).
- The Army has completed transition of AN/TPY-2 (FBM) radar operations to organic soldier operations for all but one radar site. Transition to organic maintenance is still ongoing. Operator training and interactive electronic technical manuals continue to be deficient.

- The MDA demonstrated C2BMC S8.2-3 BMDS planner functionality in support of BMDS Capability Increment 5 functionality, and collaboration between the planner and the Aegis mission planner, the Air and Missile Defense workstation, and the THAAD tactical planner for defense design development.

Recommendations

1. The MDA should develop a comprehensive operational cybersecurity test and evaluation strategy for each BMDS sensor and C2BMC. This strategy should be included in the Integrated Master Test Plan and reflect:
   - Coordination with Deputy Assistant Secretary of Defense for Developmental Test and Evaluation to implement cybersecurity developmental test prior to operational test.
   - Coordination with the Navy to conduct integrated operational cybersecurity testing of the SBX concurrent with the XBR.
   - Coordination with the Air Force to conduct integrated operational cybersecurity testing of the UEWRs and COBRA DANE radar.
   - Plans to address test limitations and mitigate system deficiencies identified in previous cybersecurity assessments.
   - A process for using previous cybersecurity assessment results to inform cyber testing requirements and future engineering cycles.

Ground-Based Midcourse Defense (GMD)

Executive Summary

- The Ground-based Midcourse Defense (GMD) element has demonstrated capability to defend the U.S. Homeland from a small number of intermediate-range ballistic missile (IRBM) or intercontinental ballistic missile (ICBM) threats with simple countermeasures when the Homeland Defense Ballistic Missile Defense System (BMDS) employs its full architecture of sensors and command and control.
- The Missile Defense Agency (MDA) declared a BMDS Homeland Defense technical capability of 44 Ground-Based Interceptors (GBIs) in December 2017.
- In FY18, GMD participated in two BMDS hardware-in-the-loop ground tests, and the MDA conducted extensive test planning in preparation for Flight Test, GBI-11 (FTG-11), which is the first GMD element operational test. FTG-11 is currently scheduled for 2QFY19.
- Quantitative evaluation of GMD operational effectiveness is not yet possible due to lack of sufficient ground testing with independently accredited modeling and simulation (M&S). Comprehensive cybersecurity assessments are required to support a GMD survivability assessment.

System

- GMD counters IRBM and ICBM threats to the U.S. Homeland. GMD consists of:
  - GBIs at Fort Greely, Alaska, and Vandenberg AFB, California.
  - GMD ground system, including Ground Fire Control (GFC) nodes, Launch Management System (LMS), and In-Flight Interceptor Communication System Data Terminals.
  - GMD secure data and voice communications system, including long-haul communications using the Defense Satellite Communication System, commercial satellite communications, and fiber-optic cable (both terrestrial and submarine).
  - External interfaces that connect to North American Aerospace Defense/U.S. Northern Command's Command Center; Command and Control, Battle Management, and Communications (C2BMC) system; Space-Based Infrared System; AN/TPY-2 Forward-Based Mode radars in Japan; and Aegis Ballistic Missile Defense ships through C2BMC.

Mission

Military operators from the U.S. Army Space and Missile Defense Command/Army Forces Strategic Command (the Army component to U.S. Strategic Command) will use the GMD system to defend the U.S. Homeland against IRBM and ICBM attacks using GBIs to defeat threat missiles during the midcourse segment of flight.

Major Contractors

- GMD Prime: The Boeing Company, Network and Space Systems – Huntsville, Alabama
- Boost Vehicle: Northrop Grumman Corporation, Innovation Systems – Chandler, Arizona
- Kill Vehicle: Raytheon Company, Missile Systems – Tucson, Arizona
- Fire Control and Communications: Northrop Grumman Corporation, Information Systems – Huntsville, Alabama

Activity

- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- The MDA delivered the 44th GBI in November 2017 and declared a BMDS technical capability for Homeland Defense the following month.
- The MDA did not conduct GMD flight testing in FY18.
- The GMD program conducted a cybersecurity Enhanced Homeland Defense (EHD) Ground Systems (GS) 7A laboratory-based risk reduction assessment in June 2018 to collect packet capture data, validate cybersecurity tools, and conduct penetration activities in preparation for additional pending cybersecurity testing. A second EHD GMD GS 7A

laboratory-based risk reduction assessment followed by the EHD Adversarial Assessment is planned for FY19.
- GMD participated in two BMDS hardware-in-the-loop ground tests:
  - The first ground test in November 2017 used hardware and software representations of the Homeland Defense BMDS, including the full GMD element, sensor architecture, and command and control suite. This test characterized the BMDS Capability Increment 4 functionality and limitations for ICBM threats.
  - The second test in July 2018 added the BMDS Overhead Persistent Infrared Architecture to the Homeland Defense BMDS and assessed the BMDS performance employing new Exo-atmospheric Kill Vehicle (EKV) Knowledge Database capabilities and GS enhancements during strategic and regional/theater scenarios for U.S. Northern Command and U.S. Indo-Pacific Command.
- In January 2018, the MDA Director extended the Development and Sustainment Contract through 2023 to manage overall program risk while achieving the expanded GMD capability called for in the Missile Defeat and Defense Enhancement Budget Amendment.
- The MDA fielded GMD GS 7A.0.0 hardware and software in January 2018 to improve element efficiency and availability. This enhancement integrated the functions of the independent Command Launch Equipment sub-system into the GFC and LMS. The MDA fielded updates to the initial software (version GS 7A.0.1) in June 2018.
- In February 2018, the MDA moved its Developmental Baseline Review (DBR) planning for the Redesigned Kill Vehicle (RKV), which is the follow-on capability to the EKV program, to the GMD Increment 6 program.
- In May 2018, the MDA definititized the RKV development contract per the approved Acquisition Plan with the Boeing Company.
- Throughout FY18, the MDA continued development of enhancements to the Capability Enhancement-I (CE-I) and CE-II EKVs. Updated software for fielding to the CE-I GBIs, and to the CE-II GBIs, is scheduled for FY19.
- The MDA conducted several executive-level reviews in preparation for FTG-11, and is on track for the first operational test of the GMD element in FY19.

Assessment
- Previous DOT&E assessments that GMD has demonstrated capability to defend the U.S. Homeland for a small number of IRBM or ICBM threats with simple countermeasures when the U.S. Homeland Defense BMDS employs its full architecture sensors and command and control remain unchanged.
- While the MDA made some progress during FY18, quantitative evaluation of GMD operational effectiveness requires extensive ground testing with independently accredited M&S that the MDA has not yet done. Also, more comprehensive threat-realistic operational cybersecurity testing (e.g., Adversarial Assessments preceded by Cooperative Vulnerability and Penetration Assessments), is required to support a quantitative GMD survivability assessment.
- Ground test data and resulting assessments are classified (see the classified DOT&E "FY18 Assessment of the BMDS," to be published in February 2019).

Recommendations

The MDA should:
1. Develop independently accredited M&S to support quantitative evaluation of GMD effectiveness.
2. Develop a comprehensive operational cybersecurity test and evaluation strategy for the GMD architecture; this strategy should be included in the Integrated Master Test Plan and reflect:
   - GMD coordination with Deputy Assistant Secretary of Defense for Developmental Test and Evaluation to implement cybersecurity developmental testing prior to operational testing.
   - Coordination with the Air Force to conduct integrated operational cybersecurity testing of the Upgraded Early Warning Radars and COBRA DANE radar.
   - Plans to address test limitations and mitigate system deficiencies identified in previous cybersecurity assessments.
   - A process for using previous cybersecurity assessment results to inform cyber testing requirements and future engineering cycles.

Aegis Ballistic Missile Defense (Aegis BMD)

Executive Summary

- The Missile Defense Agency (MDA) conducted four Aegis Ballistic Missile Defense (BMD) intercept flight tests in FY/CY18. Aegis BMD successfully intercepted three of the four ballistic missile targets in those tests. The Standard Missile-3 (SM-3) Block IB variant was successful in two of these tests. The SM-3 Block IIA variant succeeded in one test and failed in another.
- Aegis BMD participated in five non-intercept flight tests in FY/CY18 with simulated SM-3 Block IB and Block IIA variants engaging live targets and a live SM-6 Dual I missile engaging a simulated target.
- Aegis BMD provided hardware-in-the-loop (HWIL) representations for four Ballistic Missile Defense System (BMDS) ground tests that provided information on Aegis BMD interoperability and weapon system functionality in various regional/theater and strategic scenarios.
- The MDA delivered high-fidelity digital modeling and simulation (M&S) runs for record (RFRs) results in FY18 to support assessments of Aegis Baseline (BL) 9.C1 and SM-3 Block IB Threat Update (TU) missile performance for select scenarios.

System

- Aegis BMD is a sea- and land-based missile defense system that employs the multi-mission shipboard Aegis Weapon System, with improved radar and new missile capabilities to engage ballistic missile and anti-air warfare (AAW) threats. Aegis BMD includes:
  - Computer program modifications to all Aegis Weapon System elements, including the AN/SPY-1 radar, to support multiple BMDS mission capabilities including long-range surveillance and track, engagement support surveillance and track, and organic engagement with the SM-3, SM-6, or modified SM-2 Block IV missile variants against ballistic missiles
  - A modified Aegis Vertical Launching System, which stores and fires SM-3 Block IA, Block IB, and Block IIA guided missiles, modified SM-2 Block IV guided missiles, and SM-6 Dual I guided missiles
  - SM-3 Block IA, Block IB, and Block IIA guided missiles that use maneuverable kinetic warheads (KWs) to accomplish midcourse engagements of short-range ballistic missiles (SRBMs), medium-range ballistic missiles (MRBMs), and intermediate-range ballistic missiles (IRBMs)
  - Modified SM-2 Block IV guided missiles that provide Sea-Based Terminal (SBT) capability against SRBMs and MRBMs
  - SM-6 Dual I (fielded capability) and Dual II (under development) guided missiles that provide SBT capability against SRBMs and MRBMs in their terminal phase of flight, anti-ship cruise missiles, and all types of aircraft

Aegis Cruiser

Aegis Ashore and Vertical Launch System

- Aegis BMD ships and Aegis Ashore are designed to conduct missile defense operations, send/receive cues to/from other BMDS sensors through tactical datalinks, and conduct engagements using remote track data from BMDS sensors.
- Aegis Ashore (BL 9.B1) is the current land-based version of Aegis BMD, with an AN/SPY-1 radar and Vertical Launching System to enable engagements against MRBMs and IRBMs with SM-3 guided missiles. The operational Aegis Ashore site in Romania is the land-based component of the second phase of the European Phased-Adaptive Approach (EPAA) for the defense of Europe. A second site in Poland, currently undergoing construction and scheduled for completion in 2020, will complete the third phase of the EPAA for the defense of Europe.
- The following table summarizes the Aegis BMD weapon system configurations currently deployed or under development.

WEAPON SYSTEM	AEGIS BASELINE (BL) NOMENCLATURE	PLATFORM	MISSILES
Aegis BMD 5.1	BL 9.C2	Guided-Missile Destroyers (DDGs)	SM-3 Blocks IA, IB, and IIA SM-6 Dual I and Dual II SM-2 Block IV
	BL 9.B2	Aegis Ashore	SM-3 Blocks IA, IB, and IIA
Aegis BMD 5.0 (Capability Upgrade)	BL 9.C1	DDGs	SM-3 Blocks IA and IB SM-6 Dual I SM-2 Block IV
	BL 9.B1	Aegis Ashore	SM-3 Blocks IA and IB
Aegis BMD 4.1	Not Applicable	DDGs and Guided-Missile Cruisers (CGs)	SM-3 Blocks IA and IB SM-6 Dual I
Aegis BMD 4.0.3			SM-3 Blocks IA and IB SM-2 Block IV
Aegis BMD 3.6.4			SM-3 Blocks IA and IB SM-2 Block IV

Mission

The Navy can accomplish three missile defense-related missions using Aegis BMD:

- Defend deployed forces and allies from short- to intermediate-range theater ballistic missile threats
- Provide forward-deployed radar capabilities to enhance defense against ballistic missile threats of all ranges by sending cues or target track data to other BMDS elements
- Provide ballistic missile threat data to the Command and Control, Battle Management, and Communications (C2BMC) system for dissemination to Combatant Commanders' headquarters to ensure situational awareness

Major Contractors

- Aegis BMD Weapon System: Lockheed Martin Corporation, Rotary and Mission Systems – Moorestown, New Jersey
- AN/SPY-1 Radar: Lockheed Martin Corporation, Rotary and Mission Systems – Moorestown, New Jersey
- SM-3, SM-2 Block IV, and SM-6 Missiles: Raytheon Company, Missile Systems – Tucson, Arizona

---

Activity

- The MDA conducted all FY/CY18 testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- The MDA conducted four Aegis BMD intercept flight tests in FY/CY18, successfully engaging three of the four ballistic missile targets:
  - During the Formidable Shield-17 (FS-17) Navy fleet exercise in October 2017, an Aegis BMD 4.0.3 destroyer intercepted an MRBM target with an SM-3 Block IB TU missile. Participating NATO naval assets intercepted three AAW targets as part of a multinational integrated air and missile defense exercise.
  - During Flight Test Standard Missile-29 (FTM-29) in January 2018, the Aegis Ashore Missile Defense Test Complex (AAMDTC) at the Pacific Missile Range Facility in Kauai, Hawaii, attempted to intercept an air-launched IRBM target with an SM-3 Block IIA missile using the Aegis BL 9.B2 Engage on Remote (EOR) capability. The system failed to achieve an intercept when the SM-3 Block IIA third stage rocket motor did not ignite. The MDA subsequently conducted a failure investigation, identified the root cause, implemented a corrective action, and demonstrated the correction through a flight test.
  - During Japanese Flight Test Mission-05 (JFTM-05) Event 2 in September 2018, a Japanese Aegis destroyer organically intercepted a simple-separating SRBM target with an SM-3 Block IB TU missile.
  - During FTM-45 in October 2018, an Aegis BL 9.C2 destroyer organically intercepted a simple-separating MRBM target with an SM-3 Block IIA missile. This was the first intercept using a production-representative SM-3 Block IIA missile, and the second Block IIA intercept overall. This flight test also demonstrated the corrective action for the previous FTM-29 missile failure.
- Aegis BMD participated in five non-intercept flight test events in FY/CY18 with SM-3 Block IB and Block IIA variants engaging live targets and a live SM-6 Dual I missile engaging a simulated target:
  - During FS-17 in October 2017, Aegis BMD 4.0.3 and Aegis BL 9.C1 destroyers conducted simulated engagements of ballistic missile targets using remote data. NATO naval assets transmitted the remote track data through C2BMC and a NATO communications gateway. NATO assets that did not participate as BMD assets fired simulated and live missiles and engaged four AAW targets.

  - During Standard Missile Controlled Test Vehicle-03 (SM CTV-03) in October 2017, an Aegis BMD 4.1 destroyer engaged a simulated ballistic missile target with a live SM-6 Dual I missile. The firing supports certification of the Aegis BMD 4.1 upgrade to include hosting SBT capability.
  - During Flight Test Other-33 (FTX-33) in March 2018, the AAMDTC with BL 9.B2 software detected and tracked a complex SRBM target. The AAMDTC forwarded track data to an Aegis BMD laboratory to conduct a simulated EOR engagement.
  - During the Pacific Dragon 2018 Navy fleet exercise in August 2018, the AAMDTC with BL 9.B2 software conducted a simulated SM-3 Block IIA EOR engagement against an SRBM target using track data provided by U.S. and Japanese Aegis BMD ships. Laboratory representations of Aegis BMD also conducted simulated Launch on Remote engagements using track data provided by airborne sensors.
  - During JFTM-05 Event 2 in September 2018, an Aegis BL 9.C2 destroyer conducted a simulated engagement against a simple-separating SRBM target, which served as risk reduction for FTM-45.
- Four BMDS ground tests provided information on Aegis BMD interoperability and weapon system functionality in various regional/theater and strategic scenarios:
  - Ground Test-18 (GT-18) Sprint 1 DT RFRs in April 2018 explored BMDS performance in U.S. Indo-Pacific Command (USINDOPACOM) defense scenarios using an HWIL environment. Aegis BMD 3.6.4, 4.1, 4.0.3, and BL 9.C1 participated in the test.
  - Ground Test Integrated-07b (GTI-07b) U.S. European/ Central Commands (E/C) OT RFRs in April and May 2018 examined remote engagement, surveillance, and tracking performance to support an assessment of EPAA Phase 3 using an HWIL environment. Three Aegis BMD laboratory sites and the AAMDTC participated. GTI-07b (E/C) tested Aegis BL 9.C2, BL 9.B2, BL 9.C1, BL 9.B1, BMD 3.6.4, and BMD 4.1, and supported assessments of SM-3 Block IIA and SM-6 Dual II missiles. Warfighter support included U.S. Navy Aegis BMD teams from three Aegis BMD ships, Aegis Ashore, and Commander, Operational Test and Evaluation Force (OPTEVFOR) evaluators.
  - GT-18 Sprint 2 DT RFRs in July 2018 collected developmental data in an HWIL venue to support the inclusion of the Aegis BL 9.C2 SBT Increment 2 and SM-3 Block IIA EOR capabilities into the operational capability baseline for defense of USINDOPACOM.
  - Ground Test Distributed-07b (GTD-07b) (E/C) DT/OT RFRs in August and September 2018 used a distributed environment to explore BMDS performance in theater/ regional defense of USEUCOM and USCENTCOM to collect data to support deployment of EPAA Phase 3. GTD-07b (E/C) tested Aegis BL 9.C2, BL 9.B2, BL 9.C1, and BMD 4.1.
- The BMDS Operational Test Agency and OPTEVFOR recommended accreditation of all participating Aegis BMD HWIL M&S for the regional/theater and strategic scenarios assessed ground testing, with the exception of the M&S for Aegis BMD 4.1, which was only accredited for use in GTD-07b (E/C).
- The MDA delivered high-fidelity digital M&S RFR results in FY18 to support assessments of Aegis BL 9.C1 and SM-3 Block IB TU missile performance for select scenarios. OPTEVFOR accredited the FY17/18 RFR sets for Aegis BL 9. B1 and BL 9.C1 performance assessments.
- A December 2017 SM-3 Block IB Acquisition Decision Memorandum requires the MDA and DOT&E to ensure periodic flight testing of the Block IB throughout the life of the program in the Integrated Master Test Plan (IMTP). The MDA has addressed this requirement by adding surveillance firings to the test program. The MDA conducted two successful end-to-end flight tests of the production-representative Block IB TU missile during FS-17 and JFTM-05 Event 2.

Assessment

- Results from flight testing, high-fidelity M&S, HWIL, and distributed ground testing demonstrate that Aegis BMD can intercept non-separating, simple-separating, and complex-separating ballistic missiles in the midcourse phase. However, flight testing and M&S did not address all expected threat types, ground ranges, and raid sizes.
- FTM-45 successfully and fully demonstrated the Aegis BL 9.2 organic engagement capability and corrective action for the previous FTM-29 missile failure. FTM-29 was only partially able to demonstrate EOR capability given the in-flight missile failure. In FTM-29, the Aegis Weapon System supported the SM-3 Block IIA missile and demonstrated bi-directional communication between the SM-3 Block IIA guidance section and the KW until loss of signal at horizon. However, the weapon system did not exercise all aspects of communication after KW eject. DOT&E considers the FTM-29 failure to be an example of a shortfall in conducting ground testing in an operationally representative way, and an example of a deficiency found in OT that DT should have discovered.
- The MDA implemented process improvements to better identify, report, and fix common failures and anomalies identified during SM-3 ground testing prior to flight testing.
- SM CTV-03 demonstrated the capability of the Aegis BMD 4.1 upgrade to fire an SM-6 Dual I missile. The BMD 4.1 build incorporates BL 9.C1 capabilities into the BMD 4.0 baseline.
- FS-17 demonstrated the Aegis BMD 4.0.3 capability to interoperate with NATO partners over operational communication architectures during cruise missile and ballistic missile engagements, and to use remote data provided by NATO partners to prosecute remote engagements. JFTM-05 Event 2 demonstrated inter-ship communication between U.S. and Japanese destroyers using a realistic communications architecture while prosecuting ballistic missile engagements. Pacific Dragon demonstrated interoperability between U.S.

Aegis BMD assets, Japanese destroyers, and Republic of Korea naval assets.
- Aegis BMD has exercised rudimentary engagement coordination with Terminal High-Altitude Area Defense firing units, but not with Patriot. The MDA plans to include Patriot in FTO-03. MDA ground tests have routinely demonstrated that inter-element coordination and interoperability need improvement to increase situational awareness and improve engagement efficiency.
- The MDA has been collaborating with DOT&E and the Under Secretary of Defense (Research and Engineering) to establish an affordable ground testing approach to support assessments of reliability. DOT&E cannot assess SM-3 missile reliability with confidence until the MDA is able to provide additional ground test data that simulates the in-flight environment. DOT&E is working with the MDA to determine if existing ground test venues are able to provide the needed missile reliability data.

Recommendations

The MDA should:

1. Ensure that ground tests of all SM-3 missile components, sections, and all-up rounds use the same configuration as will be flown in flight tests (i.e., "test as you fly").
2. Determine how to properly score acceptance ground test data for production missiles to enable their use in estimating SM-3 reliability.
3. Fund and execute high-fidelity M&S RFRs for Aegis BL 9.2 SM-3 Block IIA and SM-6 Dual II scenarios that span the engagement battlespace.

Terminal High-Altitude Area Defense (THAAD)

Executive Summary

- The Missile Defense Agency (MDA) conducted one tracking exercise to demonstrate Terminal High-Altitude Area Defense (THAAD) interoperability with the Patriot system.
- The Army Research Laboratory Survivability/Lethality Analysis Directorate (ARL/SLAD) conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) with THAAD to identify cybersecurity vulnerabilities. The Army Threat Systems Management Office (TSMO) conducted an Adversarial Assessment (AA) with THAAD to support a cybersecurity survivability assessment.
- THAAD participated in three Ballistic Missile Defense System (BMDS) ground tests, providing information on THAAD interoperability and functionality within the BMDS for various regional/theater scenarios.
- The THAAD program continued to address deficiencies from the first conditional materiel release in February 2012. The program completed urgent software releases of THAAD system software builds TH 2.8.2 and TH 2.8.3.
- The THAAD program made progress in resolving missing documentation and addressing limitations that affect THAAD models and simulations. The BMDS Operational Test Agency accredited two THAAD models and simulations with associated limitations.
- Testing in FY18 demonstrated that THAAD training, documentation, and reliability deficiencies, previously reported in DOT&E Annual Reports, persist.

System

- THAAD complements the lower-tier Patriot system and the upper-tier Aegis Ballistic Missile Defense (BMD) system. It is designed to engage threat ballistic missiles in both the endo- and exo-atmosphere.
- THAAD consists of five major components:
  - Missiles
  - Launchers
  - AN/TPY-2 Radar (Terminal Mode)
  - THAAD Fire Control and Communications
  - THAAD Peculiar Support Equipment
- THAAD can provide and accept target cues for acquisition from Aegis BMD, from other regional sensors, and through command and control systems.

Mission

The U.S. Northern Command, U.S. Indo-Pacific Command (USINDOPACOM), U.S. European Command (USEUCOM), and U.S. Central Command (USCENTCOM) intend to use THAAD to intercept short- to intermediate-range ballistic missile threats in their areas of responsibility. The U.S. Strategic Command deploys THAAD to protect critical assets worldwide from these same threats.

Major Contractors

- Prime: Lockheed Martin Corporation, Missiles and Fire Control – Dallas, Texas
- Interceptors: Lockheed Martin Corporation, Missiles and Fire Control – Troy, Alabama
- AN/TPY-2 Radar (Terminal Mode): Raytheon Company, Integrated Defense Systems – Tewksbury, Massachusetts

Activity

- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- The THAAD program re-prioritized and accelerated capability development to support the U.S. Forces Korea (USFK) Joint Emergent Operational Need (JEON), issued in February 2017.
- Three BMDS ground tests using THAAD hardware-in-the-loop representations and THAAD Digital representations provided information on THAAD interoperability and functionality in various regional/theater scenarios:

  - In Ground Test Integrated-07b (GTI-07b) USEUCOM/USCENTCOM (E/C) in April 2018, the MDA examined USEUCOM and USCENTCOM defense using THAAD 3.0.0 software.
  - In Ground Test-18 (GT-18) Sprint 1 in April 2018, the MDA examined USINDOPACOM defense using THAAD 3.0.0 software.
  - In Ground Test Distributed-07b (GTD-07b) (E/C) in September 2018, the MDA again examined USEUCOM and USCENTCOM defense using THAAD 3.0.0 software.
- The MDA conducted one tracking exercise, Flight Test Other-35 (FTX-35), in April 2018 at White Sands Missile Range, New Mexico, to test THAAD and Patriot interoperability.
  - THAAD tracked a close-range ballistic missile (CRBM) target, exchanged messages with a Patriot battery, and supported a THAAD Fire Control/Communications firing solution.
  - The THAAD battery consisted of THAAD Configuration 2 hardware, THAAD 3.0.0 software, one launcher equipped with simulated interceptors, THAAD Fire Control and Communications, and the AN/TPY-2 radar (Terminal Mode) with x86 architecture.
- ARL/SLAD, in support of the MDA, conducted a CVPA on the THAAD battery with THAAD 3.0.0 software in March 2018 in accordance with the DOT&E-approved test plan.
- TSMO, in support of the MDA, conducted an Adversarial Assessment (AA) on the THAAD battery with THAAD 3.0.0 software in April 2018 in accordance with the DOT&E-approved test plan.
- The THAAD program continued to address deficiencies from the first conditional materiel release. The program completed urgent software releases of the THAAD system software builds TH 2.8.2 and TH 2.8.3.

Assessment

- The THAAD Project Office improved its approach to cybersecurity assessments in FY18 by working across the MDA and with the Army to develop a comprehensive test plan. Its approach serves as a model for cybersecurity testing on other BMDS programs.
- During GTI-07b (E/C), GT-18 Sprint 1, and GTD-07b (E/C), the MDA demonstrated aspects of THAAD functionality in different theater scenarios to support BMDS Increment 5, European Phased Adaptive Approach (EPAA) Phase 3, and USFK JEON. The BMDS Operational Test Agency reported findings that affect THAAD interoperability, track management, and radar functions. Details are classified and will be published in the classified DOT&E "FY18 Assessment of the BMDS" in February 2019. THAAD made progress in addressing model limitations and both Simulation Over Live Driver and Real-time Integrated Simulation and Tactical Software received accreditation recommendations, with associated limitations, for the GTD-07b event.
- In FTX-35, the MDA demonstrated THAAD interoperability with a Patriot battery by exchanging messages over tactical networks while simultaneously tracking a CRBM target.
- Testing in FY18 demonstrated that THAAD training and documentation deficiencies persist. DOT&E detailed these problems and made recommendations to fix them in the FY17 DOT&E Annual Report.
- To address THAAD launcher reliability problems, the Army tested five launchers using prototype 3-kilowatt generators with hardware improvements at WSMR, demonstrating the potential to improve the generator reliability to meet the manufacturer's specification for Mean Time Between Failure. The Army has addressed workmanship, maintenance, and procedural issues uncovered during testing and the Expeditionary Energy and Sustainment Systems Project Office (3-kilowatt generator project office) has plans to test.
- During FTX-35, the unit (soldiers and contractor logistical support) experienced numerous problems integrating the new x86 radar and synchronizing the new prime power unit (PPU) with legacy PPUs. Details are classified and will be published in the classified DOT&E "FY18 Assessment of the BMDS" in February 2019.
- The MDA and the Army continued to address deficiencies from the Army's first conditional materiel release in FY12 and the conditional software materiel release for THAAD system software build TH 2.2.0 that affect fielded hardware and software. The THAAD program successfully addressed all conditions for the Institutional Conduct of Fire Trainer, transitioning it to a full training materiel release.

Recommendations

The MDA should:

1. Address limitations stated in the MDA and BMDS Operational Test Agency accreditation for ground testing of THAAD models and simulations.
2. Address the cybersecurity findings from the FY18 CVPA and AA.
3. Coordinate with the Office of the Deputy Assistant Secretary of Defense (Developmental Test and Evaluation) to evaluate cybersecurity during DT prior to OT.

Live Fire Test and Evaluation

Live Fire Test and Evaluation

Live Fire Test and Evaluation (LFT&E)

Summary

- In FY18, DOT&E executed LFT&E oversight for the following:
  - 84 Service acquisition programs
  - Three LFT&E investment programs:
    - Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME)
    - Joint Aircraft Survivability Program (JASP)
    - Joint Live Fire (JLF) Program
  - Three special interest programs:
    - Warrior Injury Assessment Manikin (WIAMan)
    - Combat Damage Assessment
    - Test and Evaluation of Emerging Technologies
- In support of major acquisition decisions, DOT&E published 11 combined OT&E and LFT&E reports and 4 LFT&E reports summarizing the lethality and survivability of the subject systems and offering recommendations intended to further improve lethality and survivability in expected operational scenarios.
- In support of the National Defense Strategy, DOT&E continued efforts to realign the three LFT&E investment programs to focus on the following priorities:
  - Develop a more lethal force by enhancing the capabilities of the joint weaponeering and combat effectiveness tools and by developing critical aircraft survivability enhancement technologies.
  - Strengthen alliances by providing weaponeering tools and training to coalition partners in support of current operations, and by teaming with coalition partners to better characterize and mitigate combat-induced system vulnerabilities.
  - Enable Department reforms by investing in more efficient software development architectures, modeling and simulation (M&S) tools, threat model development, and other innovative T&E methods. These efforts will allow the test community to conduct T&E more efficiently, and more effectively support rapid prototyping and fielding.
- Special interest programs continue to make progress in addressing a test instrumentation shortfall for assessing injuries to ground combat vehicle occupants. These programs also continue to collect combat damage assessment data to ensure operational relevance of LFT&E. Lastly, special interest programs have been established to assess and develop methods to effectively test emerging technologies including non-lethal weapons, directed-energy weapons, and counter-unmanned aerial systems (C-UAS).

LFT&E ACQUISITION PROGRAMS

The primary objective of LFT&E is to evaluate the survivability and lethality of acquisition programs and to identify system design deficiencies to be corrected before fielding or full-rate production. In FY18, DOT&E executed LFT&E oversight for 84 acquisition programs. Of those, 21 operated under the waiver provision of section 2366, title 10, U.S. Code, by executing an approved alternative LFT&E strategy in lieu of full-up system-level testing. In FY18, DOT&E published the following reports reflecting a sample of programs under LFT&E oversight:

- "AC-130J Block 20 Initial Operational Test and Evaluation Report," published in April 2018, reported on the AC-130J survivability against small arms, anti-aircraft artillery, legacy man-portable air-defense systems (MANPADS), and radio frequency (RF)-guided surface-to-air missiles. Additionally, it reported on the AC-130J lethality of the 30 mm gun, 105 mm cannon, and the Griffin missile against their intended targets. LFT&E made seven recommendations intended to further improve the AC-130J survivability and lethality in expected operational scenarios.
- "Patriot Post-Deployment Build-8 (PDB-8) and Missile Segment Enhancement (MSE) Initial Operational Test and Evaluation Report," published in April 2018, reported on the lethality of the Patriot Advanced Capability – 3 (PAC-3) system with both PDB-8 and MSEs. While the PAC-3 system was successfully evaluated against a wide variety of potential threats, the report identified five threats for which the system could not be evaluated and would require future analysis. The report supported the U.S. Army's Full-Rate Production decision for the PAC-3 MSE system in June 2018.
- "Soldier Protective System (SPS) Vital Torso Protection (VTP) Live Fire Report," published in April 2018, reported on the ballistic performance of lighter-weight hard armor inserts to protect soldiers against specified small arms threats. The report recommended the Army establish a credible correlation between threat-induced deformations in the armor inserts and the probability of injury.
- "Integrated Head Protection System (IHPS) Live Fire Report," published in May 2018, reported on the ballistic performance of the SPS helmet subsystem to protect soldiers against specified small arms threats. The report recommended the Army establish a credible correlation between threat-induced deformations in the helmet and the probability of injury.
- "Amphibious Combat Vehicle (ACV) 1.1 Operational Assessment Report," published in June 2018, summarized the force protection performance of two prototype vehicles,

developed by competing contractors, against small arms, heavy machine guns, underbody blast (UBB) mines, and IEDs.
- "M109A7 Family of Vehicles Live Fire Report," published in June 2018, reported on the vehicle's ability to provide force protection and continue with the mission when engaged with threats expected to be encountered in combat.
- "Army Tactical Missile System (ATACMS) Modification (MOD) Combined Live Fire and Operational Test Report," published in September 2018, reported on the lethality, survivability, operational effectiveness, and suitability of the ATACMS MOD. The report was delivered to support the Army's decision to field this upgraded system.

LFT&E INVESTMENT PROGRAMS

JOINT TECHNICAL COORDINATING GROUP FOR MUNITIONS EFFECTIVENESS (JTCG/ME)

JTCG/ME is the Department's sole developer of Joint Munition Effectiveness Manuals (JMEMs). JMEM products include tools that enable users across Combatant Commands (CCMDs) to adequately plan combat missions. JMEM tools estimate the effectiveness of a weapon against a specified target and help determine the appropriate type and number of weapons required to achieve the desired lethal effect on that target. As such, JMEMs rely on detailed data describing:
- The physical characteristics and performance of weapons and targets
- Credible mathematical methods that employ these data to generate weapons effectiveness estimates
- User-friendly software that permits mission planners to calculate and visualize weapons effectiveness estimates, and assess mission success risks

JTCG/ME is chartered to authenticate weapons effects data across the Services, develop methods to assess and enable effective weapons employment, and provide reach-back analysis and forward support to prosecute targets. Current JMEM product lines include:
- JMEM Weaponeering Software (JWS)
- Joint Anti-Air Combat Effectiveness (J-ACE) tool
- Digital Precision Strike Suite (DPSS) Collateral Damage Estimation (DCiDE) tool
- Digital Imagery Exploitation Engine (DIEE).

Future product lines include Joint Non-Kinetic Effectiveness (J-NKE) capabilities such as cyber, electromagnetic fires, and directed energy. There are also specialized products driven by the needs of CCMDs, coalition partner interoperability, and lessons learned from current operations. These products include Probability of Kill (Pk) Lookup Tools, Quick Weaponeering Tables, Collateral Damage Estimation (CDE) tables, and scenario-specific CDE analysis packages. Products support mission planners and ongoing operations, and JTCG/ME works with users to establish warfighter requirements for current and future products and training.

JOINT AIRCRAFT SURVIVABILITY PROGRAM (JASP)

The purpose of the JASP is to increase military aircraft combat survivability – therefore force lethality – in current and emerging threat environments. JASP funds research and development of emerging aircraft survivability technologies, improves core aircraft survivability assessment tools, and collects and interprets aircraft combat data. JASP focused on projects intended to: 1) develop measures to avoid detection and counter engagement of advanced RF- and infrared (IR)-guided threats, 2) improve aircraft force protection, and 3) improve aircraft survivability to combat-induced fires. In FY18, JASP funded 38 multi-year projects and delivered 23 final reports.

JOINT LIVE FIRE (JLF) PROGRAM

The purpose of the JLF program is to improve force lethality by resolving survivability and lethality challenges of new and fielded weapons systems, and strengthen and leverage alliances by conducting joint survivability and lethality T&E. Lastly, the JLF programs support the Department's business reforms by advancing T&E methods to increase their effectiveness and efficiency to support rapid prototyping and fielding. In FY18, JLF funded 26 projects and delivered 11 reports.

LFT&E INVESTMENT PROGRAM INITIATIVES

In FY18, DOT&E continued to align its investment programs with the three lines of effort identified in the National Defense Strategy. Examples that pertain to this alignment are discussed below.

BUILD A MORE LETHAL FORCE

1. Joint Weaponeering Tools

In FY18, LFT&E investment programs enhanced the capabilities of the JMEM Weaponeering System (JWS). This enabled more effective air-to-surface and surface-to-surface weaponeering across warfare domains. Specifically, JTCG/ME:
- Released a new version of the JWS tool (v2.3) and continued development of the next version (v2.4). Both versions focus on connectivity to other targeting and mission planning capabilities and updated weapon/target data sets for improved estimates and more seamless planning. Specific JWS v2.3 improvements include:
  - Information assurance and cybersecurity
  - Connectivity to permit automatic and optimum transfer of data between planning tools (Modernized Integrated Database, Joint Targeting Toolbox (JTT), and DIEE)

  - Weapons effectiveness estimates and planning optimization for structural and maritime targets by enhancement of the Fast Integrated Structural Tool and Ship Weaponeering Estimation Tool
  - Effectiveness estimates for F-35 gun munitions and C-130 gunship
  - Predicted accuracy of GPS/Inertial Navigation System weapons from satellite time and space calculations (by integrating the Dilution of Precision Tool)
  - Target Location Error estimate from airborne and ground-based sensors
  - Weapons and target vulnerability data with over 65 new target vulnerability data sets across warfare domains
- Provided new accredited Collateral Effects Radii (CER) Reference Tables to mitigate risk to non-combatants during weapons employment decisions. Kinetic strike planners use the JTCG/ME CER tables to minimize civilian casualties.
- Continued the development of two new JMEM tools to enable weaponeering and targeteering with non-kinetic weapons:
  - The Cyber Operation Lethality and Effectiveness (COLE) tool provides cyber effects estimations. Efforts in FY18 focused on standardization of data required to address offensive cyber weapon characterization, target vulnerability, operational environment, and uncertainty metrics. The COLE tool is founded on prior software development work initiated by the Air Force, the Army, the Defense Advanced Research Projects Agency, and data from operational test activities. The first version of the COLE tool is scheduled to be delivered in FY19.
  - The directed-energy weapon effects estimation and standardization tool provides high-energy laser effect estimations. Efforts in FY18 focused on addressing the uniqueness of the high-energy laser kill mechanisms, the uniqueness of the target vulnerability to laser lethal effects, and the atmospherics and other environmental factors that are required to establish a probability of effects calculation. The first version of a directed-energy weaponeering tool and a collateral damage estimation software is scheduled to be delivered in 1QFY19.
- Supported the warfighter with analysis and products for urgent operational needs and future JMEM production:
  - Provided direct forward and reach-back support to Combatant Commanders/Task Forces to enable weapons employment and strike decisions for high-value targets in current operations.
  - Supported current use and future JWS development requirements by hosting and supporting JWS training sessions, Operational Users Working Groups (OUWGs) and user help-desk support. These are critical venues for receiving user feedback and development of future JWS requirements.

2. Joint Anti-Air Combat Effectiveness Tool

In FY18, LFT&E investment programs improved air combat lethality by developing and releasing enhanced versions of the Joint Anti-air Combat Effectiveness (J-ACE) tools. J-ACE provides an assessment of full kill chain capability serving as the primary tool used to underpin air combat tactics, techniques, and procedures (TTP) development. Specifically, JTCG/ME fielded a new version of J-ACE (v5.3) and continued the development of the next J-ACE version (v5.4) with new capabilities, to include:

- Increased aircraft aero performance modeling by integrating the BLUEMAX6 (six degrees of freedom aero performance) model
- Improved real-time user interaction by integrating Hand-On-Throttle-And-Stick controls
- Increased ability to estimate countermeasure effectiveness by leveraging Enhanced Surface-to-Air Missile Simulation (ESAMS)
- Improved Graphical User Interface
- Improved connectivity between J-ACE and debrief/analysis tools at test and training ranges
- Improved target detection capability by leveraging National Air and Space Intelligence Center Radio Frequency models, and an initial Suppression/Destruction of Enemy Air Defense Capabilities.

3. Aircraft Survivability Technology

In FY18, LFT&E investment programs continued the development of aircraft survivability enhancement technologies to defeat near-peer and second-tier adversary threats (i.e., advanced RF and IR threats), and to improve the ability of U.S. aircraft to avoid either threat engagement or to mitigate damage when hit with a rocket-propelled grenade (RPG) or small arms:

- **RF Threats**. JASP funded the development of advanced Digital RF Memory based jamming techniques to provide countermeasure capability against new, more capable threat systems. JASP also co-funded a project with the Georgia Tech Research Institute to assess the sensitivity of countermeasure parameters such as missile break-lock, miss distance, deployment timing, and similar in order to develop the next generation RF towed decoy technology.
- **IR Threats.** JASP sponsored the development of IR countermeasure (IRCM) jam code requirements for Directional Infrared Countermeasure (DIRCM) systems to defeat two new threat systems. JASP also studied the potential advantages of using guided IRCM expendables to counter advanced IR-guided missile seekers. Lastly, JASP optimized algorithms used in existing missile warning sensors (MWS) to enable identification of hostile missile threats with newer classes of IR-guided seekers.
- **RPG Threats.** JASP funded the development and testing of three anti-RPG kill mechanism solutions. Testing

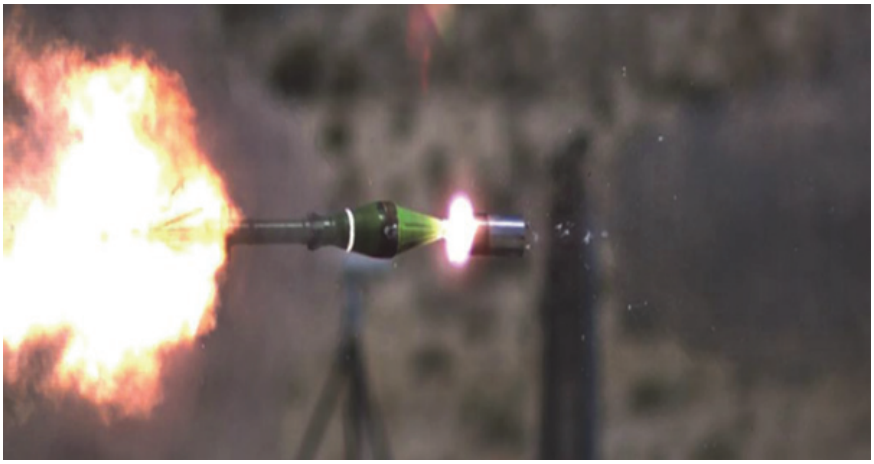


Figure 1. Kinetic Kill Vehicle Impact on RPG PG-7 85 mm (HEAT)

showed two concepts met the performance goals for lethality and collateral damage effects making them viable candidates for future helicopter active protection systems. JASP also continued characterization of debris from Active Protection System (APS) Kill Vehicle (KV) engagements against RPGs as shown in Figure 1.

- **Small Arms.** JASP continued development of aircraft hardening techniques to include transparent and opaque armors. Efforts supported the development of three highly efficient transparent armor designs for small arms projectile protection that reduce weight while improving the thermal durability. Efforts also supported the development of a spaced armor concept capable of stopping small arms armor-piercing (AP) projectiles at substantially less weight than current opaque armors.

In FY18, LFT&E investment programs continued the development and testing of aircraft survivability solutions to maximize residual aircraft flight capability in the event of combat-induced aircraft fires or fuel leaks. Significant FY18 efforts:

- Supported the development of a new intelligent fire suppression system demonstrating a 100 percent success rate in suppressing spray fires using less than 13 grams of agent per fire event.
- Evaluated the V-22's Fuel Management Units and any adverse effects on the fire suppression system due to associated fuel fire in the wing and mid-wing dry bay locations.
- Evaluated the potential fire vulnerabilities associated with auxiliary power unit (APU) accumulators commonly fielded with all versions of H-60 military helicopters.
- Investigated materials to deliver new, lighter weight, more reliable sealing technology for fuel bladders with the goal of reducing weight by 50 percent compared to current self-sealing fuel bladder materials.

STRENGTHEN ALLIANCES AND ATTRACT NEW PARTNERS

In FY18, LFT&E strengthened partnerships by providing weaponeering tools and training to coalition partners in support of current operations, and by teaming with coalition partners to better characterize and mitigate combat-induced system vulnerabilities. Specifically:

- JTCG/ME delivered two JWS version releases and three standalone Pk Lookup tools to key coalition partners in support of current operations under Foreign Military Sales agreements. These deliveries compared current Department efforts with U.S. interests and improved interoperability with allies and partners.
- JTCG/ME leveraged the Test Assistance Group (TAG) to enhance weapons characterization processes. The TAG activities foster an environment of reuse and learning across the coalition, interagency, industry, and DOD partners. For example, JTCG/ME leveraged TAG to partner with Sandia National Laboratories to advance three-dimensional fragmentation modeling and tracking using artificial intelligence techniques, high-speed stereoscopic optical, and x-ray development. These techniques and partnerships have the potential to reduce the number of weapon test articles and labor-intensive activities in future weapon lethality T&E.
- JTCG/ME influenced and supported NATO and international test operation procedures (ITOPs) by archiving, publishing, and sharing weapon characterization standards in updates to the JTCG/ME Weapon Test Procedures Manual.
- The JLF program initiated a project with Canadian counterparts to better characterize realistic torpedo and mine threat effects on Navy platforms. JLF funded the testing of near-field underwater explosion (UNDEX) phenomena while our Canadian counterparts provided the test article (panels extracted from a decommissioned Canadian ship). The collective effort will enhance Canadian and U.S. understanding

of UNDEX bubble phenomena and facilitate the validation of numerical predictions for realistic attacks. The effort will enhance our ability to develop/design more effective underwater weapons.

REFORM THE DEPARTMENT FOR GREATER PERFORMANCE AND AFFORDABILITY

In FY18, LFT&E investment programs enabled Department reforms by funding the development of more efficient software architectures, M&S tools, threat models, and other innovative T&E methods. These investments are intended to enable the test community to conduct T&E more effectively and efficiently, and to support mid-tier acquisition (rapid prototyping and rapid fielding).

1. Software Development Architecture

In FY18, JTCG/ME identified a new software architecture for JMEM tools to provide greater efficiency and optimization of weapons effects across all warfare domains in response to the changing strategic environment, and urban and close-combat operations. For example:

- The next generation JWS tools (v3.x) will use the U.S Air Force's Endgame Framework (EF) as the underlying software architecture to maximize modularity and flexibility of design modification, decrease development time, and reuse of standard capabilities across the community. JTCG/ME finalized the concept plan development and benchmarked the methods available for development within EF.
- The next generation J-ACE (v6.x) will also use EF as the underlying software architecture as well as the Hybrid Integrated Visualization Engine. The new architecture will help address enduring development requirements to include rotary-wing aircraft capability, expanded suppression/destruction of enemy air defense capabilities, and increased electronic warfare and countermeasure capabilities.

2. Modeling and Simulation Tools

JTCG/ME, JASP, and JLF integrated their efforts to rebaseline strategic roadmaps for underlying survivability and lethality M&S tools. These M&S tools are the foundation of JMEM products and LFT&E of acquisition programs. Efforts were focused on the following M&S tools:

- **Computation of Vulnerable Area Tool (COVART).** JASP supported development of an upgrade to COVART to enable six degrees of freedom equations for fragment and projectile penetration calculations. This capability will improve the accuracy of threat residual mass, velocity, and trajectory calculations thereby improving the accuracy and confidence in system Pk analysis. JASP also funded an effort to quantify the sensitivity of system-level Pk values on penetration errors and threat input parameters. In FY18, the model manager modified COVART to enable Monte Carlo processing of penetration errors.
- **Fast Air Target Encounter Penetration (FATEPEN).** JLF and JTCG/ME efforts expanded the capability and accuracy of FATEPEN, a threat penetration model used to predict weapon lethality and platform vulnerability to warhead-generated fragments. JLF collected fragment penetration data for buildings constructed from concrete masonry unit (CMU) blocks commonly observed in ongoing areas of operation. JTCG/ME will utilize these results to develop an accredited CMU target model for FATEPEN, allowing for better lethality predictions of U.S. munitions and better quantification of collateral damage effects. JLF efforts also improved FATEPEN accuracy in modeling lethal effects of irregular fragments ejected by many contemporary munitions.
- **Projectile Penetration (ProjPEN).** JLF sponsored collection of yawed projectile penetration data to support improved accuracy of ProjPEN, a threat penetration model used to predict weapon lethality and platform vulnerability to projectiles. The data will enable improved prediction of the damage caused by AP and armor-piercing incendiary (API) rounds on aircraft as a function of aircraft's velocity.
- **Dynamic System Mechanics Advanced Simulation (DYSMAS).** Hydrocodes have difficulty simulating UNDEX bubble dynamics. JLF funded a test series to quantify energy losses for UNDEX bubbles. The data generated by this task will support the model development task funded separately by the Office of Naval Research. These data will form the cornerstone of model validation for the DYSMAS M&S tool used to assess the vulnerability of submarine hulls and ship structures to large standoff weapons such as mines.
- **Advanced Survivability Assessment Program (ASAP).** Navy equipment "kill" criteria used in ASAP are based on antiquated empirical data. JLF is executing a plan to collect fragility data of shipboard equipment to increase assessment confidence levels. In FY18, JLF identified equipment (or surrogates) to be procured in FY19 and tested in FY20. This effort will improve the validation and pedigree of fragility criteria against modern vital equipment. Ultimately, it will improve the quality of naval ship LFT&E assessments.
- **Integrated Recoverability Model (IRM).** Vulnerability and Recoverability (V&R) M&S rely on estimation of equipment thermal fragility criteria to predict realistic system-of-system performance. One of the most challenging V&R events is a shipboard fire, and prediction efforts have been limited by simple models with significant error ranges. JLF is developing a statistically accurate equipment thermal fragility and failure prediction method. Completion of this program will enhance naval vulnerability data libraries for operationally significant survivability effects and improve critical LFT&E M&S tools.
- **Next Generation Fire Prediction Model.** JASP continued to improve the prediction model of aircraft dry bay fire

ignition due to ballistic threats. JASP, in coordination with Lawrence Livermore National Laboratory, continued with efforts to accurately predict the convergence of energy deposition and hydrodynamic ram (HRAM)/fuel deposition resulting from threat penetration. JASP continued the development of an accurate, fast running engineering model that will form the basis of the Next Generation Fire Prediction Model.

- **Enhanced Surface-to-Air Missile Simulation (ESAMS).** ESAMS is the primary tool used by government and industry to assess the engagement of U.S. aircraft by radar-directed surface-to-air missile systems. JASP continues to develop ESAMS upgrades to accurately model rotorcraft survivability, representative jamming environment, clutter, and existing and emerging RF threats. JASP is also funding an effort to compare ESAMS results with hardware-in-the-loop simulation and flight test data to assess the adequacy of T&E tools and methods used to evaluate performance of new techniques against advanced threat radars.
- **Modeling System for Advanced Investigation of Countermeasures (MOSAIC).** JASP is funding efforts to integrate a capability for guided expendables, as well as a tool to improve effectiveness analysis in MOSAIC.

3. Threat Model Development

To advance LFT&E, it is important to ensure adequate availability of adversary targets/threats and their models since the survivability and lethality evaluation of our systems largely depends on our understanding of adversaries' capabilities and damage effects. In FY18, JLF:

- Sponsored development of a representative TM-62M Russian antitank mine surrogate. The results of this work will allow the LFT&E community to ensure a more operationally representative survivability evaluation of U.S. ground combat vehicles to UBB events.
- Sponsored development of high-fidelity physics-based hydrocode and engineering level models for two widely proliferated (classified) shaped-charged warheads. The modeling methodology established in FY18 will serve as the analytical bridge to develop high-fidelity engineering-level models for similar warheads.
- Funded development of an instrumented inert threat system for use in counter-munition effectiveness evaluations during live fire hard-kill APS testing. Successful conclusion of this work will result in a test surrogate that is more accurate, cheaper, and provides better data to support APS effectiveness analyses. The U.S. Army Redstone Test Center, using JLF funding, defined a tandem warhead threat that best represents contemporary threats to U.S. forces.
- Validated an OG-7V grenade threat model to better evaluate fragmentation grenade effects on rotary-wing aircraft. A threat model, based on UH-60A partial fuselages test data, is being written for the Threat Pedigree books distributed in the Vulnerability Toolkit. The resulting validated fragmentation grenade threat model will lower the cost of rotary-wing design and vulnerability assessments in the future.

4. Innovative T&E Methods

- **Scalable Test Methods.** JLF funded the Air Force Research Laboratory (AFRL) Munitions Directorate to apply scalable experimentation methods in LFT&E. The intent was to provide data for validating JMEM warfighter tools that predict blast effects from detonations inside buildings in a more efficient manner. As new weapons and target sets materialize, JMEM developers will have a tailorable scale model they can use to validate blast effect models at a fraction of the cost of full-scale testing. Such a test method will provide warfighters more accurate weaponeering tools to predict the desired internal building effects and associated collateral damage.
- **Sensitivity Analyses.** The confidence in the results of some vulnerability and lethality M&S tools is either not known or low. JLF funded a project intended to apply sensitivity analyses to better quantify uncertainty in standard vulnerability metrics for variations in model input parameters. The most sensitive parameters will be identified to enable using higher fidelity vulnerability and lethality M&S tools with greater confidence.
- **New M&S capabilities.** The Navy currently has neither an insulation damage model nor significant data relating fire insulation impairment to blast severity. This results in overly conservative estimates of insulation effectiveness against heat/fire. JLF funded the development of an insulation damage model, suitable for whole-ship vulnerability assessments, to relate fire insulation impairment to blast severity. This will improve LFT&E assessments of future Navy ship acquisition programs for typical air-delivered threat weapons.

Figure 2. Buried Ordnance Test using a simulated asphalt roadbed. Results from such tests are used to choose strike packages that achieve desired effects while minimizing collateral damage.

- **Data Analytics.** The DCiDE and the DIEE v2.1 targeting solution products applied advanced automated tools and analytics enabling their release in FY18. DCiDE expedites and simplifies the Collateral Damage Estimation (CDE) process while DIEE enables seamless planning and linkage to various mission planning systems. Both tools increased efficiency and optimized mission planner workflow. In FY18, the Chairman of the Joint Chiefs of Staff issued guidance for the Services, CCMDs, and Combat Support Agencies to upload and use DIEE v2.1. To further validate these automated tools, JTCG/ME initiated a CDE test program to generate data and enhance/validate current weaponeering/CDE methodologies required by Strike Approval Authorities. JTCG/ME executed four buried ordnance tests to evaluate the effects of burial medium and weapon class on warhead performance, crater ejecta, and collateral damage. The results of one of these tests are shown in Figure 2.

LFT&E SPECIAL INTEREST PROGRAMS

WARRIOR INJURY ASSESSMENT MANIKIN (WIAMAN)

In December 2017, the Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) approved the initiation of the WIAMan acquisition effort as a Limited Production Instrumentation and Testing Program. This decision supported efforts to prepare for engineering and manufacturing development activities. In June 2018, the WIAMan Engineering Office (WEO) demonstrated Technical Readiness Level 6 with the four, first generation (Gen 1) anthropomorphic test devices (ATDs), in a realistic UBB event.

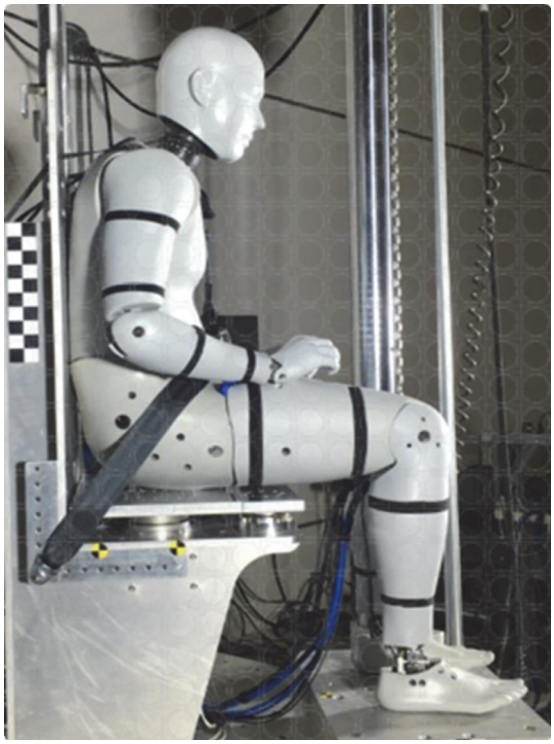


Figure 3. Generation 1 WIAMan ATD

In FY18, the WEO continued the biomechanics research to support development of both human injury probability curves (HIPCs) and injury assessment response curves (IARCs). The biomechanics team has recreated over 370 injuries in the laboratory setting that will be utilized for the development of HIPCs and IARCs. The WEO also completed the final side-by-side male/female test on the Accelerative Loading Fixture. The results of this pilot study will be used to inform a decision about the need to develop unique injury assessment capability for female soldiers. Lastly, the WEO completed a new finite element model (FEM) of the Gen 1 ATD and performed validation studies.

The Army has a requirement for 40 WIAMan ATDs. The current acquisition program is funded through FY19 and will procure up to 10 WIAMan ATDs. The Army has not yet funded WIAMan beyond FY19. The Army plans to use these WIAMan ATDs for AMPV full-up system-level testing in FY20.

COMBAT DAMAGE ASSESSMENT

JASP continued sponsoring aircraft combat damage incident reporting in the DOD through the Joint Combat Assessment Team (JCAT). The JCAT is a team of Army, Navy, and Air Force personnel that deploy to investigate aircraft combat damage in support of combat operations. The team supports assessments remotely from the continental United States and deploys outside of the United States when necessary.

JASP continued working with the U.S. Army Aeromedical Research Laboratory (USAARL) to study and document aviation combat injuries in Operation Iraqi Freedom and Operation Enduring Freedom. The results will be documented in USAARL reports and the Combat Damage Incident Reporting System (CDIRS). JASP, with the support of the Defense Systems Information Analysis Center and the National Ground Intelligence Center (NGIC), continued efforts to transition CDIRS from an Air Force SIPRNET server to NGIC hosting to enable access across the Services. The transition is expected to be complete in early FY19.

The JCAT and JASP Program Office worked in coordination with the Office of the Deputy Assistant Secretary of Defense for Systems Engineering, Office of the Under Secretary of Defense for Personnel and Readiness, and the Joint Staff's Force Structure, Resource, and Assessment Directorate to execute an Aircraft Combat Damage Reporting (ACDR) Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Policy Change Request (DCR) proposal. The JCAT and JASP are working with the Services to implement the approved DCR recommendations.

TEST AND EVALUATION OF EMERGING TECHNOLOGIES

Joint Non-Lethal Weapons (JNLW) Test and Evaluation Working-Level Integrated Product Team (T&E WIPT)

Non-lethal weapon systems are being developed, tested, and evaluated by each of the Services. In FY18, DOT&E hosted the JNLW T&E WIPT meeting in which each Service briefed its non-lethal weapons portfolio (T&E status, program successes, and failures). The JNLW T&E WIPT will become an annual forum to compare cross-Service experience in order to foster progress in non-lethal weapon systems. DOT&E is currently developing procedures by which programs in this portfolio will be evaluated in the future.

Counter-Unmanned Aerial Systems (C-UAS)

C-UAS systems continue to be developed and evaluated for military operations. In FY18, DOT&E worked with the Services to emphasize the need to test and evaluate C-UAS systems in threat-representative cellular environments. Testing will properly evaluate collateral damage concerns, and develop appropriate sensors to evaluate C-UAS system effectiveness in contested environments.

Directed-Energy Weapon T&E

A variety of directed-energy weapon systems are maturing to the point of military utility. In FY18, DOT&E worked with the Services to identify and develop T&E requirements related to laser weapons. DOT&E is working with the Services to determine how to relate meteorological conditions to laser propagation in T&E activities; develop sensors for dynamic targets; and identify methods to verify, validate, and accredit M&S tools that will be needed during future laser weapon LFT&E.

Cybersecurity

Cybersecurity

Cyber Assessments

SUMMARY

DOD missions and systems remain at risk from adversarial cyber operations. Operational tests continued to discover mission-critical vulnerabilities in acquisition programs, and assessments during Combatant Command (CCMD) training exercises continued to identify previously undetected vulnerabilities. However, there were an increasing number of instances where the cyber Red Teams employed during DOT&E assessments experienced greater difficulty in penetrating network defenses or maintaining previously acquired accesses. These improvements are both noteworthy and encouraging, but we estimate that the rate of these improvements is not outpacing the growing capabilities of potential adversaries, who continue to find new vulnerabilities and techniques to counter the fixes and countermeasures by DOD defenders.

DOT&E assessment data for this summary are based on more than 50 cybersecurity assessments with CCMDs and Services, and nearly 70 cybersecurity OT&E events (see Table 1 on page 231). Additionally, DOT&E sponsored classified assessments of nuclear command, control, and communications; cross domain solutions; data breaches; and Public Key Infrastructure. The demand for cyber expertise to plan and execute cyber assessments across the DOD, and for the in-depth analyses of the data produced by these events, is rapidly increasing and stressing available resources.

For example, the U.S. Army's Threat Systems Management Office Red Team performed more than 200 events in FY18, meeting or exceeding threat-portrayal objectives in most cases. However, DOT&E observed a growing number of instances where the Red Team needed more time to achieve objectives. This was due in part to improved network defenses, but also due to insufficient time to prepare the array of representative cyber-attacks attributed to the portrayed adversary. There remains a gap between DOD cyber Red Team capabilities and the advanced persistent threat, and assessments that do not include a fully representative threat portrayal may leave warfighters and network owners with a false sense of confidence about the magnitude and scope of cyber-attacks facing the Department. DOT&E is working with the DOD Red Teams to close that gap by helping them acquire additional personnel, more advanced capabilities, and training; however, more resources are urgently needed in this area.

Recent advances in cyber technologies indicate that automation – and even artificial intelligence – are beginning to make profound changes to the cyber domain. Warfighters and network defenders must prepare for the onslaught of multi-pronged cyber-attacks across both critical mission systems and the multitude of supporting systems and networks that enable these missions. Preparations must include realistic demonstrations of fight-through capabilities, resilience, and alternate modes when stressed by Red Teams portraying advanced adversaries. Even though directed by the Chairman of the Joint Chiefs in 2011, these realistic demonstrations have yet to become routine.

DOT&E remains committed to working with the acquisition community and operational commands in discovering and documenting cybersecurity problems, providing information to facilitate their remediation, and verifying the efficacy of solutions or mitigations.

CYBER ASSESSMENT ACTIVITY

DOT&E oversees cybersecurity OT&E for major defense acquisition programs, and performs congressionally-directed cybersecurity assessments of operational networks and systems during CCMD and Service training exercises. DOT&E also supported operational assessments of offensive cyber capabilities, and performed analyses to characterize operational implications if an adversary exploited known compromised information.

Based on results from operational tests and exercise assessments, DOT&E publishes classified reports on overarching cybersecurity topics of interest. One report published this past fiscal year explored the performance of cyber defenses against observed attacks to identify specific changes that have proven to contribute to improved defensive performance.

Operational Test and Evaluation with Cybersecurity

DOT&E continued to emphasize the importance of OT&E of cybersecurity and recommended such testing for all systems that transmit, receive, or process electronic information, by direct, wireless, or removable means. These operational tests focus on confirming that forces and units equipped with the systems can complete operational missions in a cyber-contested environment. In FY18, DOT&E monitored more than 70 such tests across 38 acquisition programs.

DOT&E published updated procedures for planning, conducting, and reporting cybersecurity testing results. DOT&E also continued efforts to improve techniques and tools for testing network gateways, non-Internet Protocol systems, and industrial control systems using the find-fix-verify paradigm.

DOT&E observed rapidly increasing demand for cybersecurity OT&E, with FY18 having the largest number of such tests. The increased demand coupled with the increase in data from the tests is stressing the test community's cybersecurity resources. Table 2 (on page 234) shows the operational test community organizations involved in cybersecurity.

Cybersecurity Assessment Program

DOT&E's Cybersecurity Assessment Program worked with the CCMDs and Services to define tailored Cyber Readiness Campaigns that help address vulnerabilities and improve cyber defense through a series of focused events throughout the year. In FY18, DOT&E provided resources for operational test agencies, intelligence subject matter experts, and DOD cyber Red Teams to plan and conduct the 54 events listed in Table 1 (on page 233). The events included assessments of physical security, focused attack techniques such as phishing, cyber activities causing mission effects, and assistance in understanding and correcting discovered problems. DOT&E published a new Cybersecurity Assessment Program Handbook of best practices and guidance to the assessment teams for planning, conducting, and reporting on the campaigns and events. As in the other areas of cyber-related activity, DOT&E observed increasing CCMD and Service demand for cyber expertise to support these assessment events.

Assessment of Offensive Cyber Capabilities

DOT&E worked with offensive cyber capability developers to integrate operationally realistic testing into the non-traditional acquisition lifecycles of these capabilities, which often involve compressed timelines. DOT&E observed or supported more than 10 such events in FY18. Concurrently, DOT&E worked with the Joint Technical Coordinating Group for Munitions Effectiveness to identify the data required to build analysis tools to predict offensive cyber effects.

Operationally, the processes for planning and employing offensive capabilities is a complex undertaking. DOT&E assessed the synchronization of cyber fires with component schemes of maneuver, integration of intelligence support, and support to commander objectives, and made recommendations to improve these critical procedures.

Persistent and Advanced Cyber Operations

DOT&E employs limited Persistent Cyber Operations (PCO) in assessments for several CCMDs. These assessments with longer dwell time afforded the PCO Red Teams time to probe deeper into network and system vulnerabilities. This approach results in assessments that are both more thorough and more threat-representative.

In addition to identifying vulnerabilities that matter to the warfighter, the PCO facilitates the development of solutions or mitigation strategies that will reduce the effect of demonstrated attacks, and performs follow-on assessments to verify the solutions work as intended. The PCO Find-Fix-Verify model is the most rapid and effective way to achieve a higher degree of cybersecurity and warfighter mission assurance.

The Advanced Cyber Operations (ACO) Team augments other Red Teams with expertise that not all Red Teams possess, leads the development and acquisition of new Red Team capabilities, and supports testing of offensive cyber capabilities as a cyber opposing force.

Cybersecurity Assessments with Coalition Partners and Networks.

DOT&E observed or assessed several events with coalition partners in FY18, and performed several Find-Fix-Verify assessments on the Combined Enterprise Regional Information Exchange System (CENTRIXS) network. During the Australian-led (U.S. Indo-Pacific Command supported) exercise Talisman Saber 19, the Australian exercise lead plans to integrate demonstrations of non-kinetic and kinetic effects to assist Blue Force training objectives. DOT&E is planning to assess bi-lateral cyber activities associated with this coalition exercise.

Cyber Ranges

For the last several years, DOT&E advocated for a cyber range structure that supports both test and training requirements. Because of the similarity of functions in test and training, a common architecture across these ranges is needed to provide efficiency and flexibility to address the increasing demand for cyber range resources, and to effectively respond to rapidly evolving and increasingly sophisticated cyber threats

DOT&E engaged with the Persistent Cyber Training Environment (PCTE) program to monitor their technology assessments, advocate for the acquisition of effective and suitable range capabilities, to collaborate in the development of a test and evaluation approach, and to encourage dual-use across test and training ranges. In 3QFY19, DOT&E will co-sponsor a range demonstration with the PCTE program and the Test Resource Management Center that will examine emerging technologies such as automated opposing force capabilities and continuous monitoring for network defense. DOT&E is also interacting with both test and training communities to promote a clear understanding of cyber-range requirements, common architectures, and standards.

Engagement with the Intelligence Community

DOT&E formed a team of engineers, system designers, system operators, cyber Red Team members, Intelligence Community experts, and program representatives to characterize the operational risk posed by program information that is known to be compromised. The assessments combine the insights from the subject matter experts to identify and then confirm vulnerabilities and attack techniques to inform mitigation efforts. The positive reception to the first reports by senior DOD leadership led to demand for additional efforts for other programs and systems. Here, as with the other cyber efforts, the demand is outpacing and stressing available resources.

Coordination with USD(A&S) on Statutory Cybersecurity Assessments

In FY18, DOT&E continued collaboration with USD(A&S) for cyber assessments of major DOD weapons systems, as directed by section 1647 of the FY16 National Defense Authorization Act (NDAA). DOT&E invited USD(A&S) representatives to participate in cybersecurity assessments with the DOT&E Cybersecurity Assessment Program when the events included systems of mutual interest.

OBSERVATIONS

This section describes noteworthy observations from FY18 exercise assessments and special evaluations. Most of the observations highlight the challenges facing the DOD in securing networks and supporting critical missions with survivable and resilient capabilities, but several include positive themes that network defenses have improved over the past several years. However, the tenuous balance between network defense and adversary capabilities leans heavily in the favor of potential adversaries, and the DOD must continue to emphasize the importance of cyber expertise at all levels and in all mission areas: warfighter, network defenders, leadership, and assessors. The summary areas each warrant continued monitoring and further assessment. DOT&E can provide more detailed classified information on each topic.

Leadership Emphasis on Cybersecurity of Warfighter Networks. DOT&E performed an assessment of a major command which identified several vulnerabilities that could impact mission assurance. Senior leadership at the command self-reported to senior DOD leadership that the command's mission assurance posture was potentially degraded, and made mitigation of these vulnerabilities a top priority. Within 60 days, all identified vulnerabilities had been remedied, were verified by the assessment team, and the command leadership reported that their mission assurance posture had improved. This example of a rapid "Find-Fix-Verify" cycle is an objective of all DOT&E cybersecurity assessments.

Nuclear Command, Control, and Communications (NC3). Protected, assured, and resilient command, control, and communications are essential for all military operations and especially so for the NC3 components of our national capability. At the request of the DOD Chief Information Officer (CIO) and the Defense Threat Reduction Agency (DTRA), DOT&E participated in classified cybersecurity assessments to characterize the status and identify options for improving the mission assurance and cyber-related aspects of the NC3 capability.

Legacy Systems and Cybersecurity. DOT&E performed several preliminary assessments of systems and networks that had been developed and fielded several decades ago, and which were widely believed to be safe from current-era cyber-attacks. However, initial findings identified technology updates that were not part of the original design or security plan and which could provide avenues for a cyber-attack.

Trust Relationships Facilitate Adversary Cyber-Attacks. The network compromises achieved by a Red Team during an assessment at one command allowed a separate Red Team – portraying a common adversary – to attack a different command. Trust relationships are critical to the operational support relationships between separate warfighter commands, but they must be designed and monitored to prevent mission impacts by adversaries.

Physical Security Linkage to Cybersecurity. DOT&E continues to assess physical security of facilities and installations because lapses in these areas can enable cyber-attacks. One assessment in FY18 found a serious set of cyber and physical vulnerabilities that, if exploited, could degrade critical missions. The DOD leadership, supported by DOT&E, took immediate steps to prevent a similar exploit in the future; DOT&E plans to provide independent verification of the efficacy of the remediation actions taken.

Stolen Credentials. Multiple DOT&E assessments – as well as commercially available information – confirm that credential theft is one of the most common cyber-attack actions that leads to data breaches. Credential theft is attractive to both DOD Red Teams and cyber adversaries because of the reduced risk of detection associated with using stolen credentials compared to other hacking tools and techniques. DOT&E works with acquisition programs and operational organizations to identify and amend practices that enable compromise of credentials.

Breaches of Cleared Defense Contractors. DOT&E worked with law enforcement and the intelligence community to understand the potential impacts from past breaches on DOD systems and networks. DOT&E led several multidisciplinary teams in the evaluation of specific systems to assess the potential value to adversaries of known compromised information. These evaluations extended beyond list reviews of compromised documents, and included deeper analyses by Red Team personnel to identify how compromised information could be aggregated to enhance a potential cyber-attack. DOT&E communicated assessment results to appropriate DOD leadership and program officials, with the recommendation that additional resources be provided to expand this important assessment mission.

Operational Cyber Defenses. DOT&E performed analyses on 4 years of exercise assessments (FY14-17) to examine the changing nature of DOD cyber defenses. The analysis identified that defenders demonstrated increasing ability to detect Red Team activity, that Red Teams prefer to employ stolen credentials over software vulnerabilities, and that defenders need to improve speed and accuracy for processing reported incidents. DOT&E identified additional recommendations in this classified report to further improve the defensive posture and DOD mission assurance.

Cyber Expertise of Red Teams. DOT&E employs cyber Red Teams in most assessments, and in FY18, there were several instances where Red Teams were not available to support an assessment. In FY19, DOT&E intends to execute assessments where more advanced threat portrayal will be required, and the ability of Red Teams to meet these requirements is in question.

Currently Red Teams lack the time and funding to develop new tools and capabilities. The manning models for the Service Red Teams vary widely and are not uniformly successful. Reviews

of the capabilities of several Red Teams in FY18 showed that the best teams were overscheduled and overwhelmed by workload.

As demand for cyber Red Teams continues to increase, DOT&E observed numerous losses of master-level Red Teamers in FY18 to commercial jobs that were higher paying or which required less travel. Red Team capacity and retention options must be increased to meet the demands of testing, training, and other assessment activities.

IMPROVING CYBERSPACE OPERATIONS – OPERATORS AND AUTOMATION ARE KEY

Test and assessments in FY18 again found that low-capability attack techniques too often posed a risk for disrupting operational missions, however, DOT&E observed instances of successful cyber defense operations. A common thread running through these successful operations was the presence of a knowledgeable cyber operator with adequate defensive technology and tools.

DOT&E identified five improvement areas to enable cyber defenders to do their jobs well:

- Scope the task by defining the key cyber terrain, operational missions, tasks, and expectations.
- Foster unity of effort amongst participants that have different roles (offensive, defensive) and responsibilities (internal and external to assigned key cyber terrain).
- Know the key cyber terrain, operational concepts, and available tools.
- Match tools and skills to the operational tasks, missions, and key cyber terrain.
- Practice and train in operationally representative conditions against realistic cyber-attacks.

Scope the Task

- Focus defenders on mission-critical cyber terrain and provide appropriate technology such as real-time sensors and monitoring.
- Minimize the attack surface of mission-critical cyber terrain by using technologies such as Virtual Desktop Infrastructure, best practices such as segregated network enclaves, rigorous configuration management, and eliminating non-mission-critical connections.

Foster Unity of Effort

- Establish a centralized and standardized cyber reporting process that includes the necessary analytics and forensics.
- Develop and deploy cyber situational awareness tools.
- Establish specific duties, responsibilities, and tools to coordinate the activities of local defenders, help desks, system managers, and other key cyber defensive teams. A "one-size-fits-all" model does not work well.

Know the Terrain

- Identify and monitor mission-critical cyber terrain.
- Provide terrain-specific tools and training for needed skills such as automated monitoring, analysis, and forensics.
- Provide system and terrain-specific tools to automate configuration management, system backups, system isolation, and restoral.
- Establish mission and terrain specific training for cyber defenders.

Match Tools and Skills to the Task

- Establish a federated approach to cyber defense, vice relying on network boundary defenses, e.g. stop "flattening" the networks and relying on defensive tools at the network boundary.
- Work with academia, the private sector, and national labs to improve defensive cyber techniques, tools, and technologies.
- Pair automated tools to the specific attributes of the systems and networks defended, and provide defenders training on those tools.

Practice and Train

- Establish PCO (both automated and human penetration testing) on all mission-critical DOD cyber terrain to reflect current threats, attack vectors, and known exploits.
- Develop tools to help automate cyber-attacks to supplement and support cyber teams. This automation will help reduce the deficit in Red Team resources, and allow for continuous testing of acquisition programs and continuous monitoring of operational networks.

TABLE 1. CYBERSECURITY OPERATIONAL TESTS AND ASSESSMENTS IN FY18		
EVENT TYPE	**ACQUISITION PROGRAM OR TYPE OF EVENT**	
Programs Completing Operational Tests of Cybersecurity	Amphibious Combat Vehicle	Global Command and Control System – Joint
	AEGIS Modernization (Baseline Upgrades)	Global Positioning System Next Generation Operational Control
	Armored Multipurpose Vehicle	Integrated Personnel and Pay System – Army Increment 2
	AN/APR-39 Radar Warning Receiver	Integrated Strategic Planning and Analysis Network Increment 4
	Air Operations Center – Weapon System 1	Joint Air-to-Ground Missile
	Army Tactical Missile System – Service Life Extension Program	Joint Light Tactical Vehicle
	Ballistic Missile Defense System Program	Joint Precision Approach and Landing System
	Coastal Battlefield Reconnaissance and Analysis System	Joint Warning and Reporting Network
	Command Post Computing Environment	Key Management Infrastructure Increment 2
	Distributed Common Ground System - Army	Mounted Computing Environment
	Defense Enterprise Accounting and Management System	Near Real Time Identity Operations
	DOD Healthcare Management System Modernization	P-8A Poseidon Program
	Enclave Control Node	Paladin/FASSV Integrated Management (PIM)
	Enhanced Polar System	Public Key Infrastructure Increment 2
	F-35 – Lightning II Joint Strike Fighter Program	Stryker Family of Vehicles to include all variants
	Family of Beyond Line-of-Sight Terminals	Teleport, Generation III
	Fire Scout Unmanned Aircraft System	Triton
	Global Hawk Unmanned Aircraft System Multi-Spectrum Sensor	UH-60V BLACKHAWK
	Ground/Air Task Oriented Radar	Unmanned Aircraft System Gray Eagle
Cybersecurity Assessment Program	**Physical Security Assessment (2 Events)** U.S. Navy, U.S. Special Operations Command (USSOCOM)	
	Cooperative Network Vulnerability Assessment (4 Events) U.S. Air Force, U.S. Africa Command (USAFRICOM), U.S. Central Command (USCENTCOM) (2)	
	Cyber Operations (7 Events) U.S. Navy, USAFRICOM (2), U.S. Indo-Pacific Command (USINDOPACOM) (3), U.S. Northern Command (USNORTHCOM)	
	Mission Effects with Cyber Operations (29 Events) U.S. Air Force (2), U.S. Army (2), U.S. Forces Kores (2), U.S. Navy (2), USAFRICOM, USCENTCOM, USINDOPACOM (7), USNORTHCOM (2), USSOCOM (3), U.S. Southern Command (USSOUTHCOM), U.S. Strategic Command (USSTRATCOM) (3), U.S. Transportation Command (USTRANSCOM)	
	Targeting Processes for Offensive Cyber Operations USINDOPACOM	
	Dedicated Phishing Campaign USAFRICOM	
	Range Event U.S. Army	
	Sharing Solutions Fix Event (8 Events) U.S. Air Force (2), U.S. Forces Korea (2), U.S. Cyber Command (USCYBERCOM) (2), USINDOPACOM (2)	
	Table Top Exercise U.S. Navy	

TABLE 2. CYBERSECURITY TEST COMMUNITY	
OPERATIONAL TEST AGENCIES	
Military Services	Air Force Operational Test and Evaluation Center
	Army Test and Evaluation Command
	Navy Operational Test and Evaluation Force
	Marine Corps Operational Test and Evaluation Activity
Defense Agencies	Joint Interoperability Test Command
CYBER TEAMS	
Air Force	57th Information Aggressor Squadron
	177th Information Aggressor Squadron
	92nd Cyberspace Operations Squadron
	46th Test Squadron
	18th Flight Test Squadron
	Air Force Information Operations Center
	688 Information Operations Wing
Army	1st Information Operations Command
	Threat Systems Management Office
	Army Research Laboratory, Survivability/Lethality Analysis Directorate
Navy	Navy Red Team
	Space and Naval Warfare Systems Command Red Team
	Navy Operational Test and Evaluation Force
Marine Corps	Marine Corps Red Team
Defense Agencies	National Security Agency
	Defense Information Systems Agency Red Team

Test and Evaluation Resources

Test and Evaluation Resources

Test and Evaluation Resources

Public law requires DOT&E to assess the adequacy of test and evaluation (T&E) resources and facilities for operational and live fire testing and evaluation. DOT&E monitors and reviews DOD- and Service-level strategic plans, investment programs, and resource management decisions so that capabilities necessary for realistic operational and live fire tests are supported. This report highlights areas of concern in testing current and future systems and discusses significant challenges, DOT&E recommendations, and T&E resource and infrastructure needs to support operational and live fire testing. FY18 focus areas include:

- Hurricane Damage to T&E Infrastructure
- Personnel and Capabilities to Support Cyber-related Operational Testing
- Threat Representation for OT&E of Space Systems
- Automated Ballistic Missile Flight Termination Systems
- Nuclear Survivability Test Capability
- Directed-Energy Weapons T&E
- Counter-Unmanned Aerial Systems T&E
- Advanced Electronic Warfare Test Resources for Air Warfare
- Range Enhancements to Support OT&E of Air Warfare Programs
- Fifth-Generation Aerial Target
- Aircraft Survivability Equipment Test Capability Gaps
- Navy Advanced Electronic Warfare Test Resources and Environments
- Ship Self-Defense Test Capabilities
- Multi-Stage Supersonic Targets
- Torpedo Surrogates for Operational Testing of Anti-Submarine Warfare Platforms and Systems
- Submarine Surrogates for Operational Testing of Lightweight and Heavyweight Torpedoes
- Army Support of OT&E
- Electronic Warfare for Land Combat
- Tactical Engagement Simulation with Real Time Casualty Assessment
- Test and Evaluation of Army Software-Defined Tactical Radios
- Warrior Injury Assessment Manikin
- Foreign Materiel Acquisition Support for T&E
- Range Sustainability

Hurricane Damage to T&E Infrastructure

Hurricane Michael significantly damaged the infrastructure at Tyndall AFB, Florida; Naval Surface Warfare Division (NSWC) Panama City Division (PCD); and the Gulf of Mexico (GOMEX) operating area when it made landfall in October 2018. The storm effect to the test infrastructure at Tyndall AFB included severe damage to the Air Force's primary/preferred BQM-167 aerial target launch site and primary QF-16 aerial target base and test control and range support structure. Two QF-16 unmanned aerial targets were damaged beyond repair. Range safety boat piers were damaged, and one of three range safety and subscale recovery boats was beached and needed recovery by the Navy. Damage to T&E infrastructure such as radar and telemetry antennas extended along the GOMEX coast as far as Eglin AFB.

The Air Force estimates that Tyndall AFB will be unavailable for target support from 6 months up to 3 years. Losses to T&E instrumentation such as telemetry and radar systems in the Florida pan handle are estimated at $65 Million. Although these capabilities exist at other ranges, their temporary unavailability at Tyndall AFB will cause inefficiencies in acquisition test programs requiring these test assets through the spring of 2019. Although a back-up capability resides at Holloman AFB, New Mexico, some maintenance and operational manpower augmentation from Tyndall's manpower pool are required. However, Tyndall manpower is limited while they salvage their personal property and homes which were heavily damaged or destroyed by Hurricane Michael. Additionally, increased testing at Holloman AFB will affect scheduling of airspace at White Sands Missile Range, New Mexico.

Hurricane Michael caused significant damage to the infrastructure and multiple research, test, and training facilities at NSWC PCD, limiting access to the base for several weeks. Recovery costs are estimated to be $238 Million. NSWC PCD was not fully staffed through October 2018 while personnel dealt with the hurricane damage to personal property. NSWC PCD testing for several mine countermeasures programs was delayed for more than 2 months due to this storm.

Earlier in 2018, Hurricane Florence downed trees that damaged fences and caused electric outages for the eastern shore towers at Aberdeen Test Center in Maryland used for range safety observations and noise management. Repairs were quickly implemented and did not impact testing. Repair costs were estimated at $2,500.

Personnel and Capabilities to Support Cyber-related Operational Testing

Well-qualified personnel and effective, up-to-date test capabilities are essential to planning and conducting adequate, operationally threat-representative cybersecurity testing. Currently, the DOD has had difficulty hiring and retaining cybersecurity

professionals, and lacks the resources to develop and field specialized, automated cybersecurity test tools. Meanwhile, the demand for cybersecurity testing continues to grow in both the government and private sectors. The Operational Test Agencies (OTAs) and cyber Red Teams currently do not have enough experienced cybersecurity professionals to accommodate the increasing number and complexity of test events projected in FY19 and beyond, and lack the funds and expertise to develop specialized cybersecurity test tools.

To address this problem, the DOD must overcome significant barriers:

- There is a global shortage of cyber expertise driving up the cost to hire well-qualified cyber people. A 2017 Global Information Security Workforce Study sponsored by the non-profit International Information System Security Certification Consortium forecasts 1.8 million unfilled cybersecurity positions globally by 2022. Currently, there are close to 300,000 unfilled positions in the United States alone. The OTAs have over 30 unfilled cybersecurity T&E billets, representing almost a fifth of the current OTA manning structure.
- Most cybersecurity positions within the Department are not compensated commensurate with the position's required experience and expertise. Further, it takes considerable time and specialized on-the-job training to develop a skilled workforce to perform cybersecurity testing of weapons systems. Once trained, the risk of losing experienced cybersecurity personnel to the private sector is high due to the compensation differences, creating an ongoing challenge to maintain and grow an experienced DOD cybersecurity workforce.
- The DOD reliance on software-intensive weapons systems creates a need to not only test traditional information technologies, but also other capabilities: vehicle and aircraft data buses, radar and acoustic systems, radio frequency (RF), wireless, and the datalinks that support DOD weapons systems. Cybersecurity testers in the DOD are handicapped by lack of expertise and developmental support to obtain test capabilities and tools to address these areas.

In order to obtain top-notch cyber talent, the Department should secure seed funding for a select group of Service academies, private companies, universities, and national laboratories to grow the DOD cybersecurity testing workforce and capabilities. Hiring more cyber experts will not be enough. The large and chronic lack of qualified cyber personnel means that there will never be enough cyber experts to adequately cyber-test all DOD networks and systems. The Department should focus some of the newly-acquired cyber expertise on the development of advanced, automated cybersecurity test tools to augment the skills of cyber testers and provide additional test capacity.

If implemented, these recommendations will enable more threat realistic cybersecurity assessments for critical networks and systems across the DOD. Doing so will permit the Department to more effectively conduct its missions in the cyber-contested environments of today and the future.

Threat Representation for OT&E of Space Systems

U.S. adversaries are actively pursuing offensive space control capabilities to diminish and overcome U.S. military space superiority. Although the Services normally test space systems against representative natural hazards and space phenomena, they have not adequately tested them against representative threats emulating the full spectrum of hostile environments. Within the T&E community, there are limited infrastructure, tools, and resources for realistic representation of the space threat.

Several DOD laboratories have threat-representative systems (e.g., laser, high-energy chambers, etc.); however, the Service OTAs and Program Offices have not made use of these assets. The Intelligence Community also has some space threat modeling tools that have not yet been utilized.

In a memorandum dated March 2016, DOT&E provided guidance to the Service acquisition officials and OTAs to improve their ability to identify and track space threat representation capabilities; identify space threat representation gaps, and request funding to fill those gaps; and to develop modeling and simulation (M&S) capabilities to support the assessment of space threats. To enable adequate testing using threat systems and threat surrogates against satellites for OT&E, the Services should fund pre-launch testing of either first articles or production-representative "test satellite" articles against all validated threats. Representative operational crews should operate satellites being threat tested for OT&E using the ground stations that control the satellites and capabilities intended for operational employment. Post-launch, the Services should fund threat-representative articles through the operational life of space systems to support ground testing and training against an evolving threat; system-of-systems assessments; ongoing tactics, techniques, and procedures (TTP) development; and exercises.

The OT&E of space systems must reflect all threats that U.S. space systems will face, and the Services should provide the additional resources required to ensure these threats are realistically represented and assessed during OT&E. Air Force Operational Test and Evaluation Center (AFOTEC) and the Air Force Space and Missile System Center Program Offices need to define their test resource requirements for contested space. Additionally, the DOD needs to prioritize space threat test resources in the budget cycle to support development of the necessary infrastructure for contested space and space-threat testing. Although the Air Force conducted analysis to determine threat test resource needs and submitted requirements for funding, the submission was not funded to support realistic operational testing.

Automated Ballistic Missile Flight Termination Systems

Locations for ballistic missile flight test are limited to test ranges using safety systems employing range-certified flight termination systems onboard the ballistic missiles. The operational realism and number of ballistic missiles involved in a single flight test is capped by the number of available safety systems. For example, the Missile Defense Agency's Flight Test, Integrated-03 (FTI-03) had to be reduced in content by 50 percent due to the

loss of a range safety ship that required unexpected mandatory maintenance.

Ballistic missile safety systems are typically labor- and resource-intensive. In addition to its flight termination system, each ballistic missile requires multiple sources of independent position and velocity data to be supplied in real-time to its dedicated safety system. Automated flight termination systems are already in use in some applications, but are not wide-spread across current DOD ranges that conduct ballistic missile flight testing. Expanded certification of Automated Ballistic Missile Flight Termination Systems for use on DOD ranges would provide significant resource efficiencies and test flexibility to the ballistic missile test community. However, the ranges must continue to maintain access to man-in-the-loop commanded flight termination systems until availability of automated solutions and entry cost for implementation is improved.

Nuclear Survivability Test Capability

Nuclear survivability T&E capabilities must enable adequate assessment of system performance in nuclear blast environments. While the Department has reconstituted some capabilities such as the Large Blast Thermal Simulator (to assess thermal shock and follow-on blast effects) and the Fast Burst Reactor (to generate neutron flux environments), several nuclear survivability T&E infrastructure gaps remain. The DOD should continue with the advancements to enable:

- Survivability assessments of a full ship at sea, in an operational mode, subjected to electromagnetic pulse (EMP) effects. Although the Navy is attempting to pursue full-ship EMP hardening T&E via Low-Level Continuous Wave Illumination coupled with M&S, this method will only provide limited information on ship survivability with significant uncertainties.
- Assessments of DOD systems in cold and warm X-ray enivornments generated by nuclear blasts. Improved T&E capabilities are needed to advance understanding of cold/warm X-ray environments on systems and improve M&S tools. In FY18, the Central Test and Evaluation Investment Program (CTEIP) sponsored the development of a design solution for X-Ray Simulators for Test and Evaluation of Nuclear Survivability (XSTENS). However, these X-ray simulators will not test cold X-ray system impulse effects.
- Assessments of DOD systems exposed to radioactive dust suspension after a nuclear blast. The combined abrasive and chemical effects of such dust could cause damage to optical sensor windows, leading surface edges, and hot engine components. Improved test capabilities are needed to enable accurate assessment of the durability of U.S. military systems in such an environment.

Development of the nuclear survivability T&E infrastructure will support mission assurance, the U.S. nuclear deterrent posture, and enhance national security. DOT&E supports ongoing efforts to address current nuclear survivability testing shortfalls.

Directed-Energy Weapons T&E

The recent advancements of directed-energy weapons (high-energy lasers and high-power microwaves) warrant commensurate advancements of the test infrastructure and evaluation methods to adequately measure the capabilities and limitations of such systems in relevant operational environments. Directed-energy weapons use a different damage mechanism (function of atmospheric conditions, dwell time, and power) than kinetic weapons (function of fragments/blast) presenting unique T&E challenges that need to be addressed.

The T&E infrastructure is currently not set up to fully assess changes in laser performance as a function of temperature, pressure, humidity, vibration, and other environmental and atmospheric conditions. To enable more adequate assessment of the lethality of directed-energy weapons across the spectrum of relevant operational conditions, the DOD needs to identify and construct a metrology equipment suite capable of measuring atmospheric reference data relevant to laser propagation. The DOD should then develop tools to allow for a more adequate characterization and linkage between the atmospheric reference data and effects on laser propagation due to turbulence, extinction, and thermal blooming. This T&E infrastructure enhancement will enable the development of a standard and consistent T&E protocol (with associated metrology data) to measure and predict laser propagation as a function of a spectrum of operationally relevant atmospheric conditions.

The DOD should also develop hardware-in-the-loop facilities to more efficiently assess laser effects on targets. This will require development of instrumented threat surrogates capable of measuring incident laser irradiance in real-time. These instrumented threat surrogates should be reconfigurable, reusable, and/or expendable. Programs such as the Big Area Target System and the Irradiance Collection and Reporting System are critical steps in the advancement of this T&E capability and require continued development and resourcing.

Future instrumented threat surrogates will also require calibration designed to support verification, validation, and accreditation of laser propagation M&S tools. Adequate M&S tools would enable the DOD to estimate directed-energy weapons damage effects on various targets. These capabilities would also enable the DOD to define the TTP needed not only to execute relevant operational T&E events but to plan future operations and missions with directed-energy weapons. Lastly, the M&S tools need to adequately capture collateral effects (due to laser reflections) so that risk to operational T&E events and combat missions can be safely assessed.

Counter-Unmanned Aerial Sysems

The DOD has been developing an array of technologies, both kinetic and non-kinetic, to counter unmanned aerial systems (UAS), a growing threat to U.S. warfighters, equipment, and facilities. A more adequate evaluation of counter-UAS (C-UAS)

capabilities, in a range of contested environments, requires advancements in C-UAS test infrastructure, instrumentation, and UAS targets.

- C-UAS need to be evaluated in an operationally relevant cellular environment that adequately represents the threat command and control (C2) system. This requires investment in the Advanced Cellular Communication Network (ACCN) test infrastructure equivalent to those deployed globally. Test ranges are in need of various software upgrades and firmware patches to existing cellular infrastructure as well as modernization of signal generation, monitoring, and instrumentation to address expanded 4G and new 5G communications standards.
- Current range infrastructure is short of GPS trackers as well as appropriate high-speed cameras, optical sensors, and radar systems to evaluate the variety of C-UAS under test. Ranges require expanded fiber-optic test networks to enable the extension of high-speed data acquisition systems.
- Ranges also need additional optical imaging and tracking systems to enable the simultaneous tracking of multiple targets.
- Relevant diagnostics need to be developed to support T&E lethality evaluation for non-kinetic kill mechanisms (such as jamming), particularly if the kill mechanism does not cause a recognizable, catastrophic kill. Mission kills (e.g., the threat has effectively been denied the ability to complete its mission due to sensor losses) can be difficult to detect with the current T&E infrastructure of ground sensors.
- As the swarm threat proliferates, additional investment will be required for instrumentation to quantify the significance of the effect on individual elements and potential interaction between elements within a swarm. Miniaturization of threat instrumentation to enhance test capability to meet future swarm test is an area that also requires investment.

Advanced Electronic Warfare (EW) Test Resources for Air Warfare

In February 2012, DOT&E identified significant shortfalls in EW test resources – in particular surface-to-air threat representation on the open-air ranges, which resulted in nearly $500 Million of funding for the Electronic Warfare Infrastructure Improvement Program (EWIIP). The intent of EWIIP was to buy ground radar emulators for the open-air ranges, provide corresponding upgrades to anechoic chambers and the Joint Strike Fighter (F-35) mission data file reprogramming lab, and provide intelligence products to support the development of the threat emulators.

Table 1 displays the status of various components of the EWIIP effort.

TABLE 1. RECOMMENDATIONS ON ELECTRONIC WARFARE TEST RESOURCES

DOT&E Recommendation	Current Status
Develop a combination of open- and closed-loop ground radar emulators in the numbers required for operationally realistic open-air range testing.	EWIIP has delivered open-loop systems, called Radar Signal Emulators (RSEs) that are currently undergoing integration into range infrastructure for use in OT&E. The EWIIP Closed-Loop PESA* Simulator (CLPS) systems are scheduled to deliver in the spring of 2020. *Passive Electronically-Scanned Array
Provide Integrated Technical Evaluation and Analysis of Multiple Sources intelligence products needed to guide threat simulations.	Products delivered and in use to support development of the open- and closed-loop threat radar emulators.

Range Enhancements to Support OT&E of Air Warfare Programs

In 2015 and 2016, DOT&E and USD(AT&L) allocated $22 Million to fund integration of the Air Warfare Battle Shaping (AWBS) system and Radar Signal Emulators (RSEs). AWBS is a variant of the Air-to-Air Range Instrumentation system used for scoring and post-mission reconstruction and analysis of OT&E missions. Use of RSEs with AWBS will provide operationally realistic scenarios and lessen some of the test and training requirements at other ranges. Additionally, conducting test trials at multiple range locations could shorten the duration of various tests. AWBS is projected to declare basic Initial Operational Capability (IOC) in early 2019, followed by full integration of the RSEs for use in test by late spring 2019.

Fifth-Generation Aerial Target (5GAT)

DOT&E has been investigating the means to develop a full-scale aerial target to represent the characteristics of fifth-generation threat aircraft in order to adequately assess the performance of current and future U.S. air defense weapon systems. The 5GAT study effort began in 2006 and examined the design and fabrication of a dedicated 5GAT. The 5GAT team – comprised of Air Force and Navy experts, retired Skunk Works engineers, and industry experts – completed the preliminary design in 2016. The fully owned Government design includes the aircraft outer mold line, internal structures, loads analysis, propulsion, and subsystems. The DOD provided additional funding in FY18-19 to complete the final design, tooling, fabrication, and flight tests (FY19), and to build a second prototype. The 5GAT effort is currently building the first demonstration prototype, including flight propulsion, system integration, and flight simulation/verification activities. The team built one full-scale, flight-representative wing that will be used for structural load tests and a system integration laboratory, as well as a full-scale test article for radar cross-section testing. The prototyping effort will provide cost-informed alternative design and manufacturing approaches for future air vehicle acquisition programs, and

verified cost data for all-composite aircraft design/development, alternative tooling approaches, and innovative management applications. The 5GAT effort can also be used to assist with future weapon system design/development, planning and investment, and future analysis of alternative activities. It is also intended to demonstrate reduced signature, basic aerodynamic performance, alternative cost models for aircraft development, and provision for special mission systems.

Aircraft Survivability Equipment Test Capability Gaps

To support aircraft survivability equipment (ASE) testing for high-priority threats, DOT&E and TRMC updated the Infrared Countermeasure Test Resource Requirements Study (ITRRS), which identified shortfalls in infrared countermeasure (IRCM) testing and developed a prioritized IRCM investment roadmap of projects to mitigate current testing shortfalls. The ITTRS priorities include:

- Upgrades to both open-air test ranges and indoor test facilities needed to test the latest missile warning systems and IRCM
- Open-air test range improvements that include additional firing points for multi-threat environments and angular separation, upgrades to improve test efficiency, improved instrumentation, and jitter and atmospheric distortion measurement capability
- Upgrades to hardware-in-the-loop and installed system test facilities to better represent the latest threats in a simulated operational environment
- Expansion to heavily-utilized, hardware-in-the-loop, and installed system test facilities to better support program test schedules
- Increased dynamic range and fidelity for ground-based missile plume simulators to expand their testing envelopes
- Improved surrogate threat missiles to support open-air testing
- Increased cooperation among the military and intelligence agencies to collect more threat systems
- Threat system storage facilities to store actual threats as they become available
- Airborne signature measurement

A high ITRRS priority is the ability to measure threat signature data for the development or improvement of the threat models for IR-guided missiles and unguided hostile fire munitions used for the T&E of ASE. These signature models drive a large number of T&E simulation tools. The DOT&E Center for Countermeasures (the Center) is the executing activity for the Joint Standard Instrumentation Suite (JSIS) project. JSIS is an integrated suite of instrumentation designed to mitigate the threat signature data gap, as well as provide ground truth for live fire missile and hostile fire tests for IRCM system testing. A JSIS IOC supported two threat live fire events this fiscal year. JSIS Full Operational Capability (FOC) development will begin in FY19 and deliver additional capabilities for use as they become available. FOC is required to meet the needs of current and future missile warning systems.

In a complementary effort, DOT&E and TRMC drafted threat M&S capability investment roadmaps addressing M&S investment needs for both IR and RF threats, ensuring adequate evaluation of airborne combat systems. These roadmaps identified projects for new threat model development for current and emerging threats, updates to existing models, enhanced intelligence community threat assessments of current and emerging threats, and implementation of a threat M&S for the T&E enterprise management process. As a result of these roadmaps, funding was allocated to develop 10 IR and 10 RF high-priority threat models not currently available for T&E.

In addition to threat signature data, time, space, and position information (TSPI) is critical to understanding threat missile performance, building the threat fly out model, and evaluating system under test performance. The DOT&E T&E Threat Resource Activity (DOT&E/TETRA), with support of the Center, is leading the Advanced Satellite Navigation Receiver project in FY19 to equip small threat missiles with a telemetry pack that will provide accurate position information, guidance signals, and other advanced capabilities for testing ASE in live fire testing. The current capability is limited and parts obsolescence will halt future procurement by 2021. This new capability is intended to improve current and future threat fly out models and reduce test costs. Current funding is sufficient to begin the design work and reduce technical risk, but future funding will be necessary to complete the design and produce the first articles for evaluation.

Navy Advanced Electronic Warfare Test Resources and Environments

Improving Capability to Realistically Represent Multiple Anti-Ship Cruise Missile (ASCM) Seekers for Surface Electronic Warfare Improvement Program (SEWIP) Operational Testing

A gap in the ability to realistically represent multiple ASCM seekers during test was initially identified in this section of the DOT&E FY13 Annual Report. The Navy subsequently developed a programmable seeker simulator that could represent different ASCM seekers by specifying electronic waveform emission characteristics for one of several possible threats. However, the effective radiated power (ERP) was not among those characteristics, resulting in simulated attacks by ASCM representations displaying disparate levels of ERP that are unlikely to be encountered during a stream raid attack of two ASCMs (along the same bearing and elevation and within close proximity of one another). The programmable seeker simulator, termed the "Complex Arbitrary Waveform Synthesizer," should be modified such that its ERP more realistically represents the second ASCM of a dual ASCM stream raid.

The next SEWIP Block 2 FOT&E is projected for FY20 on a Product Line Architecture-compliant DDG 51 with Block 2 integrated with the Aegis Combat System. This integration was not part of the Block 2 IOT&E. Subsequent FOT&E is intended with the DDG 1000 destroyer and CVN 78 aircraft carrier combat systems.

Improving the Fidelity of ASCM Seeker/Autopilot Simulators for EW Testing

DOT&E initially identified a gap in the fidelity of ASCM seeker/autopilot simulators in the this section of the FY13 Annual Report. The gap arose because of continued reliance on manned aircraft for captive-carry of ASCM seeker simulators. This had only a limited effect on SEWIP Block 2 IOT&E, but will severely limit the adequacy of SEWIP Block 3 IOT&E. Captive-carried ASCM seeker surrogate limitations restrict their usefulness for SEWIP Block 3 operational tests. First, it is difficult to tell if the SEWIP Block 3 electronic attack (EA) is having the desired effect on the captive-carried ASCM seeker. Second, the captive-carried simulators do not demonstrate a kinematic response to EA by SEWIP Block 3 and thus do not demonstrate the effect that such kinematic responses will have on ships' hard-kill systems (e.g. missiles, guns). Third, Learjet aircraft that carry the captive-carried ASCM seekers do not fly fast enough to be credible representations of ASCM threats. Fourth, because Learjets fly substantially higher than ASCMs, the RF environment experienced by the captive-carry ASCM surrogate is different than that of an actual ASCM. These differences may make the captive-carry results unrealistic. Lastly, the Navy has very few captive-carry ASCM surrogates with which to test and many are not representative of modern ASCM threats. To mitigate these limitations, the Navy needs to develop high-fidelity ASCM surrogates that can be used to control aerial targets. These closed-loop targets could be used to demonstrate SEWIP Block 3 operational effectiveness in live testing. If these limitation are not mitigated it is unlikely that the Navy's current test assets will be able to credibly determine SEWIP Block 3 operational effectiveness. SEWIP Block 3 IOT&E is projected for FY23 on a DDG 51-class ship.

Developing Test Surrogates for Hostile Airborne and Surface Radar Systems

In addition to the ASCM surrogates described above, adequate operational testing of active EA systems like SEWIP Block 3 require development of threat airborne and surface (e.g., coastal defense) radars that active EA systems may be required to thwart. The Navy tests such capababilities at the Shipboard Electronic Systems Evaluation Facility (SESEF), where a pulse generator, known as the Combat Electromagnetic Environment Simulator (CEESIM), an amplifier, and an antenna are used to emulate hostile radars. Such test facilities provide some capability to demonstrate an EW system's ability to detect and identify threat radars, but the existing capability is not adequate to test EA systems. To test such systems, the threat radar surrogate must emulate the RF aspects of the threat radar, the signal processing of the radar, and the electronic protection aspsects of the radar. In October 2016, DOT&E directed the Navy to develop such threat radar surrogates. Without such test assets, it is unclear how the Navy will credibly test active EA systems like SEWIP Block 3.

Ship Self-Defense Test Capabilities

The close-in ship self-defense battlespace is complex and presents a number of challenges. For example, this environment requires:

- Weapon scheduling with very little time for engagement
- The combat system and its sensors to deal with debris fields generated by successful engagements of individual ASCMs within a multi-ASCM raid
- Rapid multi-salvo kill assessments for multiple targets
- Transitions between Evolved Seasparrow Missile (ESSM) guidance modes
- Conducting ballistic missile defense and area air-defense missions (i.e., integrated air and missile defense) while simultaneously conducting ship self-defense
- Contending with stream raids of multiple ASCMs attacking along the same bearing, in which directors illuminate multiple targets (especially true for maneuvering threats)
- Designating targets for destruction by the Close-In Weapons System (CIWS)

Multiple hard-kill weapon systems operate close-in, including the Standard Missile 2, the ESSM, and the CIWS. Soft-kill systems such as the Nulka MK 53 decoy launching system also operate close-in. The short timelines required to conduct successful ship self-defense stress combat system logic, combat system element synchronization, combat system integration, and end-to-end performance.

Navy range safety restrictions prohibit close-in testing on a manned ship because targets and debris from successful intercepts will pose an unacceptable risk to the ship and personnel at the ranges where these self-defense engagements take place. The Navy has invested in a seagoing, unmanned, remotely controlled self-defense test ship (SDTS) and is using it to overcome these safety restrictions. The Navy plans to validate and accredit a high-fidelity M&S capability – utilizing data from the SDTS as well as data from manned ship testing – so that a full assessment of the self-defense capabilities of ships can be completely and affordably conducted.

The SDTS is integral to the test programs for certain weapons systems (the Ship Self-Defense System, Rolling Airframe Missile Block 2, and ESSM Block 1) and ship classes (LPD 17, LHA 6, Littoral Combat Ship, LSD 41/49, DDG 1000, and CVN 78). DOT&E continues to recommend equipping SDTS with capabilities to support testing of ship self-defense systems' performance in the final seconds of the close-in battle and to acquire sufficient data to validate ship self-defense performance M&S.

Multi-Stage Supersonic Targets

The Navy initiated a $297 Million program in 2009 to develop and produce an adequate multi-stage supersonic target (MSST)

required for adequate operational testing of Navy surface ship air-defense systems. The MSST is critical to the DDG 1000, CVN 78, DDG 51 Flight III destroyer, LHA(R), Air and Missile Defense Radar (AMDR), Ship Self-Defense System, Rolling Airframe Missile Block 2, and ESSM Block 2 operational test programs. The MSST underwent restructuring and rebaselining from 2013 – 2015 to address technical deficiencies and cost and schedule breaches, which would have postponed its IOC to 2020 and increased the total program cost to $962 Million. Based on the restructured/rebaselined MSST program's high cost and schedule delays, as well as new intelligence reports, the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN(RDA)) in 2014 directed that alternatives be examined to test against these ASCM threats and subsequently terminated the MSST program. While the details of the final Navy alternative are classified, DOT&E determined that it would be costly (the Navy estimates $739 Million), difficult to implement, dependent on the results of highly segmented tests, and would suffer from artificialities that would confound interpretation of test results. DOT&E informed the Navy that the proposed alternative was not adequate for operational testing and recommended that the Navy not pursue it. MSST aerial target capabilities are still required to complete end-to-end operational testing of Navy surface ship air defense systems and to validate M&S capabilities for assessing the probability of raid annihilation for Navy ships.

Torpedo Surrogates for Operational Testing of Anti-Submarine Warfare Platforms and Systems

Operational testing of anti-submarine warfare (ASW) platforms and torpedo defense-related systems includes the ability to detect, evade, counter, and/or destroy an incoming threat torpedo. The determination of system or platform performance is dependent on a combination of the characteristics of the incoming torpedo (e.g., dynamics, noise, sensors, logic, etc.). Due to differences in technological approach and development, U.S. torpedoes are not representative of many highly proliferated torpedoes. The need for threat-representative torpedo surrogates to support operational testing is detailed in DOT&E memoranda to the ASN(RDA) dated January 9, 2013, and June 18, 2015. Acquisition programs that require threat torpedo surrogates for future operational testing include: *Virginia* and *Columbia* class submarines, *Zumwalt* class destroyer, *Freedom* and *Independence* variants of the Littoral Combat Ship (ASW mission package installed), AN/SQQ-89 surface ship undersea warfare combat system, and Acoustic Rapid Commercial Off-the-Shelf Insertion (A-RCI) submarine sonar system. Based on the 2014 Naval Undersea Warfare Center (NUWC) Division study, the Navy has taken the following actions to address the gaps in threat representation of torpedo surrogates:

- NUWC Division Keyport commenced a prototype technology development project that is expected to deliver a threat representative, high-speed, quiet propulsion system. This effort was initially funded as an FY16 Resource Enhancement Program (REP) project at approximately $1 Million. This project experienced cost and schedule overruns and transferred to the follow-on General Threat Torpedo (GTT) REP project.
- NUWC Division Keyport commenced development of a GTT that will complete development of the high-speed, quiet propulsion system prototype and provide threat-representative tactics and countermeasure logic. The GTT project is funded as a FY17 REP project at approximately $6.2 Million. DOT&E expects the GTT to fill in many of the gaps in threat representation of torpedo surrogates; however, the ability of a successfully developed GTT to adequately support operational testing futher depends on future Navy decisions to procure a sufficient quantity of GTT units.

Submarine Surrogates for Operational Testing of Lightweight and Heavyweight Torpedoes

The Navy routinely conducts in-water operational testing of lightweight and heavyweight ASW torpedoes against manned U.S. Navy submarines. Although these exercise torpedoes do not contain explosive warheads, peacetime safety rules require that the weapons run above or below the target submarine with a significant depth offset to avoid collision. While this procedure allows the torpedo to detect, verify, and initiate homing on the target, it does not support assessment of the complete homing and intercept sequence. One additional limitation is that U.S. nuclear attack submarines may not appropriately emulate the active target strength (sonar cross-section) of smaller threats of interest, such as diesel-electric submarines.

Since early 2013, DOT&E has participated in a Navy working group attempting to define the requirements for a mobile set-to-hit torpedo target. The group has identified a spectrum of options and capabilities, ranging from a torpedo-sized vehicle towing a long acoustic array to a full-sized submarine surrogate. At the very least, the target is expected to be capable of depth changes, high speeds, autonomous operations, and certified for representative lightweight torpedo set-to-hit scenarios. More advanced goals might include realistic active and passive sonar signatures to support ASW search, and reactive capability to present a more realistically evasive target.

Army Support of OT&E

In FY18, the Army initiated modernization and acquisition reforms through the establishment of eight Cross Functional Teams (CFTs) and the activation of the Army Futures Command (AFC). A primary goal of the AFC and the CFTs is to support the rapid acquisition and fielding of new warfighting capabilities to counter advancements made by near-peer adversaries. The CFTs are aligned with the Army's six modernization priorities: Long Range Precision Fires, Next Generation Combat Vehicles, Future Vertical Lift, Army Network, Air and Missile Defense Capabilities, and Soldier Lethality.

The warfighting systems developed under the six modernization priorities will be some of the more software-dependent, interconnected, and complex systems the Army has ever acquired. To ensure the Army is fielding combat credible weapon systems, it must demonstrate effectiveness and

suitability under the operationally representative conditions found in full-spectrum warfare. The Army Test and Evaluation Command (ATEC) will perform a critical role in supporting the Army's modernization efforts. The rapid development and acquisition of advanced warfighting capabilities will require a T&E workforce that is prepared and resourced to support shorter timelines. Substantial growth in the areas of autonomy, electronic warfare, cybersecurity, navigation warfare, and big data analysis continue to put increased demands on the Army T&E enterprise. The Army must contend with competition from industry as it struggles to recruit, retain, and grow an analytically and technically competent T&E workforce.

Beginning with the FY14 Annual Report, DOT&E expressed concern with the continued budget and staffing reductions at ATEC and the office of the Army Test and Evaluation Executive. When adjusted for inflation, there has been a 13 percent reduction in funding for Operational Test Command (OTC) and an 18 percent reduction in funding for the Army Evaluation Center from FY14 through FY18. DOT&E is concerned that these budget and staffing levels will not be sufficient to support the Army's aggressive modernization goals. DOT&E will continue to monitor the Army T&E workforce regarding its capability and capacity to support the evaluations of Army acquisition programs.

Electronic Warfare for Land Combat

Over the past 17 years of counterinsurgency warfare, the Army's EW capabilities have atrophied while its vulnerabilities have grown due to the expanded dependency on terrestrial and satellite RF-based networks and GPS. Recently, the Army began to rebuild its EW capabilities and strengthen its cyber defense through the development of new EW capabilities, the addition of EW and cyber threats during combat training center rotations, and by incorporating Cyber and ElectroMagnetic Activity (CEMA) sections into the staff elements of brigades, divisions, corps, and combatant commands. These efforts underscore that EW and cyber threats should be considered part of the operational environment.

During operational testing, threat EW capabilities are part of a broader combat force that is available to the opposing force (OPFOR) commander. Whenever possible, the threat systems and the TTP employed by the OPFOR during test should represent those of adversaries. Providing this realistic threat EW environment is complex and challenging due to the technical, safety, and regulatory conditions that must be met for each test. Satisfying these conditions often places severe limitations on the duration and emitted power of open-air EA, which will affect testing of the Army EA systems currently in development. To overcome these challenges the Army must continue to enhance EW test equipment and work to develop new practices and procedures. It must continue to support a technically competent and experienced workforce with appropriate training and resources.

A commitment to creating threat-representative EW environments during operational testing is necessary to ensuring that systems are survivable and will support units operating in contested electromagnetic environments. Threat EW environments should be considered for all operational testing, but are critical to the operational testing of future Army network initiatives, Nett Warrior/Leader Radio, Manpack Radio, Joint Battle Command – Platform, and Assured Positioning, Navigation, and Timing.

Tactical Engagement Simulation with Real Time Casualty Assessment

Realistic operational environments and a well-equipped OPFOR intent on winning are fundamental to the adequate operational test of land and expeditionary warfare combat systems. Force-on-force battles between tactical units represent the best method of creating a complex and evolving battlefield environment for testing and training. Tactical Engagement Simulation with Real Time Casualty Assessment (TES/RTCA) systems integrate live, virtual, and constructive components to enable these simulated force-on-force battles and provide a means for simulated engagements to have realistic outcomes. TES/RTCA systems should replicate the critical attributes of real-world combat environments, such as direct and indirect fires, IEDs and mines, and simulated battle damage and casualties. TES/RTCA systems must record the time-space position information and firing, damage, and casualty data for all players and vehicles in the test event as an integrated part of the test control and data collection architecture. Post-test playback of these data provide a critical evaluation tool to determine the combat system's capability to support soldiers and marines as they conduct combat missions.

All current TES/RTCA systems utilize the Instrumentable – Multiple Integrated Laser Engagement System (I-MILES) to ensure simulated engagements have realistic outcomes. Because these outcomes are based on the survivability and lethality characteristics of the systems they represent, I-MILES must be updated prior to IOT&E for every new or upgraded vehicle or weapon system. Timely updates to I-MILES are critical to enabling force-on-force training and ensuring that new and upgrated vehicles are prepared to be integrated into the Army Combat Training Centers (CTCs). The TES/RTCA systems used during operational test in FY18 were all training systems that were updated or modified to support operational testing and highlight the synergy that exists between the operational test and training communities.

Beginning in FY20, the Army cut funding that was programed for the Integrated Live, Virtual, Constructive, Test and Training Environment (ILTE) program. The ILTE program was established to acquire the TES/RTCA upgrades needed to support Army combat vehicle operational testing and is the only funding line dedicated to supporting major operational test instrumentation requirements in the Army. DOT&E believes that cutting funding to ILTE is counter to the lethality goals set by the National Defense Strategy, and the Army modernization and readiness priorities. Sustained investment and regular upgrades in TES/RTCA capabilities are necessary for testing systems such as Soldier Lethality efforts, Amphibious Combat Vehicle, Bradley

and Abrams Upgrades, Armored Multi-Purpose Vehicle, AH-64E Block III, Mobile Protected Firepower, Joint Light Tactical Vehicle, Stryker Upgrades, and Next Generation Combat Vehicle.

Test and Evaluation of Army Software-Defined Tactical Radios

Software-Defined Radios have become a cornerstone technology of the Army tactical radio communication systems. They provide the Army with improved capabilities such as simultaneous voice, data, and video communications; voice and data retransmission; increased throughput; multi-channel operations; and interoperability with fielded radios. Because of the complexity of these tactical radio networks and the added capabilities they provide, improved test instrumentation and data collection methods are needed to support the evaluations. The Army will need to develop instrumentation to support operational testing of radios with advanced networking waveforms. These improvements to instrumentation and data collection methods are necessary to support the T&E of the Leader Radio and Manpack Radio and experimentation of the Integrated Tactical Network.

Warrior Injury Assessment Manikin

Hybrid III is an anthropomorphic test device (ATD) currently used for LFT&E, but it lacks biofidelity in an underbody blast (UBB) test environment. It does not exhibit a human-like response when exposed to UBB loading conditions and can not fully assess operator survivability to vehicle shock, blast, and fragment damage. The Warrior Injury Assessment Manikin (WIAMan) Engineering Office (WEO) is developing the WIAMan ATD to address this LFT&E capability shortfall. The LFT&E section describes the WIAMan project on page 227.

Foreign Materiel Acquisition Support for T&E

DOT&E is responsible for ensuring U.S. weapons systems are tested in realistic threat environments. Use of actual threat systems and foreign materiel to create realistic threat environments in testing helps to determine a system's operational effectiveness in a combat environment. To acquire test capabilities, DOT&E/TETRA develops an annual prioritized list of foreign materiel required for upcoming operational tests. These requirements are submitted to the Defense Intelligence Agency (DIA) Joint Foreign Materiel Program Office and are consolidated with Service requirements to drive Service and Intelligence Community collection opportunities. DOT&E coordinates with the Department of State to identify other opportunities to acquire foreign materiel for use in OT&E.

Foreign materiel requirements span all warfare areas, but DOT&E continues to place a priority on the acquisition of man-portable air defense systems (MANPADS) and anti-tank guided missiles (ATGMs). Foreign MANPADS are needed to address significant threat shortfalls that affect testing for IRCM programs like Common Infrared Countermeasures (CIRCM), Large Aircraft Infared Countermeasure (LAIRCM), and Department of the Navy (DON) LAIRCM. For some programs, a large quantity of MANPADS is required – for development of threat M&S, for use in hardware-in-the-loop laboratories, and for LFT&E – to present realistic threats to IRCM equipment. Using actual missiles and missile seekers aids evaluators in determining the effectiveness of IRCM equipment. Foreign ATGMs are required to support the testing of the Expedited Active Protection System.

Traditional sources have been fully consumed, and there is a critical need to identify and develop new sources and opportunities for acquiring foreign materiel. Foreign materiel acquisitions are usually lengthy and unpredictable, making it difficult to identify appropriate year funding. Programs have funded as much as $60 Million a year for acquisition opportunities that arise. DOT&E recommends a no-year or non-expiring funding line for foreign materiel acquisitions, funded at a level of $10 Million per year.

Range Sustainability

In previous reports, DOT&E highlighted the many challenges the Department faces in preventing various activities that may limit the ability of the Department to fully utilize the capabilities of its current test and evaluation infrastructure. At a time when the Department is attempting to define testing requirements for the leap-ahead technologies envisioned by the National Defense Strategy, it is imperative that the test capabilities it has today be preserved as a foundation for future testing needs. The following are the areas of particular concern.

Airspace. The newest generation of weapon systems are designed to create effects at longer distances, and new weapon systems under development will require extremely long distances for testing. Studies are in process to determine how best to accommodate these requirements. However, a number of external factors (to include urban development, incompatible infrastructure, electromagnetic interference, and the presence of endangered species) may act to limit the use of current, dedicated airspace.

Maritime Sustainability. The DOD requires extensive sea ranges for testing and training associated with naval warfare and for testing long-range weapons. However, potential for expanded oil, gas, and wind energy development may limit the use of these ranges through the introduction of fixed structures and increased surface vehicle traffic. The Department is especially concerned about increased development in the eastern Gulf of Mexico, where the current statutory moratorium on oil and gas development expires in 2022, and off the coast of California, which is being examined especially for wind development.

Frequency Spectrum. National spectrum policy supports turning over more spectrum resources to commercial users, at the same time telemetry data rates for weapon systems are increasing. The Department is conducting research and development to identify techniques and implement systems that more effectively utilize the currently available spectrum. However, it is imperative that future sales be carefully structured to ensure no additional loss of capabilities and that additional spectrum be identified to satisfy current and future DOD testing requirements.

Water Usage. An emerging issue in some of the western ranges is the availability of sufficient water to sustain range operations. Long-term drought conditions have strained available water resources, and these water resources must be shared amongst all local users. Extensive collaboration with state and local entities will be required to ensure short- and long-term water issues can be resolved.

Renewable Energy. Renewable energy infrastructure, particularly wind turbines and the electrical transmission lines, create particular issues for the DOD test infrastructure. To date, the Department has been effective in limiting the impact of renewable energy projects. However, as renewable energy technology advances, and new locations are proposed (including offshore), the Department will face a continuing challenge in limiting deliterious effects.

Privately Operated Drones. Inexpensive yet highly capable remotely operated air vehicles have the potential to jeopardize safe and secure conduct of test operations. Recent actions by the Federal Aviation Administration to establish a regulatory regime for unmanned aerial vehicles (UAVs) are useful in establishing controls, as is recent legislative action to extend the SECDEF authority to protect facilities included in the Major Range and Test Facility Base from intrusion by UAVs. As new legislation and regulations emerge, measures to protect test activities and land, air, and sea range integrity will continue to be incorporated into T&E strategic and event planning.

Cyber Intrusion of Range Instrumentation. Some of the current range instrumentation rely on obsolete technology, which makes it difficult to harden them to protect sensitive information. Adequate funding for range instrumentation modernization is required to ensure that all instrumentation can be upgraded or replaced to standards that incorporate cybersecurity as a key performance parameter.

Foreign Investment. Foreign intelligence services may be able to conduct surveillance of weapon systems under test or training by investing in U.S. entities. Intelligence may be gathered either by establishing a physical presence in the vicinity of test or training activities or by investing in technology firms in order to obtain access to data streams during testing. DOT&E currently reviews projects under review by the Committee on Foreign Investment in the United States (CFIUS), with the goal of identifying foreign investment proposals that pose a significant risk to test and training activities. The recently enacted Foreign Investment Risk Review Modernization Act of 2018 will, when fully implemented, expand the universe of transactions subject to review, thereby allowing greater scrutiny. Although it is anticipated that the number of cases to be reviewed will increase substantially, DOT&E will continue to subject transactions to review.

Joint Test and Evaluation

Joint Test and Evaluation

Joint Test and Evaluation (JT&E)

The primary objective of the Joint Test and Evaluation (JT&E) Program is to rapidly provide non-materiel solutions to operational deficiencies identified by the joint military community. The program achieves this objective by developing new tactics, techniques, and procedures (TTP) and rigorously measuring the extent to which their use improves operational outcomes. JT&E projects may develop products that have implications beyond TTP. Sponsoring organizations transition these products to the appropriate Service or Combatant Command (CCMD) and submit them as doctrine change requests. Products from JT&E projects have been incorporated into joint and multi-Service documents through the Joint Requirements Oversight Council process, Joint Staff doctrine updates, Service training centers, and coordination with the Air Land Sea Application Center. The JT&E Program also develops operational testing methods that have joint application. The program is complementary to, but not part of, the acquisition process.

The JT&E Program uses two test methods: the Joint Test and the Quick Reaction Test (QRT), which are both focused on the needs of operational forces. The Joint Test is, on average, a 2-year project preceded by a 6-month Joint Feasibility Study. A Joint Test involves an in-depth, methodical test and evaluation of issues and seeks to identify their solutions. DOT&E funds the sponsor-led test team, which provides the customer with periodic feedback and useable, interim test products. The JT&E Program charters two new Joint Tests annually. The JT&E Program managed eight Joint Tests in FY18. Projects annotated with an asterisk (*) were completed in FY18:

- Digitally Aided Close Air Support (DACAS)*
- Joint Counterair Integration (JCI)
- Joint Cyber Insider Threat (J-CIT)
- Joint Hypersonic Strike, Planning, Execution, Command and Control (J-HyperSPEC2)
- Joint Interoperability for Medical Transport Missions (JI-MTM)
- Joint Laser Systems Effectiveness (JLaSE)
- Joint Sense and Warn (J-SAW)
- Multi (enhanced) Domain Unified Situational Awareness (MeDUSA)

QRTs are intended to solve urgent issues in less than a year. The JT&E program managed 16 QRTs in FY18:

- Aviation Radio Frequency Survivability Validation (AVRFSV)*
- Critical Strategic Power Projection Infrastructure (CRSPPI)
- Intelligence Prioritization for Cyberspace Operations (IPCO)*
- Joint Accuracy of Nationally Derived Information (JANDI)
- Joint Ballistic Missile Defense (BMD) Overhead Persistent Infrared (OPIR) Operational Space Track (J-BOOST)*
- Joint Contaminated Human Remains (CHR) Recovery in a Chemical Environment (JCRCE)
- Joint Chemical Biological Radiological Nuclear (CBRN) Tactical Information Management (J-CTIM)
- Joint Enterprise Data Interoperability (JEDI)
- Joint Enhanced Emissions Control (EMCON) Procedures (JEEP)
- Joint Intelligence Production in a Cloud Environment (JIPCE)*
- Joint Intelligence, Surveillance, and Reconnaissance (ISR) to Tactical Data Link (TDL) Modernization (JITM)
- Joint Missile Seeker Defeat (JMSD)*
- Joint Optimization of Electromagnetic Spectrum (EMS) Superiority (JOES)
- Joint Procedures for Integrated Tactical Warning and Attack Assessment (ITWAA) of Hypersonic Glide Vehicles (HGV) (J-PITH)
- Joint Radio Frequency-Enabled Cyberspace Operations (JRF-ECO)
- Joint Sensor to Tactically Responsive Integrated Kinetic Effects (J-STRIKE)*

JOINT TESTS

DIGITALLY AIDED CLOSE AIR SUPPORT (DACAS) (CLOSED MAY 2018)

Sponsor/Start Date: Joint Staff J6/February 2016

Purpose: To develop, test, and evaluate standardized TTP in order for Joint Terminal Attack Controllers (JTAC), Joint Fires Observers, and Close Air Support (CAS) aircrew to realize the advantage of DACAS capabilities, including shared situational awareness, increased confidence prior to weapons release, and improved kill chain timeliness.

Products/Benefits:

- TTP that outline network management considerations and provide mission planning and execution procedures to ensure all users have standardized information to operate on the network and to deliver proper system configuration for first-try connectivity
- Decreased human input error through machine-to-machine data exchange leading to increased speed of CAS execution

- Enable JTAC and aircrew to access existing networks and exploit DACAS benefits
- Enhance operational effectiveness and increase confidence prior to weapons release by providing a common and accurate shared situational awareness

JOINT COUNTERAIR INTEGRATION (JCI)

Sponsor/Start Date: U.S. Indo-Pacific Command (USINDOPACOM)/February 2017

Purpose: To develop, test, and evaluate TTP to provide counterair shooters and command and control (C2) operators with the ability to integrate joint defensive counterair (DCA) resources in a contested, degraded, and operationally limited (CDO) environment to protect defended assets from expected threats. The JCI solution integrates joint DCA by pairing targets with the correct weapon system by focusing on sharing ID/Platform/Type in order to enhance joint DCA efficiency and lethality.

Products/Benefits:
- TTP that enables operators to integrate joint DCA forces in a CDO environment to improve tactical-level operations, enhance coordination between assets, and minimize exploitation of gaps in area coverage
- JCI consolidated procedures that support sharing of threat information across various land, sea, and air tactical-level platforms to optimize use of weapons and reduce possibility of fratricide
- Integration of Army, Air Force, Navy, and Marine Corps DCA assets to counter a peer threat in a CDO environment
- Validated findings that will lead to recommendations in standardizing C2 procedures and tactical message information

JOINT CYBER INSIDER THREAT (J-CIT)

Sponsor/Start Date: U.S. Army Research Laboratory/ August 2016

Purpose: To develop, test, and deliver the Cyber Insider Threat Detection and Reporting (CIDaR) TTP to enable detecting and reporting of cyber insider threats prior to having a negative impact on national security interests.

Products/Benefits:
- CIDaR TTP that includes planning and network management considerations for configuring and utilizing existing organizational organic hardware and software to monitor user activities by analyzing data and log files
- CIDaR TTP that provides procedures for Cybersecurity Service Provider operators to analyze and report insider threat events
- CIDaR TTP that supports regulatory guidance, strategies, and directives that mandate an insider threat program

JOINT HYPERSONIC STRIKE, PLANNING, EXECUTION, COMMAND AND CONTROL (J-HYPERSPEC2)

Sponsor/Start Date: U.S. Strategic Command (USSTRATCOM)/August 2018

Purpose: To develop, test, and evaluate C2 concept of operations (CONOPS) that enable warfighters to effectively plan and promptly employ hypersonic weapons to fully capitalize on this emerging capability.

Products/Benefits:
- CONOPS supporting planning and execution decisions for hypersonic weapons whether land, air, or sea launched; planning addresses command relationships, resource allocation, organization structure, authorities, and whether centralized or distributed; execution decisions address considerations for targeting to achieve strategic- and operational-level effects to include identifying risk
- Enables effective employment of hypersonic weapons to provide a highly responsive, long-range, non-nuclear strike option for distant, defended, and/or time-critical threats when forces are denied access, not available, or not preferred

JOINT INTEROPERABILITY FOR MEDICAL TRANSPORT MISSIONS (JI-MTM)

Sponsor/Start Date: DOD Chief Information Officer/ August 2017

Purpose: To develop, test, and evaluate standardized TTP to access and utilize existing patient information from various health information systems across the DOD during the patient movement coordination and validation process.

Products/Benefits:
- Faster access to required information resulting in quicker validation of patient movement requests and movement to the appropriate care level
- Richer picture of patient history for better informed medical decisions
- Improved capability to plan and deliver appropriate transport and onboard medical staff in order to provide the best en route care for patients
- Reduced workload and potential for errors during manual information reentry into the patient movement planning system

JOINT LASER SYSTEMS EFFECTIVENESS (JLASE)

Sponsor/Start Date: Naval Surface Warfare Center, Dahlgren Division/April 2017

Purpose: To develop and test procedures that integrate emerging high energy laser (HEL) weapon systems with weaponeering and

collateral damage estimation (CDE) methodology within the Joint Targeting Cycle.

Products/Benefits:
- Joint Targeting Cycle procedures for Laser Weaponeering and CDE
- Integration of HEL systems into the Joint Targeting Cycle focusing on capabilities analysis, weaponeering, and damage estimation
- Development of HEL weapon Joint Munitions Effectiveness Manual (JMEM) data for use by weaponeers with joint targeting systems as part of the JMEM Weaponeering System
- Increased confidence of warfare commanders in the ability of laser weapons to provide scalable lethality ranging from degrading sensors to catastrophic destruction
- Recommendations to assist the Services in HEL system development and acquisition as well as with integrating HEL into the operational environment
- TTP for the integration of HEL weapon systems into joint and Service operations in order to engage enemy targets according to the commander's intent

JOINT SENSE AND WARN (J-SAW)

Sponsor/Start Date: U.S. Air Forces in Europe (USAFE) – Air Forces Africa (AFAFRICA) and USINDOPACOM/August 2018

Purpose: To test and evaluate a concept of employment (CONEMP) and TTP to integrate a portable surveillance system into existing U.S. and coalition integrated air defense system architecture for use in air warning and defense engagement command and control.

Products/Benefits:
- CONEMP and TTP that provide CCMDs with specific technical and operational processes and procedures to integrate tracks into a Theater Air Defense System, manage track identification and evaluation, and provide the ability to warn U.S. defended assets for passive and active defense response
- Improved air defense systems that enable earlier sensing and warning to U.S. and allied defensive capabilities for threat response and consequence mitigation
- Integration of passive sensors against air threats that enable defense of the homeland from attack and defend allies from aggression
- Validated findings that will lead to recommendations to improve selected elements of doctrine, organization, training, materiel, leadership and education, personnel, and facilities

MULTI (ENHANCED) DOMAIN UNIFIED SITUATIONAL AWARENESS (MEDUSA)

Sponsor/Start Date: USINDOPACOM and U.S. Northern Command (USNORTHCOM)/February 2018

Purpose: To test and evaluate non-materiel solutions supporting the development of standardized displayable common operational picture (COP) information layers within the unclassified domain, the transfer of the layers via a cross domain solution to the classified domain, and the utilization of products from the SIPRNET COP.

Products/Benefits:
- Validated technical processes and procedures for generating standardized unclassified domain products and displaying them on a SIPRNET COP in order to enhance commanders' situational awareness and understanding within their areas of responsibility
- Senior Leader Guide with best practices and lessons learned for gaining situational awareness utilizing unclassified COP information on a consolidated SIPRNET COP
- Decreased resource requirement and human input error through machine-to-machine data exchange leading to better synchronization or de-confliction of information
- Increased situational awareness and understanding through the use of an enhanced comprehensive view of data on a single COP

QUICK REACTION TESTS

AVIATION RADIO FREQUENCY SURVIVABILITY VALIDATION (AVRFSV)
(CLOSED APRIL 2018)

Sponsor/Start Date: U.S. Army Aviation Center of Excellence/ October 2016

Purpose: To increase rotary-wing asset survivability effectiveness against the most widely proliferated radio frequency (RF) threats through the employment of a combination of aircraft survivability equipment, countermeasures, and maneuvers.

Products/Benefits:
- TTP for rotary-wing aircraft to maintain freedom of maneuver against and defeat RF threats
- Validated helicopter RF counter procedure for use in Army Techniques Procedure Manual 3-04.2
- Collected high fidelity data to be utilized in modeling and simulation to support future TTP development
- Utilization of test results to drive Aircraft Survivability Equipment recommendations to shape future DOD requirements

CRITICAL STRATEGIC POWER PROJECTION INFRASTRUCTURE (CRSPPI)

Sponsor/Start Date: North American Aerospace Defense Command (NORAD)-USNORTHCOM/June 2017

Purpose: To develop Interagency Infrastructure Assessment (IIA) TTP to enable the assessment of selected critical interagency infrastructures. Sponsor lacks specific agreements, procedures, and access to conduct assessments in areas that the DOD does not own or control. A lack of information and assessment of certain critical infrastructures, facilities, and transportation nodes significantly degrades the sponsor's ability to prepare for and rapidly respond to high consequence, multi-domain threats to U.S. critical strategic infrastructures.

Products/Benefits:
- IIA TTP, with an accompanying implementation plan, to prescribe all aspects of manning, agreements, funding support, and coordination to initiate an IIA program of record
- TTP providing users with the necessary tools to assess force flow vulnerabilities within a contested environment due to state or non-state actors
- Reports stemming from use of TTP will be stored on a digital database used by U.S. Transportation Command, the Department of Transportation, the Transportation Security Administration, and other government agencies allowing access to all reports in a timely manner

INTELLIGENCE PRIORITIZATION FOR CYBERSPACE OPERATIONS (IPCO)
(CLOSED AUGUST 2018)

Sponsor/Start Date: U.S. Special Operations Command (USSOCOM)/February 2017

Purpose: To develop and assess TTP for integration of cyber intelligence planning into mission execution. Joint Task Forces lack early allocation of intelligence resources to enable cyberspace operations. Significant lead time is needed for proper cyberspace operations planning.

Products/Benefits:
- Transitioned a smart book to USSOCOM and USINDOPACOM; contains TTP steps that provide a deliberate method to increase understanding of cyberspace information requirements for input into an intelligence estimate and coordination with planning elements
- These TTP improve the timing and production of required basic level intelligence preparation of the operational environment products used by the joint force and facilitates the integration of cyberspace operations into the planning and execution of joint operations

JOINT ACCURACY OF NATIONALLY DERIVED INFORMATION (JANDI)

Sponsor/Start Date: USINDOPACOM/October 2017

Purpose: To determine the root causes of errors; refine and validate TTP to mitigate positional errors when publishing nationally derived information generated onto the tactical datalinks; and determine the source of positional errors.

Products/Benefits: TTP required to update the Operational Tasking Data Link documents for USINDOPACOM, Pacific Air Forces, and Pacific Fleet based on project test results.

JOINT BALLISTIC MISSILE DEFENSE (BMD) OVERHEAD PERSISTENT INFRARED (OPIR) OPERATIONAL SPACE TRACK (J-BOOST)
(CLOSED MARCH 2018)

Sponsor/Start Date: USAFE-AFAFRICA/October 2016

Purpose: To develop TTP to optimize existing space-based technology for active and passive defense. The goal is to better use current and near-term BMD capabilities resulting in earlier missile threat situational awareness, precision cueing, engagement opportunities, and improved architecture resilience.

Products/Benefits:
- TTP that document configuration of communications networks to allow select C2 nodes, Aegis BMD, and Aegis Ashore systems to receive, interpret, and use Enterprise Sensors Processing Node tracks in testing, training, exercises, and operations
- Earlier and more refined development of defensive response options
- Increased warfighter confidence in the ability to use space-based data in support of the BMD mission set

JOINT CONTAMINATED HUMAN REMAINS (CHR) RECOVERY IN A CHEMICAL ENVIRONMENT (JCRCE)

Sponsor/Start Date: U.S. Army Quartermaster School/ June 2017

Purpose: To identify gaps in current TTP and provide TTP improvement recommendations for the safe recovery of chemically contaminated human remains. To validate procedure effectiveness and safety for mitigating hazards, preserving forensic evidence, and accomplishing preliminary decedent identification tasks.

Products/Benefits:
- Joint TTP for safe recovery of chemically contaminated human remains
- Evaluations on the utility and suitability of new human remains pouch capabilities

JOINT CHEMICAL BIOLOGICAL RADIOLOGICAL NUCLEAR (CBRN) TACTICAL INFORMATION MANAGEMENT (J-CTIM)

Sponsor/Start Date: USINDOPACOM/June 2018

Purpose: To identify gaps in current CBRN early warning and reporting processes and develop improved TTP for timely and effective protective posture decision support to friendly forces that enables continuity of operations under situations involving CBRN threats.

Products/Benefits: TTP will allow the joint community to conduct early detection of CBRN agents within the tactical environment and provide warfighters across all branches with the ability to quickly react to a CBRN attack in order to reduce the effects of such attacks.

JOINT ENTERPRISE DATA INTEROPERABILITY (JEDI)

Sponsor/Start Date: Department of the Army G-4/March 2018

Purpose: To develop a validated CONOPS to implement logistics data exchange standards among partners required for the Joint Logistics Enterprise to support Globally Integrated Operations as identified in the Chairman, Joint Chiefs of Staff Joint Concept for Logistics, and the Capstone Concept for Joint Operations: Joint Force 2020.

Products/Benefits: TTP will allow for logistical interoperability with allied partners from the United Kingdom, and the TTP will provide a greater level of sustainment to forces embedded within the ranks of a U.S. division.

JOINT ENHANCED EMISSIONS CONTROL (EMCON) PROCEDURES (JEEP)

Sponsor/Start Date: Naval Information Warfighting Development Center/June 2018

Purpose: To develop TTP to mitigate friendly systems vulnerabilities through determining which friendly emitters are detectable by adversary signals intelligence capabilities. Also, the project will measure the parameters critical for assessing U.S. systems as surrogates for adversary systems to inform TTP development.

Products/Benefits: TTP document with a matrix for tactical-level guidance.

JOINT INTELLIGENCE PRODUCTION IN A CLOUD ENVIRONMENT (JIPCE) (CLOSED JANUARY 2018)

Sponsor/Start Date: Air Combat Command/October 2016

Purpose: To develop TTP to utilize Intelligence Community Information Technology Enterprise (IC ITE)-enabled tools and tradecraft to supplement Joint Intelligence Preparation of the Environment (JIPOE) processes.

Products/Benefits: TTP and quick reference guides that enable Joint Intelligence Operations Center intelligence analysts to optimize IC ITE cloud-based intelligence information and tools, particularly BRIMSTONE and its follow-on, in support of JIPOE Step Four, Determine Adversary Course of Action.

JOINT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR) TO TACTICAL DATA LINK (TDL) MODERNIZATION (JITM)

Sponsor/Start Date: Air Combat Command A2/October 2017

Purpose: To develop a procedure for the integration of national ISR data into Link 16 architecture and to update Military Standard (MIL-STD) 6016.

Products/Benefits: TTP to employ updated MIL-STD 6016 for the communication of information directly from national ISR participants to TDL users; TTP improves the timeliness, accuracy, and completeness of national intelligence threat information being disseminated to tactical and operational warfighters.

JOINT MISSILE SEEKER DEFEAT (JMSD)
(CLOSED NOVEMBER 2017)

Sponsor/Start Date: USINDOPACOM/June 2016

Purpose: To develop and assess a missile seeker defeat CONEMP and associated TTP.

Products/Benefits: Specific TTP to enable fighter aircraft weapon systems to employ missile seeker defeat concepts against an existing adversary threat.

JOINT OPTIMIZATION OF ELECTROMAGNETIC SPECTRUM (EMS) SUPERIORITY (JOES)

Sponsor/Start Date: USINDOPACOM/June 2018

Purpose: To develop TTP for the integration of joint electromagnetic spectrum operations (JEMSO) functions into a standing JEMSO Cell for CCMD's effective use of the EMS for assured friendly C2 and to degrade adversary capabilities.

Products/Benefits: TTP to support JEMSO Cell functions to develop an EMS superiority strategy, mitigate adversary's abilities to contest friendly operations, coordinate authorizations for friendly forces, and tailor EMS signatures to limit friendly vulnerabilities.

JOINT PROCEDURES FOR INTEGRATED TACTICAL WARNING AND ATTACK ASSESSMENT (ITWAA) OF HYPERSONIC GLIDE VEHICLES (HGV) (J-PITH)

Sponsor/Start Date: Commander, NORAD-USNORTHCOM/ March 2018

Purpose: To develop and validate TTP to optimize the ITWAA C2 process to detect, identify, and characterize the hypersonic glide vehicle threat via the current space-based and terrestrial architecture.

Products/Benefits: TTP to optimize the ITWAA C2 processes; provide a means to identify and characterize HGVs employed by intercontinental ballistic missiles, intermediate-range ballistic missiles, and medium-range ballistic missiles; and define the roles and responsibilities among all stakeholders involved in the warning and assessment process.

JOINT RADIO FREQUENCY-ENABLED CYBERSPACE OPERATIONS (JRF-ECO)

Sponsor/Start Date: USSTRATCOM and USINDOPACOM/ June 2017

Purpose: To develop necessary processes for the C2 of RF-enabled cyberspace operations (RECO) by theater supporting Combat Mission Teams (CMT); these processes will serve as a baseline CONOPS.

Products/Benefits: Validated joint baseline CONOPS and TTP that will enable CMTs to remotely manage air-delivered, bi-directional RECO in order to degrade and disrupt an adversary's use of their cyberspace capabilities.

JOINT SENSOR TO TACTICALLY RESPONSIVE INTEGRATED KINETIC EFFECTS (J-STRIKE)
(CLOSED JULY 2018)

Sponsor/Start Date: U.S. Army Pacific/February 2017

Purpose: To provide more timely and effective access for theater assets to sense and destroy high value enemy targets through the seamless integration of ISR and targeting information between all domains and Services.

Products/Benefits: TTP that allows USINDOPACOM to fully exploit cross-domain fires capabilities with currently available systems to use U.S. Air Force, U.S. Navy, and national technical means sensors to engage sea-based targets with land-based batteries.

Center for
Countermeasures

Center for
Countermeasures

The Center for Countermeasures (CCM)

The Center for Countermeasures (the Center) is a joint activity that directs, coordinates, supports, and conducts independent countermeasure/counter-countermeasure (CM/CCM) T&E activities of U.S. and foreign weapons systems, subsystems, sensors, and related components. The Center accomplishes this work in support of DOT&E, the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E)), weapon systems developers, and the Services. The Center's testing and analyses directly support evaluations of the operational effectiveness and suitability of CM/CCM systems.

Specifically, the Center:

- Determines performance and limitations of missile warning and aircraft survivability equipment (ASE) used on rotary- and fixed-wing aircraft
- Determines performance of precision-guided weapon systems and subsystems when operating in an environment degraded by CMs
- Develops and evaluates CM/CCM techniques and devices
- Operates unique test equipment that supports testing across the DOD
- Provides analyses and recommendations on CM/CCM performance to Service Program Offices, DOT&E, DASD(DT&E), and the Services
- Supports Service member exercises, training, and pre-deployment activities

The Center conducts these activities — from testing and analysis of CM/CCM systems, to support training and pre-deployment activities, and development of CM/CCM tools and techniques — to help enhance the survivability of equipment, aircraft and personnel. The Center's core mission to support T&E of ASE directly leads to a "more lethal force" by enabling increased survivability of aircraft in a threat environment. Survivability enables mission success.

In FY18, the Center completed 43 T&E activities. The majority of these T&E activities focused on meeting Joint Urgent Operational Needs Statements (JUONS) and Urgent Universal Needs Statements (UUNS) for ASE. The Center's predominant involvement in JUONS and UUNS testing helped fill immediate mission needs and resulted in the successful deployment of critical ASE equipment to combat theaters, contributing to a "more lethal force."

The Center supported the field testing of other programs by providing realistic Man-Portable Air Defense System (MANPADS) threat environments for Service member aircrew pre-deployment training. In the course of these activities, the Center conducted the test support, analysis, and reporting of more than 30 DOD systems or subsystems — with special emphasis on rotary-wing survivability. The Center also provided subject matter expert (SME) support to numerous working groups, task forces, and Program Offices. While conducting test activities, the Center continues to improve its T&E capabilities and test methods.

JUONS

Advanced Threat Warner (ATW) Tests

Army: CH-47F Formal Software Release 2.6 Test

- **Sponsor:** Project Management Office Aircraft Survivability Equipment (PMO ASE)
- **Activity/Benefit:** The Center provided one Multi-Spectral Sea and Land Target Simulator (MSALTS) for single threat engagements against the integrated ATW/Common Missile Warning System (CMWS) and Guardian Laser Turret Assembly (GLTA) as installed on the CH-47F. The MSALTS provided simultaneous ultraviolet (UV) and infrared (IR) missile plume simulations; the UV simulations were used to evaluate the CMWS, the IR simulations to evaluate the ATW, and the jam beam radiometers to evaluate the GLTA. Center participation in this test was in direct support of ongoing PMO ASE ATW JUONS efforts. The Center collected data during this test that allowed PMO ASE to assess the ATW system's declaration and threat angle-of-arrival performance. These data also allowed PMO ASE to determine whether ATW Formal Engineering Software Release 2.6 correctly updated prior software releases and whether this software release was ready for fielding to aircraft platforms in theater. The PMO ASE conducted the test from May 7 – 18, 2018, at Decatur, Alabama.

Army: Formal Software Release 3.1 Tests

- **Sponsors:** U.S. Army Technology Applications Program Office (TAPO), the 160th Special Operations Aviation Regiment (SOAR) Systems Integration and Maintenance Office (SIMO), and PMO ASE

- **Tests:**
  - MH-60M Test (October 16 – 20, 2017), Decatur, Alabama
  - UH-60L Integration Test (November 15 – 17, 2017), Redstone Arsenal, Alabama
  - UH-60M Test (January 19 – 25, 2018), Redstone Arsenal, Alabama
  - UH-60M Test (January 29 – 31, 2018), Courtland, Alabama
  - UH-60M Test (February 5 – 9, 2018), Decatur, Alabama
  - CH-47F Spacer Investigation Test (March 19 – April 4, 2018), Redstone Arsenal, Alabama
- **Activity/Benefit:** The Center provided one MSALTS for single threat engagements against the integrated ATW/CMWS and GLTA as installed on the CH-47F, UH-60L, and UH-60M, and the ATW as installed on the MH-60M. The MSALTS provided simultaneous UV and two-color IR missile plume simulations; the UV simulations were used to evaluate the CMWS, the IR simulations to evaluate the ATW, and the jam beam radiometers to evaluate the Directed Infrared Countermeasure (DIRCM) systems. Center participation in these tests was in direct support of ongoing PMO ASE and TAPO ATW JUONS efforts. The Center collected data during these tests that helped PMO ASE and TAPO determine whether ATW Formal Engineering Software Release 3.1 correctly updated prior software releases and whether this software release was ready for fielding to aircraft platforms in theater. PMO ASE also used these data to evaluate new spacers installed on the CH-47F's forward and aft sensors and to assess the performance of the integrated CMWS/ATW and GLTA on the UH-60L. The Center also provided the sponsors a preliminary assessment of the ATW system as installed on each platform.

Air Force: AC-130W JUONS and Combat Mission Need Statement (CMNS) Large Aircraft IR Countermeasures (LAIRCM) Flight Test

- **Sponsor:** U.S. Department of the Air Force, Air Force Special Operations Command (AFSOC)
- **Activity/Benefit:** The Center provided one stationary and one moving MSALTS for single and dual threat engagements against the AC-130W. AFSOC used data from the MSALTS two-color IR missile plume simulations to evaluate the LAIRCM ATW and data from the MSALTS jam beam radiometers to evaluate the DIRCM. Center participation in this test was in direct support of ongoing AFSOC JUONS and CMNS efforts. The Center collected data during the test that helped AFSOC determine whether the ATW as installed on the AC-130W was ready for fielding in theater. AFSOC conducted the test on March 26 – 27, 2018, at Eglin AFB, Florida.

Air Force: CV-22 JUONS LAIRCM Flight Test

- **Sponsor:** U.S. Department of the Air Force, AFSOC
- **Activity/Benefit:** The Center provided two stationary MSALTS missile plume simulators for two-color IR missile plume simulations and jam beam data collection, and threat-representative lasers. The Center collected data from the MSALTS simulations and the laser threat illuminations to assist the AFSOC in its assessment of the LAIRCM ATW as installed on the CV-22. Center participation in this test was in direct support of AFSOC ATW JUONS efforts. AFSOC conducted the test on January 15 – 16, 2018, at Hurlburt Field, Florida.

Distributed Aperture Infrared Countermeasure (DAIRCM) Tests

Navy: Various DAIRCM Tests

- **Sponsor:** Program Executive Officer, Tactical Aircraft Programs (PMA-272) on behalf of the Detachment 1 (Det 1), 413th Flight Test Squadron (FLTS), TAPO, and SOAR SIMO
- **Tests:**
  - Contractor Flight Test (April 16 – 27, 2018), Redstone Arsenal, Alabama
  - MH-6 Risk Reduction Test (May 22 – 24, 2018), Redstone Arsenal, Alabama
  - HH-60G IT-1 Test (June 11 – 29, 2018; July 9 – 20, 2018), Redstone Arsenal, Alabama
  - MH-60 IT-1 Test (June 11 – 29, 2018), Redstone Arsenal, Alabama
  - MH-60 IT-1 Test (July 10 – 13, 2018), Houston, Texas
  - DAIRCM Free Flight Missile Test 1 (September 10 – 28, 2018), Dugway Proving Ground, Utah
- **Activity/Benefit:** The Center provided one Joint Mobile Infrared Countermeasure Test System (JMITS) (with four MANPAD threat seekers) and one MSALTS missile plume simulator for two-color IR missile plume simulations and jam beam data collection. During the free flight missile test, the Center provided the Joint Standard Instrumentation Suite (JSIS) to collect signature data during the missile firings. The Center collected data from the simulators to help PMA-272 assess the performance of the DAIRCM missile warning system (MWS) installed on the MH-6 and HH-60G helicopters in benign and low-clutter environments; the MH-6 was also tested in medium- and high-clutter environments. PMA-272 conducted the contractor flight test for a preliminary assessment of the DAIRCM software and hardware; adjustments to hardware and/or software were made after testing. PMA-272 conducted the risk reduction test to determine if adjustments made to software and hardware were successful and to set the baseline software for formal DAIRCM testing. Center participation in these tests was in direct support of ongoing PMA-272 JUONS efforts. The Center collected data and performed a preliminary assessment that was central in helping DAIRCM developers and stakeholders assess the DAIRCM's missile warning and CM capabilities.

Infrared Countermeasure (IRCM) Expendable Tests

Army: Seeker Bowl XIII IRCM Test

- **Sponsor:** Armament Research, Development and Engineering Center (ARDEC), Pyrotechnics Division, Countermeasure Flare Branch and Program Management Close Combat Systems (PM CCS)
- **Activity/Benefit:** The Center provided SME support during the IRCM effectiveness test for the CH-47F Infrared Suppression System (IRSS), C-12R Transport, Enhanced Medium Altitude Reconnaissance and Surveillance System (MARSS), Enhanced MARSS – Geographical Intelligence, and UH-60M Upturned Exhaust System aircraft. The Center also assisted with the operation of IR seekers in the Missile and Space Intelligence Center (MSIC) seeker test van. These tests evaluated the fielded flare IRCM sequences and variations of the sequence with timing and/or pattern adjustments. The Center provided near real-time data reduction and analysis of flare sequences as well as on-site recommendations on flare sequence timing and/or pattern adjustments. As a result, the ARDEC was able to determine the most effective IRCM flare solution for each platform during the course of the test and prepare its post-test briefing for its higher headquarters, PM CCS, PMO ASE, and each platform's Program Office. The data collected during this effort resulted in a change to the fielded flare sequence for the CH-47F IRSS, thus providing better protection for those aircraft against MANPADS. These fielding decisions are in support of ongoing operations, including Operation Freedom's Sentinel, and in response to a JUONS. After the test, the Center published an independent assessment analysis report. The ARDEC conducted the test from October 28 through November 17, 2017, at Test Area 6, Redstone Arsenal, Huntsville, Alabama.

UUNS

Navy: MV-22B UUNS Department of the Navy (DON) LAIRCM ATW Integrated ASE Quick Reaction Assessment Test

- **Sponsor:** PMA-272 and the Navy Operational Test and Evaluation Force (OPTEVFOR)
- **Activity/Benefit:** The Center provided two MSALTS missile plume simulators for two-color IR missile plume simulations and jam beam data collection and a laser mobile test van with threat lasers. The Center collected data and performed a preliminary assessment to help PMA-272 and OPTEVFOR evaluate the DON LAIRCM ATW system installed on the MV-22B and its readiness for rapid fielding. Center participation in this test was in direct support of ongoing PMA-272 and OPTEVFOR UUNS efforts. PMA-272 and OPTEVFOR conducted the test from October 10 – 17, 2017, at Yuma Proving Ground, Arizona.

Navy: MV-22 UUNS DON LAIRCM ATW Integrated Test

- **Sponsor:** PMA-272 and the Navy OPTEVFOR
- **Activity/Benefit:** The Center provided one MSALTS missile plume simulator for two-color IR missile plume simulations and jam beam data collection. The Center collected data and performed a preliminary assessment to help PMA-272 and OPTEVFOR evaluate the DON LAIRCM ATW system for integration onto the MV-22B aircraft. Center participation in this test was in direct support of ongoing PMA-272 and OPTEVFOR UUNS efforts. PMA-272 and OPTEVFOR conducted the test from February 12 – 23, 2018, at Yuma Proving Ground, Arizona.

ASE ACTIVITIES

Army: Common Infrared Countermeasure (CIRCM) Program of Record

- **Sponsor:** PMO ASE
- **Activity/Benefit:** The Center generated 24,150 UV/IR missile plume signatures for the CIRCM program to use during hardware-in-the-loop and flight testing. The Center provided MSALTS and JMITS simultaneous UV/IR missile plume simulations and jam beam data collection. The Center's simulators conducted single threat engagements (MSALTS) and dual threat engagements (MSALTS/JMITS) against the CMWS and CIRCM as installed on the HH-60M and UH-60M. The Center provided near real-time feedback on missile plume simulation quality and jam beam data. These tests evaluated CIRCM end-to-end functional performance while exposed to own ship motion, vibration, and electromagnetic environments specific to the aircraft. The Center also provided the JSIS to collect signature data during missile firings. The PMO ASE conducted the tests to collect data during free flight missile testing, dynamic clutter, and own ship flares and guns. After the tests, the Center published an independent assessment analysis report. The PMO ASE conducted these tests from May 9 through August 9, 2018, at Test Area 3 (TA-3), Redstone Arsenal, Huntsville, Alabama.

Army: UH-60V Limited User Test
- **Sponsor:** The Aviation Test Directorate (AVTD), U.S. Army Operational Test Command (USAOTC)
- **Activity/Benefit:** The Center provided one MSALTS for single threat engagements against the CMWS as installed on the UH-60V. The Center collected data from the MSALTS UV missile plume simulations and performed a preliminary assessment to help AVTD USAOTC evaluate the integration of the CMWS on the UH-60V helicopter and determine its operational effectiveness, suitability, and survivability as input to the Low-Rate Initial Production decision. The AVTD conducted the test on May 18, 2018, and from July 30 through August 5, 2018, at TA-3, Redstone Arsenal, Huntsville, Alabama.

Army: ATW Pre-deployment Flight Test
- **Sponsor:** U.S. Army TAPO and SOAR SIMO
- **Activity/Benefit:** The Center provided one MSALTS for two-color IR missile plume simulations in support of pre-deployment training activities. The Center collected data that helped SOAR SIMO assess the DIRCM system on the aircraft while conducting training to determine if the system was ready for fielding in theater. SOAR SIMO conducted the test from August 20 – 24, 2018, at China Lake, California.

Navy: DON LAIRCM ATW KC-130J Integration Verification Flight Test
- **Sponsor:** PMA-272
- **Activity/Benefit:** The Center provided one MSALTS missile plume simulator for two-color IR missile plume simulations and jam beam data collection. The Center collected data during this effort that helped PMA-272 evaluate the integration of the DON LAIRCM ATW onto the KC-130J aircraft equipped with the GLTA. PMA-272 conducted the test on February 2, 2018, at the Courtland Airport, Cortland, Alabama.

Navy: CH-53E DON LAIRCM ATW Software Formal Release 3.1a Flight Test
- **Sponsor:** PMA-272 and the Navy OPTEVFOR
- **Activity/Benefit:** The Center provided one MSALTS for two-color IR missile plume simulations and jam beam data collection. The Center collected data during this effort that helped PMA-272 and OPTEVFOR assess the performance of the DON LAIRCM ATW on the CH-53E helicopter equipped with the GLTA. These data also helped PMA-272 and OPTEVFOR determine whether ATW Formal Engineering Software Release 3.1a correctly updated prior software releases and whether this software release was ready for fielding to aircraft platforms in theater. PMA-272 conducted the test on May 23 – 24, 2018, at Ingalls Field, Hot Springs, Virginia.

Navy: Poseidon Multi-mission Maritime Aircraft LAIRCM Next Generation (NexGen) P-8A Flight Tests
- **Sponsor:** Navy Air Test and Evaluation Squadron TWO ZERO (VX-20)
- **Activity/Benefit:** The Center provided missile plume simulators for two-color IR simulations and jam beam data collection during multiple, separately scheduled test events. VX-20 conducted the LAIRCM System Processor Replacement (LSPR) flight test from December 3 – 8, 2017, the (2103) Legacy Processor Software Update Flight Test from December 9 –13, 2017, and the DIRCM Situational Awareness Flight Test from July 23 – 27, 2018. VX-20 conducted all these tests at Eglin AFB, Florida. The Center collected data during these efforts that helped VX-20 assess the LAIRCM NexGen system upgrades as installed on the P-8A aircraft under operationally representative conditions. VX-20 also used these data to verify that the system accomplished missile warning to turret hand-off and delivery of jam energy in a clutter environment.

Air Force: KC-135 LAIRCM NexGen LSPR and Attitude Reference Unit Replacement (ARUR) Flight Test
- **Sponsor:** U.S. Air Force, Air National Guard
- **Activity/Benefit:** The Center provided two MSALTS missile plume simulators (one stationary and one moving) for two-color IR simulations and jam beam data collection. The Center collected data during this effort that helped the Air Force assess the performance of the LAIRCM NexGen system LSPR and ARUR upgrades as installed on the KC-135 aircraft. The Air Force Air National Guard conducted the test from November 28 through December 2, 2017, at Eglin AFB, Florida.

Air Force: KC-46A LAIRCM NexGen Block 30 Flight Test
- **Sponsor:** U.S. Air Force, KC-46A Program Office
- **Activity/Benefit:** The Center provided two moving MSALTS missile plume simulators and one stationary JMITS missile plume simulator for two-color IR simulations and jam beam data collection. The Center collected data and performed a preliminary assessment to help the KC-46A Program Office assess the missile warning and DIRCM capabilities of the LAIRCM NexGen system installed on the KC-46A Block 30 aircraft in a clutter environment. The KC-46A Program Office conducted the test on June 16 – 17, 2018, at Grant County International Airport, Moses Lake, Washington.

Air Force: Joint Strike Fighter (JSF) Test Team Comparison Test
- **Sponsor:** U.S. Air Force, JSF Operational Test Team (JOTT)
- **Activity/Benefit:** The Center participated in the JOTT F-35/A-10 Comparison Test while conducting Close Air Support (CAS)/Strike Coordination and Reconnaissance/

Forward Air Controller Airborne Operations. The Center provided participating units MANPADS threat simulators for basic threat engagements, video of the engagements (after the mission) showing aircraft targeting, and log sheets with information on each engagement. The JOTT conducted the test on July 6 – 11, 2018, at MCAS Yuma, Arizona, and Naval Air Station (NAS) China Lake, California.

Air Force: Light Attack Experiment on an AT-6 Aircraft

- **Sponsor:** U.S. Air Force, 704th Test Group (TG) and the 586th FLTS
- **Activity/Benefit:** The Center provided a Mallina MANPADS MWS stimulator to support testing of the Textron AT-6 aircraft equipped with an AN/AAR-47A(V)2 MWS. The 704th TG/586th FLTS and Textron were required to test the AT-6 MWS to determine if it could correctly detect a MANPADS threat targeting the aircraft. The 704th TG and the 586th FLTS conducted the test on July 25, 2018, at the Textron facility in Wichita, Kansas.

NATO: Surface-to-Air Launch Trial (SALT) III Signature Collection and Countermeasures Test

- **Sponsor:** The Center
- **Activity/Benefit:** The Swedish Defense Research Agency under the NATO Aerospace Capability Group 3 (ACG-3), Sub Group 2 (SG2), Threat Warning Technical Team, conducted this free flight missile test from May 21 through June 1, 2018, at Vidsel Air Base, Sweden. The Center and Arnold Engineering Development Complex field teams collected radiometric signature data for the threat launches. Additionally, the Test and Evaluation Threat Resource Activity (TETRA) led diplomatic transport efforts to deliver U.S. test equipment in support of this NATO exercise. The Center will use the model updates resulting from this effort to improve MSALTS/JMITS simulations.

TRAINING SUPPORT FOR SERVICE MEMBER EXERCISES

- **Exercise and Sponsor:** The Center supported the following seven Service member exercises, focusing primarily on the JSF JOTT Integrated Product Team as it prepares for the JSF IOT&E:
  - 82nd Combat Aviation Brigade (CAB) ASE Training (December 4 – 6, 2017), Fort Bragg, North Carolina
  - 82nd CAB Field Training Exercise (February 5 – 15, 2018), Fort Bragg, North Carolina
  - JSF/Combat Search and Rescue (CSAR) JOTT (February 26 through March 2, 2018), MCAS Yuma, Arizona
  - Emerald Warrior 18 (February 26 through March 9, 2018), Hurlburt Field, Florida
  - JSF/CSAR (April 3 – 5, 2018), NAS China Lake, California
  - JSF/CAS (April 9 – 11, 2018), MCAS Yuma, Arizona
  - JSF/CAS (April 18 – 28, 2018), MCAS Yuma, Arizona
- **Activity/Benefit:** The Center provided personnel and equipment to simulate a specific MANPADS threat environment for participating aircraft, as well as SME support to observe aircraft ASE systems and crew reactions to the threat environment. At the end of each exercise, the Center's SME presented MANPADS capabilities and limitations briefings to the pilots and crews, and at the end of the briefings, allowed them to hold and manipulate the specific MANPADS. The Center provided the Services realistic threat environments used to train pilots and crew and give them a better understanding of ASE equipment and its use. The data the Center collected and provided to the trainers/testers helped the units develop and refine their tactics, techniques, and procedures to enhance survivability.

T&E TOOLS

The Center deploys its personnel and T&E tools, especially the MSALTS and JMITS missile plume simulators, throughout the country. The Center brings its latest T&E tools to the Services, providing them with cost-effective test support to collect critical data needed to assess the performance of their CM/CCM systems. In addition, the Center supports the Service's ASE programs with its unique test equipment, which reduces duplicate T&E capabilities. This benefit, along with the transportability of the Center's unique test equipment, provides the DOD a cost savings that results in "greater performance and affordability."

The Center continues to develop tools for T&E of ASE.

- The JSIS baseline was developed from FY13 – FY18 under sponsorship from the USD(AT&L) Test Resource Management Center's Central T&E Investment Program (CTEIP). JSIS 2.0, which enhances its baseline capability, will be completed in FY20.
- The Center continuously generates threat signatures for specific programs and for use in the open-air missile plume simulators JMITS and MSALTS to test installed MWS and DIRCM systems.
- The Center will upgrade JMITS/MSALTS emitters to increase bandwidth and processing capabilities to meet advanced MWS/DIRCM system requirements.
- The Center continues to upgrade its remote launcher systems.

JSIS

JSIS is a suite of equipment used to collect MANPADS and Hostile Fire threat signature data in support of ASE modeling and simulation (M&S) for T&E. These threat signature and flyout data are then used to create or improve threat models. Intelligence agencies require high fidelity threat data to produce/improve certified threat models (i.e., trajectory and signature), and threat models form the basis of the majority of ASE T&E.

JSIS is a transportable, fully integrated instrumentation suite that collects threat signatures; time, space, position information; and related threat missile and hostile fire munitions metadata. JSIS transportability is intended to allow it to be used both in the United States and abroad to reduce costs and expand the types of threat data available in the United States. The MSIC will use data collected using JSIS to create threat models for use in M&S of ASE. The Navy (PMA-272), Army (PMO ASE), and Air Force (LAIRCM System Program Office) have endorsed JSIS, and it will be an integral support element of each Program Office's aircraft self-protection capability development. Community SMEs formulated the JSIS's need as part of the IRCM Test Resources Roadmap activities. Near-term needs for operational testing with the Navy's ATW drove JSIS Initial Operational Capability (IOC), which was sponsored by the CTEIP Resource Enhancement Project. In FY18, the JSIS IOC acquisition completed. JSIS IOC was deployed to Dugway Proving Ground from June to September 2018 during free flight live events of the CIRCM and DAIRCM programs. The Center will provide MSIC the data from these events for threat model improvements that are projected for release in late 2019.

In FY18, CTEIP sponsored JSIS 2.0, which will add a missile attitude measurement capability to enhance its baseline capability. The contract to develop JSIS 2.0 was awarded in May 2018, with projected completion in FY20. Also, the Test Resource Management Center and DOT&E requested and received funding to fill capability gaps in Threat Missile M&S infrastructure from FY19 – FY23. JSIS full operational capability will address several of these capability gaps and will begin implementation in FY19.

Missile Simulator Emitters Upgrade

The JMITS and the MSALTS systems provide a transportable missile plume simulator capability to test installed MWS/DIRCM systems in an open-air environment. The Center is currently overseeing a project to upgrade the emitters on JMITS/MSALTS to increase bandwidth and processing capabilities to meet requirements of advanced MWS/DIRCM systems. IOC for the first upgraded simulator is expected during 1QFY20.

Threat Signature Generation

The Center continually generates signatures that are used as the input signatures for JMITS and MSALTS in open-air missile simulator testing of MWS/DIRCM systems. The Center has generated over 10,000 signatures for this purpose. The Center also provides signatures to various programs upon request for use in signature model analysis and test activities not involving the Center. The Center has been a key participant in an M&S Working Group that continually evaluates threat signature models with the goal of improving them and creating uniformity in model version use across the programs.

In support of the PMO ASE, the Center generated 24,150 threat signatures for the CIRCM program. The PMO ASE will use these signatures in labs and open-air testing for evaluating CIRCM performance.

Remote Launcher System (RLS)

The Center's RLS allows for the testing of ASE against live threat missiles, giving programs the ability to evaluate system performance against actual threat missiles and giving DOT&E the ability to correlate threat live fire data to prior test venue results. Free flight missile data are also used to develop missile flyout and plume signature models that labs and open-air simulators use to create simulations, develop and improve MWS algorithms, and test CMs against missiles in free flight.

The Center's three RLS test tools provide a transportable, fully-instrumented, remote launch capability for MANPADS and vehicle-launched surface-to-air missiles. Progress is underway to replace one of the current pedestals with a more robust version. IOC is expected during 2QFY19. The Center's RLS also includes a portable version designed to provide a small, portable, fully instrumented remote launch capability for MANPADS that can be used to support testing in rugged or remote locations. IOC was achieved during 3QFY18.

ALLIED T&E EFFORTS

DOT&E organizations (the Center and TETRA) co-led international efforts to partner with allied nations to support several international T&E activities that "strengthen alliances and attract new partners" in pursuit of a shared defense.

The Center and TETRA developed and supported several Allied Air Electronic Warfare (EW) Cooperative Test and Evaluation initiatives. These include:

- Efforts under the Australia, Canada, Great Britain, and U.S. Air EW Cooperative Test and Evaluation Project Arrangement (Air EW CTE PA), which is being conducted under the authority of the Multinational (Australia, Canada, Great Britain, and U.S.) Test and Evaluation Memorandum of Understanding.

- An Air EW CTE PA meeting was held from July 9 – 13, 2018, in Kingston, Canada. It was the annual "face-to-face" meeting for the Steering Committee (SC) and Project Officers (POs) from the four allied nations. The Center is the U.S. SC Chair, and PMO ASE is the U.S. PO. Several general and breakout sessions that enabled the following dedicated technical working groups (WGs) to develop plans of action took place during this meeting:
  - WG1 – M&S Capabilities
  - WG2 – Threat Environment Representation
  - WG3 – T&E Methodologies
  - WG4 – Integrated Aircraft Survivability T&E Methodology
- TETRA is the designated lead for WG2 and the Center provides SME representatives to both WG3 and WG4.
- Additionally, a radio frequency (RF) workshop was established in conjunction with the other breakout sessions for the first time. To ensure a full spectrum of Air EW T&E methodologies were being developed to handle the contested, integrated, congested electromagnetic environment, the need to include RF threats and thus RF SMEs in the group was deemed essential. TETRA organized and led the RF workshop activity.
- Over the course of the next year, all WGs and the RF workshop will continue to meet quarterly and advance their collaborative efforts. These WGs are developing opportunities to test events collaboratively, share M&S capabilities, and develop common T&E methodologies.
- Center-sponsored initiatives for coordination with two allies to develop Reciprocal Use of Test Facility Project Arrangements for collaborative T&E of Air EW systems.

The Center and TETRA continued their support for NATO's ACG-3 (Air Survivability)/SG2 (EW Self-Protection Measures for Joint Services Airborne Assets) [ACG3-SG2] with SME representatives and participation in major ACG3-SG2 trials/tests such as SALT III, Trial EMBOW, and Trial MACE. TETRA attended the two major SG2 meetings in Monterey, California, in December 2017 and London, England, in June 2018 in an effort to align U.S. needs and priorities for the SG2 upcoming trials/tests to include Trial MACE in Slovakia in July 2018.

JOINT COUNTERMEASURES T&E WG

DOT&E and DASD(DT&E) co-chartered the Joint Countermeasures Test and Evaluation Working Group (JCMT&E WG). The Center is co-lead with DASD(DT&E) of the JCMT&E WG to measure, test, and assess:

- Aircraft self-protection, CMs, and supporting tactics
- Live fire threat weapons and open-air T&E
- System performance in operationally relevant aircraft installations and combat environments
- T&E methodologies, instrumentation, analysis, and reporting

The JCMT&E WG also:

- Supported the DOD National Defense Strategy through engagement with U.S. allies and partners in measuring aircraft EW systems' effectiveness and suitability in coalition warfare environments.
- Worked within the DOD International T&E Program, the 24-nation NATO Air Force Armaments Group, SG2, and Partnership for Peace nations to deepen T&E interoperability and build a mutually beneficial international T&E network capable of decisively acting to meet shared challenges in obtaining performance and suitability data on ASE and CMs.
- Coordinated with allies to encourage alliance coalition commitment in T&E, expanded defense cooperation and developed opportunities to obtain and increase operationally relevant information to facilitate rapid fielding of new ASE capabilities.
- Initiated coordination to conduct live weapon firings of shoulder-fired and vehicle-launched missiles, small arms fire, rockets, and anti-tank guided missile firings by active duty air-defense units and test organizations.

The JCMT&E WG continues to work with the DOT&E T&E Subcommittee, National Security Council Pre-Policy Coordinating Committee, and the State Department's Office of Weapons Removal and Abatement to expand the availability of threat weapons for use by T&E programs while reducing the number of weapons that pose a serious threat to international security.

Index

Index

FY18 INDEX OF PROGRAMS

www.dote.osd.mil