DOT&E Activity and Oversight

DOD Programs

Army Programs

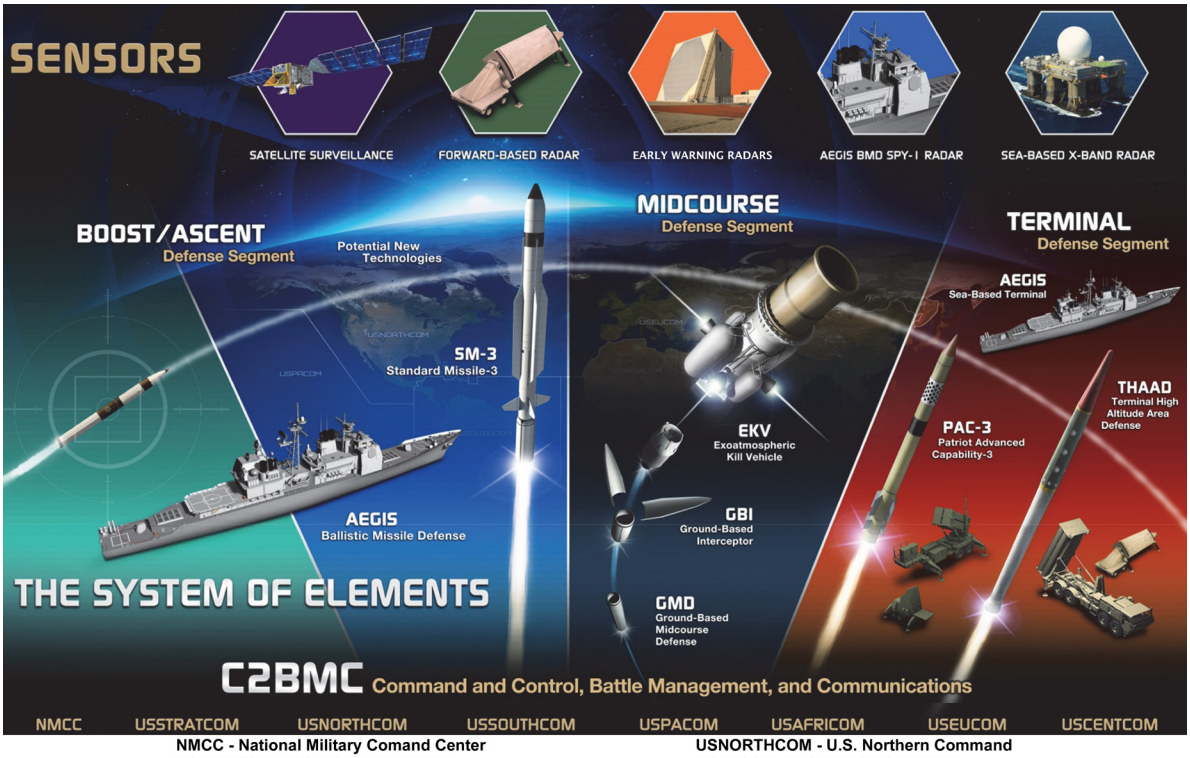
Navy Programs

Air Force Programs

Ballistic Missile Defense Programs

Ballistic Missile Defense Systems

Ballistic Missile Defense System (BMDS)



NMCC - National Military Comand Center
USAFRICOM - U.S. Africa Command
USCENTCOM - U.S. Central Command
USEUCOM - U.S. European Command
USNORTHCOM - U.S. Northern Command
USPACOM - U.S. Pacific Command
USSOUTHCOM - U.S. Southern Command
USSTRATCOM - U.S. Strategic Command

Executive Summary

- No Homeland Defense intercept flight testing occurred in FY16. Hence, previous assessments that the Ballistic Missile Defense System (BMDS) demonstrates a limited capability to defend the U.S. Northern Command (USNORTHCOM) area of responsibility from small numbers of simple intermediate-range or intercontinental ballistic missile threats (greater than 3,000 km range) launched from North Korea or Iran remain unchanged.
- The Regional/Theater BMDS demonstrates a limited capability to defend the U.S. Pacific Command (USPACOM), U.S. European Command (USEUCOM), and U.S. Central Command (USCENTCOM) areas of responsibility for small numbers of medium- and intermediate-range ballistic missile threats (1,000 to 4,000 km), and a fair capability for short-range ballistic missile threats (less than 1,000 km range).
- The Flight Test, Operational-02 (FTO-02) Event 1a flight test demonstrated an Aegis Ashore remote engagement capability with Standard Missile-3 (SM-3) Block IB Threat Update (TU) guided missiles using data from an AN/TPY 2 Forward-Based Mode (FBM) radar. This was an important demonstration of the European Phased Adaptive Approach (EPAA) Phase 2 BMDS capability. The FTO-02 Event 2a flight test demonstrated a layered BMDS with multiple combat systems sharing common defended areas and shot opportunities against two threat-representative ballistic missiles.
- The Missile Defense Agency (MDA) conducted a non-intercept Homeland Defense flight test (Ground-based Midcourse Controlled Test Vehicle-02+ (GM CTV-02+)) during which the MDA demonstrated the Capability Enhancement-II (CE-II) Exo-atmospheric Kill Vehicle (EKV) Alternate Divert Thrusters (ADTs) in an operationally realistic environment. The ADTs turned on and off as commanded and performed nominally, but the EKV experienced an anomaly unrelated to the new ADT system. The MDA collected extensive phenomenology data for discrimination improvements.
- The MDA completed the BMDS Capability Increment 6 System Requirements Review. Capability Increment 6 includes the Re-designed Kill Vehicle, Long Range Discrimination Radar, and discrimination improvements.
- Since FY10, DOT&E has assessed and reported annually that the lack of accreditation of models and simulation for performance assessment have limited DOT&E's use of these data for quantitative evaluations. This assessment remains unchanged for FY16. The MDA should increase

the development priority and associated funding for a BMDS high-fidelity, end-to-end, digital modeling and statistically significant simulation capability.
- The MDA also conducted several wargames and exercises designed to enhance Combatant Command ballistic missile defense (BMD) readiness and increase Service member confidence in the deployed elements of the BMDS.

System

The BMDS is a federated and geographically distributed system of systems that relies on element interoperability and warfighter integration for system-level operational effectiveness and efficient use of guided missile/interceptor inventory. BMDS includes five elements: four autonomous combat systems and one sensor/command and control architecture.
- Autonomous combat systems – Ground-based Midcourse Defense (GMD), Aegis BMD/Aegis Ashore Missile Defense System (AAMDS), Terminal High-Altitude Area Defense (THAAD), and Patriot
- Sensors – COBRA DANE radar, Upgraded Early Warning Radars (UEWRs), Sea Based X band (SBX) radar, AN/TPY 2 (FBM) radar, Aegis AN/SPY 1 radar aboard an Aegis BMD ship, and the Space-Based Infrared System (SBIRS)
- Command and control – Command and Control, Battle Management, and Communications (C2BMC)

Mission
- USNORTHCOM, USPACOM, 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 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
- Northrop Grumman Corporation
  - GMD Fire Control and Communications: Huntsville, Alabama
- Orbital ATK
  - GMD Booster Vehicles: Chandler, Arizona
- Raytheon Company
  - GMD EKV and SM-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 all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- The BMDS Operational Test Agency and the MDA conducted the FTO-02 Event 2a flight test in November 2015 at Wake Island and the broad-ocean area surrounding it. The primary test objective was to assess Aegis BMD system capability to prosecute a ballistic missile threat engagement in the presence of non organic post intercept debris, while simultaneously conducting anti-air warfare. The THAAD combat system, using Lot 4 interceptors for the first time, generated a non-organic post-intercept debris scene for Aegis BMD.
- The BMDS Operational Test Agency and the MDA executed the FTO-02 Event 1a flight test in December 2015 at the Pacific Missile Range Facility (PMRF) on Kauai, Hawaii. The test objective was to demonstrate the operational capability of the EPAA Phase 2 BMDS, anchored by the Aegis Ashore combat system, to defend Europe against medium-range ballistic missiles (MRBMs). The test was the first target intercept by the AAMDS and the first flight for the SM-3 Block IB TU guided missile.
- No Homeland Defense intercept flight testing occurred in FY16. The MDA conducted a non-intercept GM CTV 02+ flight test in January 2016 using GMD, the AN/TPY-2 (FBM) radar, the SBX radar, and C2BMC. This test was a demonstration of the CE-II EKV ADT and a discrimination phenomenology data collection.
- During FY16, the MDA conducted four system-level ground tests.
  - The Ground Test, Distributed-06 (GTD-06) Part 1 ground test, in October 2015, assessed BMDS-level theater/regional capabilities in USEUCOM's and USCENTCOM's area of responsibility in a distributed test environment.
  - The Ground Test, Integrated-06 (GTI-06) Part 2 ground test, in May 2016, assessed BMDS-level strategic and theater/regional capabilities in USNORTHCOM's and USPACOM's area of responsibility in an integrated test environment.
  - The Ground Test, Integrated-Israel (GTI-ISR) (16) ground test, in July 2016, assessed the interoperability of Israeli and U.S. BMDS systems in an integrated test environment.
  - The GTD-06 Part 2 ground test, in September 2016, assessed BMDS-level strategic and theater/regional capabilities in USNORTHCOM's and USPACOM's areas of responsibility in a distributed test environment.

- The MDA completed the BMDS Capability Increment 6 System Requirements Review in May 2016. Capability Increment 6 includes the Redesigned Kill Vehicle, Long Range Discrimination Radar, and discrimination improvements.
- The MDA also conducted several wargames and exercises designed to enhance Combatant Command BMD readiness and increase Service member confidence in the deployed elements of the BMDS.

Assessment

- The MDA, in collaboration with DOT&E, updated the Integrated Master Test Plan to incorporate BMDS element maturity, program modifications, and fiscal constraints.
- The FTO-02 Event 2a flight test demonstrated a layered BMDS with multiple combat systems sharing common defended areas and shot opportunities against two threat-representative ballistic missiles.
  - C2BMC software version S6.4-2.2.0 managed the AN/TPY-2 (FBM) radar, executed track reporting of sensor data to Link 16, and forwarded track data between the Aegis BMD and THAAD systems for subsequent engagements.
  - The THAAD combat system with version 2.7 software and using Lot 4 interceptors for the first time, intercepted a complex short-range ballistic missile target.
  - The Aegis BMD engaged an MRBM target. The Aegis Baseline 9.C1 destroyer operating in Integrated Air and Missile Defense radar priority mode engaged the target on remote track data from the AN/TPY-2 FBM CX-2.1.0 radar at Wake Island, and launched an SM-3 Block IB TU guided missile against the target. A faulty G-switch in the SM-3's guidance section failed early in the missile's flight, preventing a midcourse intercept. The malfunctioning G-switch precluded the separation of the missile's second stage from the first stage. A failure review board determined that the G-switch malfunctioned due to mechanical failure from abnormally high sticking in the component's lubricant. The program addressed the problem by implementing improved testing and screening of the G-switch before acceptance for installation. The new process changes were implemented and successfully flown in a controlled test flight.
  - Concurrently, the Aegis BMD ship successfully engaged a cruise missile surrogate target with an SM-2 Block IIIA guided missile.
  - THAAD also engaged the MRBM target and intercepted it.
- In FTO-02 Event 1a, sailors in the Aegis Ashore Missile Defense Test Facility at PMRF engaged an air-launched MRBM target using data from an AN/TPY-2 (FBM) CX 2.1.0 radar located at PMRF. This was an important demonstration of MRBM defense capability relevant to the EPAA Phase 2 BMDS and increased capability for theater/regional BMD. C2BMC relayed AN/TPY-2 (FBM) target track data to Aegis Ashore. Aegis Ashore fired an SM-3 Block IB TU guided missile on the remote track data, and intercepted a target for the first time. The firing assets consummated the engagement using local AN/SPY-1 radar data, rather than that of the AN/TPY-2 (FBM) radar. Although ground testing and unaccredited high-fidelity modeling and simulation have demonstrated all aspects of Aegis BMD's remote engagement capability, the lack of a flight test demonstration or data produced by accredited models reduces certainty in this capability.
- In both FTO-02 events, previously seen system network, radar track management, object discrimination and debris mitigation algorithms, and/or launch event association inaccuracies were noted again. The classified European Phased Adaptive Approach Phase 2 Operational Test and Evaluation Report and the 2015 Assessment of the BMDS report have additional assessment details and recommendations.
- During GM CTV-02+, the MDA demonstrated the CE-II EKV ADTs in an operationally realistic environment. The ADTs turned on and off as commanded and performed nominally, but the EKV experienced an anomaly unrelated to the new ADT system. See the GMD article for additional details. The MDA collected extensive phenomenology data for discrimination improvements.
- In GTD-06 Part 1, the MDA demonstrated interoperability between Aegis Ashore, Aegis BMD, THAAD, the AN/TPY-2 (FBM) radars, C2BMC, and SBIRS in scenarios against theater/regional threats in USEUCOM and USCENTCOM areas of responsibility. The MDA exercised the new capabilities of Aegis BMD software versions BL9.B1/C1, including new engagement planning functionality and an expanded threat set. These test data support the evaluation of BMDS and element-level interoperability and performance against SRBM and MRBM threats.
- In the GTI-06 Part 2 and GTD-06 Part 2 ground tests, the MDA demonstrated interoperability of the GMD GFC software version 6B3.1 with the SBIRS, UEWRs, C2BMC, AN/TPY-2 (FBM) radar, Aegis AN/SPY-1 radar in its long-range surveillance and track mode, the SBX radar, and Patriot Advanced Capability-3. The MDA evaluated a number of GMD software upgrades, including the discrimination logic, SBX tasking, and GFC salvo logic. These test data support the evaluation of GMD system performance against an expanded strategic threat set.
- BMDS-level integrated training capabilities for warfighter and interoperability functions remain limited. See the classified DOT&E European Phased Adaptive Approach Phase 2 Operational Test and Evaluation Report for additional assessment detail.
- The "integrated BMDS" refers to the full complement of BMDS combat systems that have a defensive capability for a given defended area, operating in a fully integrated fashion for the efficient use of the available interceptor inventory. The MDA has not yet demonstrated such an integrated BMDS capability. The MDA has demonstrated a basic BMDS combat capability that includes non-automated engagement planning and execution across the four threat classes (short-range, medium-range, intermediate-range, and intercontinental ballistic missiles) and in multiple phases of flight, but a

considerable amount of development is still necessary to field a robust, reliable, and fully integrated BMDS.

- In FY10, DOT&E reported, "the MDA began execution of its revamped Integrated Master Test Plan to collect the data needed to accredit the models and simulations used for assessing performance and effectiveness of the BMDS." Since then, DOT&E has assessed and reported annually that the lack of accreditation of models and simulation for performance assessment have limited DOT&E's use of these data for quantitative evaluations. This assessment remains unchanged for FY16.

Recommendations

- Status of Previous Recommendations. The MDA has addressed most previous BMDS recommendations. The following recommendations remain outstanding. The MDA should:
  1. Continue to address recommendations made in the DOT&E FTO-01 assessment found in the classified DOT&E February 2014 BMDS Annual Report, Appendix E.
  2. Increase the development priority and associated funding for the BMDS simulation-based performance assessment capability. The ability to produce high-fidelity and statistically significant BMDS level performance assessments is critical (FY14 Recommendation).
  3. Include Patriot in system-level operational flight test events in order to assess interoperability and integration between all of the BMDS combat systems and sensors. The MDA has completed initial design for flight tests in FY17-19 and has identified additional flight tests in FY20-22 to address this FY15 recommendation.
- FY16 Recommendations. The MDA should
  1. In conjunction with the Services, develop and implement integrated BMDS-level training in formal warfighter certification plans.
  2. Assess the performance of the BMDS in both flight and ground testing using realistic Link 16 loading and network configurations.
  3. Include the situational awareness tools used by the fire coordination and link management officers in their assessment of BMDS performance and ensure that warfighter involvement in testing is reflective of Combatant Command operations.
  4. Publish a comprehensive BMDS cybersecurity document that delineates the strategy for effective cybersecurity, achievable milestones for implementing the strategy, and stakeholder roles and responsibilities.
  5. Include reliability, maintainability, availability, and supportability data collectors for all participating elements in operationally realistic flight and ground test events to ensure that sufficient reliability, maintainability, availability, and supportability data are collected to allow for an assessment of operation suitability for all BMDS elements and sensors.
  6. Use targets with threat-representative reactive payloads in some future flight testing to improve the evaluation of lethality, sensor loading, battle management, and kill assessment.

Sensors / Command and Control Architecture

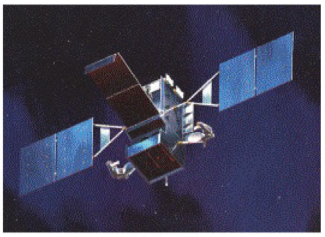

Aegis AN/SPY-1 Radar


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

Executive Summary

- The Missile Defense Agency (MDA) continued to mature the Ballistic Missile Defense System (BMDS) sensors/command and control architecture. During FY16, the MDA used the sensor/command and control architecture in one Ground-based Midcourse Defense (GMD) developmental flight test, two BMDS operational flight tests, and four ground tests. Additionally, the Air Force used the sensor/command and control architecture in one intercontinental ballistic missile (ICBM) reliability and sustainment flight test.
- Many COBRA DANE radar system components and facilities are past the original design lifespan. Options for long-term supportability are diminishing and many of the original equipment manufacturers no longer exist. The Air Force awarded a $77 Million, 2-year contract to Raytheon for operations, maintenance, and sustainment of the COBRA DANE radar.
- The MDA demonstrated AN/TPY-2 Forward-Based Mode (FBM) radar capabilities, including enhanced tracking; improved debris mitigation and launch complex association algorithms; and updated discrimination and decision control logic.
- The Army continues to transition AN/TPY-2 (FBM) radar operations and maintenance from contractor logistics support to organic soldier operations and maintenance. Training and documentation deficiencies continue to be discovered, most recently in both Flight Test, Operational-02 (FTO-02) events. Soldiers are now responsible for activities at two of the five deployed radars.
- The MDA demonstrated Command and Control, Battle Management, and Communications (C2BMC) threat assessment, threat evaluation, sensor resource management, sensor track data processing, track reporting, target selection, discrimination and debris mitigation tasking, sensor/weapon access determination, and engagement monitoring during dedicated flight and ground testing as well as when tracking real-world ballistic missile targets-of-opportunity. C2BMC provided Combatant Commanders with timely and accurate information on numerous real-world events.
- The MDA awarded Lockheed Martin a $784.3 Million contract to develop and operate the Long Range Discrimination Radar.

System

- The BMDS sensors are systems that provide real-time ballistic missile threat data to the BMDS. The data are used to counter ballistic missile attacks. The sensor systems are operated by the Army, Navy, Air Force, and the MDA.
  - The COBRA DANE radar is a fixed site, single-face, 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, multiple-face, ultra-high frequency radars operated by the Air Force and located at Beale AFB, California (two radar faces); Fylingdales, United Kingdom (three radar faces); and Thule, Greenland (two radar faces). The MDA and Air Force Space Command are also upgrading the Early Warning Radars in Clear Air Force Station, Alaska (FY17), and Cape Cod Air Force Station, Massachusetts (FY18).
  - The Sea-Based X-band (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 (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 list of BMDS sensors also includes the Aegis AN/SPY-1 radar and the Space-Based Infrared System (SBIRS)/Defense Support Program satellites. See the Aegis Ballistic Missile Defense (BMD) and SBIRS articles (pages 413 and 403, respectively), for reporting on these sensors.
- The C2BMC system is a Combatant Command interface to the BMDS. More than 70 C2BMC workstations are fielded at U.S. Strategic Command, U.S. Northern Command (USNORTHCOM), U.S. European Command (USEUCOM), U.S. Pacific Command (USPACOM), and USCENTCOM; numerous Army Air and Missile Defense Commands; Air and Space Operations 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 by displaying selective BMDS data for strategic/national missile defense and for theater/regional missile defense, utilizing multiple message formats and diverse terrestrial and satellite communications paths.
  - The C2BMC also provides a consolidated upper echelon BMD mission plan at the Combatant Command and component level. BMDS elements (Aegis BMD, GMD, Patriot, and Terminal High-Altitude Area Defense (THAAD)) use their own command and control battle management systems and mission-planning tools for stand-alone engagements.
  - The current C2BMC S6.4 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.
  - Using the BMDS Communications Network, the C2BMC forwards AN/TPY-2 (FBM) and AN/SPY-1 tracks to GMD. C2BMC uses the Tactical Digital Information Link-Joint message formats to send C2BMC system track data to THAAD, Patriot, and coalition systems for sensor cueing and for Aegis BMD engagement support.
  - The C2BMC S8.2 (projected for FY17-18) is intended to mature and expand S6.4 capabilities as the next major step toward integrated, automated sensor management and engagement coordination.

Mission
- Combatant Commands use the BMDS sensors to detect, track, and classify/discriminate ballistic missile threats that target the United States and U.S. allies.
- 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
- C2BMC: Lockheed Martin Corporation, Rotary and Mission Systems – Huntsville, Alabama, and Colorado Springs, Colorado

---

Activity
- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- During FY16, the MDA and the Air Force used the sensor/command and control architecture in nine tests. The MDA executed one GMD developmental flight test, two BMDS operational flight tests, and four ground tests; the Air Force executed one ICBM reliability and sustainment flight test.
  - The FTO-02 Event 2a flight test, in October 2015, assessed a layered BMDS defense with multiple combat systems sharing common defended areas and shot opportunities.
  - The Ground Test, Distributed-06 (GTD-06) Part 1 ground test, in October 2015, assessed BMDS-level theater/ regional capabilities in USEUCOM's and USCENTCOM's areas of responsibility in a distributed test environment.
  - The FTO-02 Event 1a flight test, in December 2015, assessed the operational capability of the regional/theater European Phased, Adaptive Approach Phase 2 BMDS, anchored by the Aegis Ashore Missile Defense System, to defend Europe against medium-range ballistic missiles.

  - The Ground-based Midcourse Controlled Test Vehicle-02+ (GM CTV-02+) flight test, in January 2016, assessed the Capability Enhancement-II Exo-atmospheric Kill Vehicle Alternate Divert Thruster performance in a flight environment while also assessing discrimination data flow through the fire control loop.
  - The Ground Test, Integrated-06 (GTI-06) Part 2 ground test, in May 2016, assessed BMDS-level strategic and theater/regional capabilities in USNORTHCOM's and USPACOM's area of responsibility in an integrated test environment.
  - The Ground Test, Integrated-Israel (GTI-ISR) (16) ground test, in July 2016, assessed the interoperability of Israeli and U.S. BMDS systems in an integrated test environment.
  - The GTD-06 Part 2 ground test, in September 2016, assessed BMDS-level strategic and theater/regional capabilities in USNORTHCOM's and USPACOM's area of responsibility in a distributed test environment.
  - The Glory Trip 219 flight test, in September 2016, is an Air Force Minuteman III ICBM reliability and sustainment assessment.
- The MDA used hardware-in-the-loop, training devices, and analytical models of the COBRA DANE radar, Beale UEWR, Thule UEWR, and Fylingdales UEWR during the GTI-06 Part 2 and GTD-06 Part 2 ground tests. In addition, the MDA used the Beale UEWR in the GM CTV-02+ flight test. The MDA also developed a COBRA DANE and Thule UEWR targets-of-opportunity campaign that will begin in FY17.
- The SBX radar was used in one GMD developmental flight test (GM CTV-02+), one ICBM reliability and sustainment flight test (Glory Trip 219), and two ground tests (GTI-06 Part 2 and GTD-06 Part 2).
- The MDA used the AN/TPY-2 (FBM) radar and C2BMC in one GMD developmental flight test (GM CTV-02+), two BMDS operational flight tests (FTO-02 Event 2a and FTO-02 Event 1a), and four ground tests (GTD-06 Part 1, GTI-06 Part 2, GTI-ISR (16), and GTD-06 Part 2). In addition, the Air Force used C2BMC and the AN/TPY-2 (FBM) radar in one ICBM reliability and sustainment flight test (Glory Trip 219).
- In January 2016, the MDA evaluated C2BMC Spiral 6.4 and AN/TPY-2 (FBM) in an Element Cybersecurity Experiment (ECE) to identify cybersecurity vulnerabilities with participation from Cyber Protection Team 800.
- In October 2015, the MDA awarded Lockheed Martin a $784.3 Million contract to develop and operate the Long Range Discrimination Radar. The MDA completed the System Requirements Review in February 2016.

Assessment

- During ground testing, the MDA gathered data to support evaluation of software upgrades and cybersecurity of the COBRA DANE radar, UEWRs, and the AN/TPY-2 and SBX radars, including verification that the COBRA DANE radar software upgrades resolved a technical issue related to scan-dependent biases.
- Many COBRA DANE radar system components and facilities are past the original design lifespan. Options for long-term supportability are diminishing, and many of the original equipment manufacturers no longer exist. In December 2015, the Air Force awarded a $77 Million, 2-year contract to Raytheon for operations, maintenance, and sustainment of the COBRA DANE radar.
- The ground test data showed mixed UEWR performance with several new missile threat objects added to the UEWR object classification database.
- The MDA demonstrated AN/TPY-2 (FBM) radar software upgrades, including enhanced tracking; improved debris mitigation and launch complex association algorithms; and updated discrimination and decision control logic.
- The MDA and the Army continue working to achieve full materiel release of the AN/TPY-2 (FBM) radar. Of the nine original materiel release conditions the Army created in 2012, the Army closed seven by 2014 and migrated the remaining two to the set of materiel release conditions associated with software version CX-1.2.3_18. Of the 25 CX 1.2.3_18 materiel release conditions, the Army closed one prior to 2016 and the Army closed four in 2016. The Army is also in the process of establishing additional materiel release conditions for software version CX-2.1.0.
- The Army continues to transition AN/TPY-2 (FBM) radar operations and maintenance from contractor logistics support to organic soldier operations and maintenance. Training and documentation deficiencies continue to be discovered, most recently in both FTO-02 events. Soldiers are now responsible for activities at two of the five deployed radars.
- In Glory Trip 219, the SBX radar acquired and tracked the Minuteman III ballistic missile through the boost and/or midcourse phases of flight.
- The MDA demonstrated C2BMC threat assessment, threat evaluation, sensor resource management, sensor track data processing, track reporting, target selection, sensor/weapon access determination, and engagement monitoring during dedicated flight and ground testing, as well as during real-world ballistic missile targets-of-opportunity.
  - The system demonstrated dual radar management and track processing/reporting utilizing operational C2BMC suites and communications.
  - The C2BMC engagement planner provided non-real-time performance analysis of the composition and location of U.S. and allied BMD assets, but does not currently provide a system-level capability to coordinate engagement decisions.
  - Software version S6.4-3.0 provided discrimination tasking of the AN/TPY-2 (FBM) radar for long-range threats, multiple-radar discrimination tasking of a threat, and several fixes related to message sequencing and timing.
  - During GM CTV-02+, the MDA used passive links to conduct real-time activities with upcoming C2BMC version S8.2 and to collect data on closed loop fire control, enhanced tracking, post intercept assessment, and discrimination.

  - During FTO-02 Event 1a, C2BMC demonstrated support to Aegis BMD Launch on Remote via track processing of AN/TPY-2 data, system track formation, system track selection, and Link 16 track reporting.
  - Flight testing with C2BMC control of two AN/TPY-2 (FBM) radars has yet to occur. However, C2BMC did exercise dual radar management, precision cueing, and system track formation during a dedicated ground test (USEUCOM and USCENTCOM areas of responsibility) and during real-world targets of opportunity (USPACOM and USEUCOM areas of responsibility).
  - C2BMC has not demonstrated real-time engagement direction capabilities.
- Problems previously discovered during testing, if not corrected, could adversely affect C2BMC effectiveness. These problems, the details of which can be found in DOT&E's classified 2015 Assessment of the BMDS, include:
  - Track management and track processing problems
  - Data management problems

Recommendations

- Status of Previous Recommendations. The MDA has addressed all but two previous recommendations for the sensors/command and control architecture. The MDA:
  1. Made progress on sensor/command and control architecture cybersecurity testing by performing basic testing and system scans during GTI-06 Part 2 and one ECE. The MDA should continue to increase the number of components and the fidelity of its cybersecurity assessments.
  2. Has initiated, but not completed, a study on the additional sensor requirements for an effective defense of Hawaii.
- FY16 Recommendations. The MDA should:
  1. With the Air Force, identify spare and replacement part sources for long-term COBRA DANE radar sustainment.
  2. With the Army, update AN/TPY-2 (FBM) Interactive Electronic Technical Manuals and improve AN/TPY-2 (FBM) radar operator training.
  3. Perform a flight test with multiple AN/TPY-2 (FBM) radars to assess the ability of C2BMC to correctly task and fuse track data from multiple sources observing realistic targets and to assess the ability to disseminate the subsequent system-level data across the BMDS. Additionally, the MDA should evaluate BMDS performance in dual radar missions, particularly Defense of Europe for USEUCOM and Homeland Defense for USNORTHCOM, using the COCOM suite (which can only manage one radar), when the C2BMC Global Engagement Manager is non-mission capable.
  4. Continue C2BMC development efforts to provide an engagement management capability to the BMDS.

Aegis Ballistic Missile Defense (Aegis BMD)

Executive Summary

- The Missile Defense Agency (MDA) conducted three Aegis Ballistic Missile Defense (BMD) intercept flight tests in FY16. Overall, Aegis BMD successfully engaged two ballistic missile targets and one anti-air warfare target and failed to intercept one ballistic missile target.
- The MDA conducted operational flight testing of the Aegis Baseline 9.1 system (i.e., Aegis BMD 5.0 Capability Upgrade) in its Aegis Ashore (Baseline 9.B1) and Aegis destroyer (Baseline 9.C1) configurations with Standard Missile-3 (SM-3) Block IB Threat Upgrade (TU) guided missiles. Additionally, the MDA conducted developmental flight testing of the SM-3 Block IB TU guided missile and Sea-Based Terminal (SBT) capability.
- Although the program completed FOT&E for Aegis BMD 3.6.1 and IOT&E for Aegis BMD 4.0 in FY11 and FY15, respectively, the program continued to use system variants (i.e., Aegis BMD 3.6.3 and 4.0.3) in flight and ground tests and a U.S. Navy Fleet exercise in FY16 to assess element- and system-level engagement capabilities, long range surveillance and track (LRS&T) capabilities, and interoperability with the BMDS and foreign missile defense assets.
- During one of the five live-guided missile tests conducted in FY16, the SM-3 Block IB TU missile failed to launch from the Aegis BMD ship.
- The MDA conducted two developmental flight tests and six design verification and qualification ground test firings of the SM-3 Block IB TU Third Stage Rocket Motor (TSRM) to verify an aft nozzle area re-design that improves missile reliability.
- Testing demonstrated engagement capabilities against short and medium-range ballistic missiles (SRBM/MRBM) in both endo- and exo-atmospheric engagements and against anti-air warfare targets.
- Flight testing, modeling and simulation (M&S), and ground testing have demonstrated Aegis BMD capabilities to perform LRS&T.
- During integration testing of an SM-3 Block IIA flight test round, the Kinetic Warhead's guidance unit experienced a failure.
- Operational Aegis BMD assets and hardware-in-the-loop (HWIL) facilities underwent cybersecurity testing.
- The MDA deployed an Aegis Ashore site to Romania, and the U.S. European Command (USEUCOM) declared it operational.

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 threats. Capabilities of Aegis BMD include:
  - Computer program modifications to the AN/SPY-1 radar for LRS&T of ballistic missiles of all ranges
  - A modified Aegis Vertical Launching System, which stores and fires SM-3 Block IA and Block IB guided missiles, modified SM-2 Block IV guided missiles, and SM-6 Dual I guided missiles
  - SM-3 Block IA and Block IB guided missiles that use maneuverable kinetic warheads to accomplish midcourse engagements of SRBMs, MRBMs, and intermediate-range ballistic missiles (IRBMs)
  - Modified SM-2 Block IV guided missiles that provide terminal engagement capability against SRBMs and MRBMs
  - SM-6 Dual I 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 Ashore (Baseline 9.B1) is a 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 first Aegis Ashore site in Romania is the central, land-based component of the second phase of the European Phased-Adaptive Approach (EPAA) for the defense of Europe.
- Aegis BMD ships and Aegis Ashore are capable of performing missile defense operations and sending/receiving cues to/from other BMDS sensors through tactical datalinks. Aegis BMD ships are capable of performing autonomous missile defense operations while both Aegis BMD ships and Aegis Ashore are capable of performing engagements using remote track data from BMDS sensors.

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 Dual I Missiles: Raytheon Company, Missile Systems – Tucson, Arizona

---

Activity

- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- In FY16, the MDA conducted operational flight testing of the Aegis Baseline 9.1 system in its Aegis Ashore (Baseline 9.B1) and Aegis destroyer (Baseline 9.C1) configurations with SM-3 Block IB TU guided missiles and conducted developmental flight testing of SBT capability.
- Although the program completed FOT&E for Aegis BMD 3.6.1 and IOT&E for Aegis BMD 4.0 in FY11 and FY15, respectively, the program continued to use system variants (i.e., Aegis BMD 3.6.3 and 4.0.3) in flight tests, system-level tests, and a U.S. Navy Fleet exercise in FY16 to assess element- and system-level engagement and LRS&T capabilities and interoperability with the BMDS and foreign missile defense assets.
- The MDA conducted three Aegis BMD intercept flight tests in FY16. Overall, Aegis BMD successfully engaged two ballistic missile targets and one anti-air warfare target and failed to intercept one ballistic missile target.
  - In October 2015, Aegis BMD participated in At-Sea Demonstration-15, a multi-event fleet exercise conducted in the United Kingdom's Hebrides Missile Range wherein assets from NATO member countries exchanged air and ballistic missile message information across operational communication architectures during cruise missile and ballistic missile engagements. In one of the nine exercise events, an Aegis BMD 3.6.3 destroyer with an SM-3 Block IA guided missile engaged and intercepted a non-separating SRBM target. Participating assets also included an Aegis BMD 3.6.3 laboratory representation, an Aegis 5.3.10 air defense ship, C2BMC, and Allied naval vessels from Great Britain, Spain, Netherlands, Italy, Canada, France, and Norway.
  - In November 2015, an Aegis Baseline 9.C1 destroyer operating in Integrated Air and Missile Defense (IAMD) radar priority mode participated in Flight Test Operational (FTO)-02 Event 2a at Wake Island and the broad-ocean area surrounding it. The MDA and BMDS Operational Test Agency (OTA) designed the test mission to demonstrate a layered BMDS with Aegis BMD and Terminal High-Altitude Area Defense (THAAD) sharing common defended areas and shot opportunities against two threat-representative ballistic missile targets. The primary Aegis BMD test objective was to prosecute a ballistic missile engagement in the presence of non-organic post-intercept debris generated by a THAAD intercept, while simultaneously conducting anti-air warfare against an anti-ship cruise missile surrogate. However, the SM-3 missile failed in flight, preventing a midcourse intercept of the ballistic missile target, while the Aegis BMD ship did successfully engage the cruise missile surrogate with an SM-2 Block IIIA guided missile. The MDA initially attempted to conduct this test in October 2015 as FTO-02 Event 2; however, due to a THAAD target malfunction, the October event was a "No Test."
  - In December 2015, the OTA and the MDA conducted FTO-02 Event 1a at the Pacific Missile Range Facility (PMRF) on Kauai, Hawaii. The test intended to demonstrate the operational capability of the EPAA Phase 2 BMDS, anchored by the Aegis Ashore combat system, to defend Europe against MRBMs. In the test, the Aegis Ashore Missile Defense Test Complex at PMRF engaged an air-launched MRBM target with an SM-3 Block IB TU guided missile using data from an AN/TPY-2 (Forward-Based Mode (FBM)) radar located at PMRF. This was the first intercept flight test for Aegis Ashore.
- Aegis BMD participated in two live-target and five live-guided missile test events in FY16. During one of the live-guided events, the SM-3 Block 1B TU missile failed to launch from the Aegis BMD ship.
  - In December 2015, the MDA conducted Aegis Ashore Control Test Vehicle-02 (CTV-02), a guided missile-only firing of an SM-3 Block IB TU missile. The MDA conducted this live-fire event as a risk reduction flight for FTO-02 Event 1a.
  - In December 2015, the MDA conducted Standard Missile Cooperative Development CTV-02, a guided missile-only, developmental flight test of the SM-3 Block IIA missile through nosecone deployment and kinetic warhead ejection. This was the second live-fire event for the SM-3 Block IIA guided missile, which is a joint U.S.-Japanese development of a 21-inch diameter variant of the SM-3.
  - In February 2016, the MDA conducted Standard Missile CTV-01, planned to be the first of two guided missile-only firings to verify the re-designed SM-3 Block IB TU TSRM aft nozzle area. The SM-3 Block IB TU missile failed to launch from the Aegis BMD 3.6.3 destroyer.

  - In May 2016, the MDA conducted SM CTV-01a, a re-test of SM CTV-01. An Aegis BMD 3.6.3 destroyer fired an SM-3 Block IB TU guided missile against a simulated test target to exercise a two-pulse firing of the TSRM using a minimum inter-pulse delay between the TSRM axial thrust burns. This was the first SM-3 Block IB firing from an Aegis BMD 3.6.3 ship.
  - In May 2016, the MDA conducted SM CTV-02. An Aegis BMD 3.6.3 destroyer fired an SM-3 Block IB TU guided missile against a simulated test target to exercise a two-pulse firing of the TSRM using a maximum inter-pulse delay between TSRM axial thrust burns.
  - In May 2016, the MDA conducted Flight Test Other-21 (FTX-21), planned to demonstrate the ability of an Aegis Baseline 9.C1-configured destroyer to detect and track an MRBM target within the Earth's atmosphere. The test was a risk reduction exercise for the future Flight Test Standard Missile (FTM)-27 flight test mission, which is planned for 1QFY17.
  - In June 2016, the Navy conducted Pacific Dragon, a Commander, Pacific Fleet-directed exercise. An Aegis Baseline 9.C2-equipped ship performed a simulated SM-3 Block IIA engagement against a separating MRBM target. This exercise served as risk reduction for the future Standard Missile Cooperative Development Project Flight Test Standard Missile-01 (SFTM-01) flight test mission and explored interoperability between U.S. Navy forces and naval assets from Japan and the Republic of Korea.
- Aegis BMD provided HWIL representations for four BMDS ground tests that provided information on Aegis BMD interoperability and functionality in various regional/theater scenarios:
  - GTD-06 Part 1 in October 2015 examined defense of USEUCOM and U.S. Central Command scenarios, using Aegis Baseline 9.B1 (Aegis Ashore Missile Defense System in Romania), Baseline 9.C1, Aegis BMD 4.0.3, and Aegis BMD 3.6.3.
  - GTI-06 Part 2 in April 2016 examined defense of U.S. Pacific Command and Homeland defense scenarios, using Aegis Baseline 9.C1, Aegis BMD 4.0.3, and Aegis BMD 3.6.3.
  - GTI-Israel-16 in June 2016 studied interoperability between the BMDS and the Arrow Weapon System for maintaining shared situational awareness, using Aegis BMD 4.0.3 and Baseline 9.C1.
  - GTD-06 Part 2 in September 2016 again examined defense of U.S. Pacific Command and Homeland defense scenarios, using Aegis BMD 3.6.3, Aegis BMD 4.0.3, and Aegis Baseline 9.C1.
- During integration testing of an SM-3 Block IIA flight test round, in preparation for SFTM-01, the MDA discovered a problem with the Kinetic Warhead's Guidance Unit.
- The Navy's Commander, Operational Test and Evaluation Force (COTF) conducted high-fidelity digital M&S runs using accredited models in support of Aegis Baseline 9.B1 in September 2016.
- COTF conducted a cybersecurity Adversarial Assessment of Aegis Baseline 9.B1 in June 2016 at the Aegis Ashore Missile Defense Facility in Romania. The Adversarial Assessment was the first cybersecurity assessment conducted on the Aegis Ashore Missile Defense System.
- USEUCOM declared the Aegis Ashore Missile Defense System in Romania operational in July 2016.

Assessment

- The Aegis BMD 4.0 system, which is the latest, widely deployed version of Aegis BMD and the primary sea-based firing asset for EPAA Phase 2, participated in HWIL and distributed ground test events in FY16 primarily to demonstrate LRS&T improvements in support of Ground-based Midcourse Defense (GMD) with the Aegis BMD 4.0.3 update.
- Prior IOT&E flight testing and supporting M&S demonstrated that Aegis BMD 4.0 has the capability to engage and intercept non-separating, simple-separating, and complex-separating ballistic missiles in the midcourse phase with SM-3 Block IB guided missiles. However, flight testing and M&S are not yet sufficient to assess the full range of expected threat types, ground ranges, and raid sizes. Details on Aegis BMD 4.0 performance can be found in the classified December 2014 Aegis BMD 4.0 IOT&E Report.
- In FY16, Aegis Baseline 9.B1 and Baseline 9.C1 underwent operational flight testing of those systems' remote engagement capabilities with SM-3 Block IB TU guided missiles using data from an AN/TPY-2 (FBM) radar (during FTO-02 Events 2a and 1a). The successful intercept in FTO-02 Event 1a by the Aegis Ashore Missile Defense Test Complex at PMRF demonstrated an MRBM defense capability relevant to EPAA Phase 2. During FTO-02 Event 2a, the SM-3 failed in flight; however, this event contributed tracking and engagement processing data relevant to an assessment of Aegis BMD's remote engagement capabilities. Similar to previous tests with remote engagements (FTM-15 in FY11 and FTM-20 in FY13), the system did not use remote AN/TPY-2 (FBM) radar data throughout the engagement. Instead, the firing assets consummated the engagement using local AN/SPY-1 radar data. Although Aegis BMD HWIL, distributed ground testing, and unaccredited high-fidelity M&S have demonstrated all remote engagement modes, the lack of a flight test demonstration of a fully remote engagement reduces certainty in that capability. High-fidelity digital M&S run results using accredited models in support of Aegis Baseline 9.B1 will be available 1QFY17 to support future assessments.
- In FTO-02 Event 2a, the SM-3 Block IB TU guided missile failed early in flight due to a faulty G-switch in the guidance section of the missile. The malfunctioning G-switch precluded the separation of the missile's second stage from the first stage. A failure review board (FRB) determined that the G-switch malfunctioned due to mechanical failure caused by abnormally high sticking in the component's lubricant. The program implemented improved testing and screening of the G-switch

before acceptance for installation to address the problem. The MDA implemented the new process changes prior to the successful SM CTV-01a and -02 flight tests.

- The MDA demonstrated the efficacy of the SM-3 Block IB TU re-designed TSRM aft nozzle area, to improve missile reliability following the FTM-16 Event 2 (FY11) and FTM-21 (FY13) failures during two flight tests (SM CTV-01a and -02) and six design verification and qualification ground test firings.
- Additional SM-3 Block IB component anomalies have occurred in recent flight and lot acceptance testing, one resulting in a failed SM-3 launch.
  - Low TSRM Attitude Control System cold gas regulator (CGR) pressures were observed in FTM-25 (FY15) and during lot acceptance testing. The CGR anomaly in FTM-25 did not preclude the target from being intercepted; however, the cold gas pressure observed was much lower than that commanded. If the regulated pressure from the CGR is too low, the Attitude Control System may not function properly. The Prime Contractor (Raytheon Missile Systems) established an FRB, which determined that now-defunct tooling procedures caused the FTM-25 CGR anomaly. The FRB determined that changes to the CGR C-seal's spring dimensions, additional inspections, and an enhanced acceptance test process addressed the low pressure anomalies from the lot acceptance tests.
  - A second anomaly was observed during SM CTV-01 when an SM-3 Block IB TU failed to launch due to the missile failing a pre-launch booster nozzle response built-in test designed to ensure safe missile egress from the firing ship. An FRB determined that random minor voltage glitches in guidance section components caused short-duration (tens of milliseconds) corrupted commands to be sent to the booster nozzle, which resulted in a failure of the built-in test. To address the problem, the program developed software that mitigates the possibility of failure by introducing logic to re-send commands up to two additional times. The new software was successfully flown in SM CTV-01a and -02, and will be installed on new production rounds.
  - Third, lot acceptance testing revealed a number of SM-3 Block IB TU kinetic warhead guidance units that were unresponsive at power up. An FRB established the root cause to be related to memory management during boot up. The MDA has implemented a minor change to the kinetic warhead's guidance unit software to correct the anomaly. These two software changes will be loaded on all Block IB TU missiles at their 4-year recertification periods.
- The successful simulated engagement in the Pacific Dragon Fleet exercise demonstrated the organic engagement capabilities of the Baseline 9.C2 system.
- The FTX-21 flight mission demonstrated the endo-atmospheric tracking capabilities of the Aegis Baseline 9.C1 system, which are relevant for the SBT engagement mission; however, no SBT engagements were attempted in FY16. To date, intercept testing of the Baseline 9.C1's SBT capabilities consists of the first two multi-mission warfare events in FY15. These events demonstrated that SM-6 Dual I and SM-2 Block IV missiles can be used to conduct SBT engagements against non-separating SRBMs, but high-fidelity M&S analyses conducted using models accredited by the BMDS OTA have not yet occurred, so SBT engagement performance cannot be quantitatively evaluated. Completion of a subset of the SBT M&S analyses is expected in 1QFY17.
- The MDA demonstrated Aegis Baseline 9.C1 system's IAMD capabilities to a limited degree in FTO-02 Event 2a, when the firing ship performed a remote ballistic missile engagement with the system operating in IAMD radar priority mode while conducting an anti-air warfare engagement against a single cruise missile surrogate. The demonstration of IAMD capabilities in FTO-02 Event 2a was not stressing, even less so than during FTM-25 (FY15), where a raid of two cruise missiles and a single ballistic missile target were simultaneously engaged in an organic engagement.
- Reliability, maintainability, availability, and supportability (RMA&S) data collected during Aegis Baseline 9.1 BMD-related testing through FY15 show that the system has lower than desired software stability. Also, the data show that the system does not currently meet its requirements for availability and mean time to repair hardware, mostly due to a series of early Aegis Display System failures and an AN/SPY-1 radar coolant leak that downed the system for an extended period of time. The majority of the Aegis Display System problems have since been addressed with the installation of new console graphics cards. DOT&E will reassess RMA&S once the MDA completes FTM-27 planned for December 2016.
- ASD-15 demonstrated Aegis BMD 3.6.3 retention of Aegis BMD 3.6.1 midcourse engagement capabilities against non-separating SRBMs, when an Aegis BMD 3.6.3 ship detected, tracked, and intercepted an SRBM using an SM-3 Block IA guided missile. ASD-15 also demonstrated that Aegis BMD can interoperate with NATO defenses and exchange air and ballistic missile message information across operational communication architectures during cruise missile and ballistic missile engagements. The MDA further demonstrated Aegis BMD 3.6.3 capabilities in FY16 during SM CTV-01a and -02, when an Aegis BMD 3.6.3 destroyer fired SM-3 Block IB TU missiles for the first time. Aegis BMD 3.6.3 is the only variant of the Aegis BMD 3.6 system that can fire SM-3 Block IB missiles.
- The MDA continues to utilize Aegis BMD assets and HWIL representations in ground test events and warfighter simulation exercises during operational flight test campaigns (e.g. FTO-02), which has helped to refine tactics, techniques, and procedures (TTPs) and overall interoperability of the system with the BMDS. However, the test events routinely demonstrated that inter-element coordination and interoperability need improvement. The tests highlighted multiple classified suitability and effectiveness shortfalls.
- The MDA continues to participate in tests of opportunity like the Pacific Dragon exercise, which provide a venue to explore interoperability between Aegis BMD assets and foreign ballistic missile defense assets. In Pacific Dragon, Aegis BMD

successfully exchanged data with Allied units from Japan and the Republic of Korea.
- Following the integration testing failure of an SM-3 Block IIA flight test round, the MDA initiated a Failure Investigation Team process and developed a fault tree. The flight test round will be disassembled and will undergo further analysis to determine the root cause of the failure.
- Cybersecurity testing results from the Adversarial Assessment of the Aegis Ashore Missile Defense Facility in Romania will be included in DOT&E's classified 2016 BMDS Annual Report to Congress.
- Testing has uncovered a number of classified survivability problems, which will be discussed in DOT&E's classified 2016 BMDS Annual Report to Congress.

Recommendations
- Status of Previous Recommendations. The program:
  1. Addressed the first recommendation from FY13 to conduct flight testing of the Aegis BMD 4.0 remote engagement authorized capability against an MRBM or IRBM target using SM-3 Block IB guided missiles, when it conducted FTO-02 Events 1a and 2a using Aegis Baseline 9.1 (BMD 5.0 Capability Upgrade) firing assets.
  2. Partially addressed the second recommendation from FY13, to conduct operationally realistic testing that exercises Aegis BMD 4.0's improved engagement coordination with THAAD and Patriot, when it conducted FTO-02 Event 2a using an Aegis Baseline 9.C1 destroyer and THAAD firing assets. This flight test did not include Patriot.
  3. Addressed the second recommendation from FY14, to determine the appropriate LRS&T TTPs for the transmission and receipt of Aegis BMD 4.0 track data for GMD use. GTI-06 Part 3 (FY15), GTI-06 Part 2, and GTD-06 Part 2 demonstrated that GMD can use data provided by Aegis BMD 4.0.3.
  4. Partially addressed the third recommendation from FY14, to ensure that sufficient flight testing of the Aegis Baseline 9.C1 system is conducted to allow for verification, validation, and accreditation (VV&A) of the M&S suite to cover the full design to Aegis BMD battlespace. Flight testing conducted in FY15 and early FY16 provided additional VV&A data, but the BMDS OTA has not yet accredited the high fidelity M&S suite.
  5. Addressed the fourth recommendation from FY14, to conduct sufficient ground and flight testing of the redesigned insulation components in the SM-3 Block IB TSRM nozzle to prove the new design works under the most stressing operational flight conditions. This occurred when the program completed a series of six design verification and qualification ground test firings and the SM CTV-01a and CTV-02 flight tests.
  6. Addressed the first recommendation from FY15, to use an industry-led FRB process to identify the root cause of low cold gas pressure anomalies observed in lot acceptance testing of the SM-3 Block IB CGR, and determine the appropriate corrective actions needed to ensure proper functioning. The FRB process determined that changes to the CGR C-seal's spring dimensions, additional inspections, and an enhanced acceptance test process were required and a follow-on study is underway to investigate the possibility of re-designing the CGR seal.
  7. Has not addressed the second recommendation from FY15, to conduct stressing simultaneous air and ballistic missile defense engagements with the Aegis Baseline 9.C1 system operating in IAMD radar priority mode, with multiple ballistic missiles and anti-ship cruise missile threats being simultaneously engaged.
  8. Has not addressed the third recommendation from FY15, to perform high-fidelity M&S analysis over the expected Aegis Ashore engagement battlespace for EPAA Phase 2 to allow for a broad quantitative evaluation of engagement capability. The MDA plans to complete the high-fidelity M&S analysis in FY18.
- FY16 Recommendations. The MDA should:
  1. Conduct high-fidelity M&S runs-for-the-record for the Aegis Baseline 9.2 system (Aegis BMD 5.1) to assess performance across the expected engagement battlespace in all Combatant Commands' Areas of Responsibility and develop an appropriate M&S VV&A plan to support that effort.
  2. Conduct a live-flight test demonstration of a fully remote engagement.
  3. Include BMDS OTA RMA&S data collectors in all flight test missions to improve the accuracy and statistical confidence of future suitability assessments.

Ground-based Midcourse Defense (GMD)

Executive Summary

- Previous assessments of the Ground-based Midcourse Defense (GMD) system remain unchanged. GMD has demonstrated a limited capability to defend the U.S. Homeland from small numbers of simple intermediate-range or intercontinental ballistic missile threats launched from North Korea or Iran. DOT&E cannot quantitatively assess GMD performance due to lack of ground tests supported by accredited modeling and simulation (M&S).
- The Missile Defense Agency (MDA) demonstrated Alternate Divert Thrusters (ADTs) for future Ground-Based Interceptors (GBIs) during the Ground-based Midcourse Controlled Test Vehicle-02+ (GM CTV-02+) flight test. Extensive phenomenology data were also collected for discrimination improvement.
- The MDA executed the Ground Test, Integrated-06 (GTI-06) Part 2 and Ground Test, Distributed-06 (GTD-06) Part 2 ground tests assessing Ballistic Missile Defense System (BMDS)-level strategic and theater/regional capabilities in U.S. Northern Command's (USNORTHCOM's) and U.S. Pacific Command's (USPACOM's) areas of responsibility. The MDA demonstrated BMDS interoperability and updated discrimination capability. The lack of accreditation of models and simulation for performance assessment limited using these data for quantitative GMD evaluation.
- The MDA emplaced six GBIs with upgraded Capability Enhancement-II (CE-II) Exo-atmospheric Kill Vehicles (EKVs) and Configuration 1 boosters.
- The MDA declared the In-Flight Interceptor Communication System Data Terminal (IDT) at Fort Drum, New York, available and USNORTHCOM accepted the site in December 2015. USNORTHCOM opened the site for operational use in July 2016.

System

- GMD counters intermediate range and intercontinental ballistic missile threats to the U.S. Homeland. GMD consists of:
  - GBIs at Fort Greely, Alaska, and Vandenberg AFB, California
  - GMD ground system, including GMD Fire Control (GFC) nodes at Schriever AFB, Colorado, and Fort Greely, Alaska; Command Launch Equipment (CLE) at Vandenberg AFB, California, and Fort Greely, Alaska; and IDTs at Vandenberg AFB, California, Fort Greely, Alaska, and Eareckson Air Station, Alaska
  - 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 Aegis Ballistic Missile Defense (BMD) ships; North American Aerospace Defense/USNORTHCOM Command Center; Command and Control, Battle Management, and Communications (C2BMC) system at Schriever AFB, Colorado, and Pearl Harbor-Hickman AFB, Hawaii; Space-Based Infrared System (SBIRS) at Buckley AFB, Colorado; and AN/ TPY 2 (Forward Based Mode (FBM)) radars at Japan Air Self Defense Force bases in Shariki and Kyoga-Misaki, Japan

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 intermediate range and intercontinental ballistic missile attacks using the GBI 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: Orbital ATK, Missile Defense Systems – Chandler, Arizona
- EKV: 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 conducted a non-intercept GM CTV-02+ flight test in January 2016. The MDA designed this test to demonstrate ADTs for future GMD interceptors and collect data for use in developing discrimination improvements.
- The MDA executed the GTI-06 Part 2 and GTD-06 Part 2 ground tests in May and September 2016, respectively. The MDA assessed BMDS-level strategic and theater/regional capabilities in USNORTHCOM's and USPACOM's areas of responsibility in integrated (i.e., GTI) and distributed (i.e., GTD) test environments. GTD ground tests use live operational networks, whereas GTI ground tests use laboratory-based networks. The MDA used hardware and software representations of the GMD system; SBIRS; Upgraded Early Warning Radars (UEWRs); C2BMC; an AN/TPY-2 (FBM) radar; an Aegis AN/SPY-1 radar in its long-range surveillance and track mode; and the Sea-Based X-band (SBX) radar. In these tests, the MDA exercised the new GFC software version 6B3.1.
- The MDA emplaced six GBIs with upgraded CE-II EKVs and Configuration 1 boosters.
- The MDA completed the Redesigned Kill Vehicle System Requirements Review in November 2015.
- The MDA declared the IDT at Fort Drum, New York, available for use and USNORTHCOM accepted the site in December 2015. USNORTHCOM opened the site for operational use in July 2016.

Assessment

- Previous assessments of GMD remain unchanged. GMD demonstrates a limited capability to defend the U.S. Homeland from small numbers of simple intermediate-range or intercontinental ballistic missile threats launched from North Korea or Iran.
  - The reliability and availability of the operational GBIs are low, and the MDA continues to discover new failure modes during testing.
  - GMD survivability data are limited and come primarily from facility testing and component-level testing, but known survivability issues exist. Few cybersecurity assessments have been performed to-date.
  - Radar availability shortfalls, the details of which are classified, affect GMD suitability.
- During GM CTV-02+, the MDA demonstrated the new CE-II EKV ADTs in an operationally realistic environment. The ADTs turned on and off as commanded and performed nominally. One controller circuit board associated with one of the ADTs experienced a short and did not command its ADT to turn on for the later part of the test. This controller circuit board is contained within the GBI guidance module and is not considered part of the ADT subsystem. An anomaly review board determined that foreign object damage was the most likely cause of the controller circuit board failure. The MDA collected extensive phenomenology data for discrimination improvement.
- In GTI-06 Part 2 and GTD-06 Part 2 ground tests, the MDA demonstrated interoperability of the GMD GFC software version 6B3.1 with the SBIRS, UEWRs, C2BMC, AN/TPY-2 (FBM) radar, Aegis BMD AN/SPY-1 radar in its long-range surveillance and track mode, and SBX radar. Discrimination improvements were ground tested as part of the BMDS Capability Increment 3 delivery. A number of GMD software upgrades were ground tested, including the discrimination logic, SBX tasking, and GFC salvo logic. These data support the evaluation of GMD system performance against an expanded strategic threat set.
- Quantitative evaluation of GMD performance will require extensive ground testing with accredited M&S. Data needed to accredit GMD threat, radar, and environmental M&S are either limited or lacking. GMD intercept flight tests have not adequately spanned the operational battlespace to provide data for validation, and subsequent accreditation, of key M&S.

Recommendations

- Status of Previous Recommendations. The MDA has completed previous recommendations with the exception of one FY14 and one FY15 recommendation:
  1. The MDA has initiated, but not completed, the FY14 recommendation to extend the principles and recommendations contained in the Independent Expert Panel assessment report on the GBI fleet to all Homeland Defense components of the BMDS.
  2. The MDA should determine any additional sensor capability requirements for an effective Defense of Hawaii capability (FY15 recommendation). The MDA has initiated analysis of the needed capability, but has not completed this study.
- FY16 Recommendations. The MDA should:
  1. Improve and demonstrate the reliability and availability of the operational GBIs.
  2. Increase emphasis on GMD survivability testing, including cybersecurity. Tests, demonstrations, and exercises to acquire additional survivability data should be planned for inclusion in the BMDS Integrated Master Test Plan.
  3. Accelerate its effort to accredit M&S for performance assessment supporting GMD OT&E, including Redesigned Kill Vehicle performance and lethality.

Terminal High-Altitude Area Defense (THAAD)

Executive Summary

- The Terminal High-Altitude Area Defense (THAAD) program participated in one Ballistic Missile Defense System (BMDS) operational flight test in November 2015, in accordance with the DOT&E-approved Integrated Master Test Plan, intercepting two ballistic missile targets.
- THAAD participated in four BMDS ground tests, providing information on THAAD interoperability and functionality within the BMDS for various regional/theater scenarios.
- The THAAD program conducted a Cybersecurity Red Team Assessment in March 2016 and a Limited User Test of the Table Top Trainer in June 2016.
- The THAAD program continued work on achieving a Full Materiel Release of the first two THAAD batteries, which achieved Conditional Materiel Release in February 2012.

System

- THAAD is intended to complement the lower-tier Patriot system and the upper-tier Aegis Ballistic Missile Defense (BMD); it can 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 accept target cues for acquisition from Aegis BMD, from other regional sensors, and through command and control systems.

Mission

U.S. Strategic Command deploys THAAD to protect critical assets worldwide. U.S. Northern Command, U.S. Pacific Command (USPACOM), U.S. European Command (USEUCOM), and U.S. Central Command (USCENTCOM) will use THAAD to intercept short- to intermediate-range ballistic missile (SRBM/IRBM) threats in their areas of responsibility.

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 Missile Defense Agency (MDA) conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- The MDA conducted system-level Flight Test Operational-02 (FTO-02) Event 2a in November 2015 at Wake Island and the broad ocean area surrounding it. This test used THAAD version 2.7 software and a Lot 4 and Fire Unit Fielded interceptor. THAAD completed near-simultaneous engagements of two targets: a complex SRBM and a medium-range ballistic missile (MRBM). The engagement of the MRBM occurred following the failure of an Aegis BMD Standard Missile-3 Block IB guided missile to intercept the target. An AN/TPY-2 (Forward-Based Mode) radar, in addition to the THAAD (Terminal Mode) radar, also tracked the targets. The MDA initially attempted to conduct this test in October 2015 as FTO-02 Event 2; however, due to a THAAD target malfunction, the event was a "No Test."
- THAAD provided hardware-in-the-loop representations for four BMDS ground tests that provided information on THAAD interoperability and functionality in various regional/theater scenarios.
  - Ground Test Distributed-06 (GTD-06) Part 1 in October 2015 examined defense of USEUCOM and USCENTCOM scenarios, using THAAD version 2.7 software.

  - Ground Test Integrated-06 (GTI-06) Part 2 in April 2016 examined defense of USPACOM and Homeland defense scenarios, using THAAD version 2.8 software.
  - GTI-Israel-16 in June 2016 studied interoperability between the BMDS and the Arrow Weapon System for maintaining shared situational awareness, using THAAD version 2.7 software.
  - GTD-06 Part 2 in September 2016 again examined defense of USPACOM and Homeland defense scenarios, using THAAD version 2.8 software.
- The THAAD program also conducted several smaller test events including a Cybersecurity Red Team Assessment in March 2016 and a Limited User Test of the Table Top Trainer in June 2016.

Assessment

- FTO-02 Event 2a demonstrated that THAAD capabilities against theater and regional threats increased during FY16. THAAD Lot 4 and Fire Unit Fielded interceptors, for the first time, intercepted one complex SRBM and one MRBM threat-representative ballistic missile target while Aegis BMD simultaneously engaged an air-breathing threat. In addition to testing against new threat characteristics, the MDA successfully demonstrated the THAAD radar advanced algorithms for the first time during this test. The test event also demonstrated that recent obsolescence redesigns of hardware and software, which were fully integrated for the first time in this test, caused unintended problems. The THAAD Project Office should further study these design changes to minimize their negative effects.
- Although THAAD has been deployed to Guam since 2013, THAAD has not yet demonstrated capability against IRBM threats in a flight test. The MDA will demonstrate this capability in FY17 during Flight Test THAAD-18 (FTT-18). This test, in addition to previous flight testing and FTT-15 (also planned for FY17), will demonstrate several key capabilities against longer range threats that the MDA should further explore using end-to-end modeling and simulation.
- During GTD-06 Part 1, GTI-06 Part 2, and GTD-06 Part 2, the MDA demonstrated aspects of THAAD functionality in different theater scenarios. The BMDS Operational Test Agency (OTA) also reported several findings, consistent with findings from earlier ground tests that affect THAAD interoperability, track management, and radar functions.
- Although analysis is still ongoing, data from FTO-02 Event 2 and Event 2a indicate that overall reliability failure rates were higher than those observed during the FY15 Reliability Growth Test. The launcher, particularly its 3-kilowatt generator, continued to experience failures.
- Problems previously discovered during testing, if not corrected, could adversely affect THAAD effectiveness, suitability, or survivability. These problems, the details of which can be found in DOT&E's classified 2015 Assessment of the BMDS, include:
  - Training and documentation are still immature. Training courses and aids are still in development, and errors and omissions in the technical manuals continue to be found during testing.
  - Environmental testing revealed some deficiencies which have not been corrected.
  - Some specific aspects of discrimination and classification need improvement.
  - Testing revealed some survivability and cybersecurity shortfalls, which are still in the process of being fixed and assessed.
- The THAAD program continued work on achieving a Full Materiel Release of the first two THAAD batteries, which achieved Conditional Materiel Release in February 2012. The THAAD Project Office continued to address the 19 open conditions that need to be resolved before the Army will grant a Full Materiel Release. The THAAD program will continue to test and fix the open conditions through FY19. Of the original 39 conditions, the THAAD Project Office closed 20 conditions in FY12-15 and 1 condition to "provide a capability to electronically transfer battle plans" in FY16.
- Work also continues on additional materiel release conditions for follow-on THAAD software versions 1.3.1, 1.4.0, and 2.7.0 (Configuration 2).

Recommendations

- Status of Previous Recommendations. DOT&E's classified February 2012 THAAD and AN/TPY-2 Radar OT&E and LFT&E report contained 7 recommendations in addition to the 39 Conditional Materiel Release conditions. The MDA should continue to address the two remaining classified recommendations (Effectiveness #2 and Effectiveness #5) and the two remaining unclassified recommendations. The MDA and the Army should:
  1. Implement equipment redesigns and modifications identified during natural environment testing to prevent problems seen in testing (Suitability #11). Some of these deficiencies have been addressed by hardware modifications included in THAAD Configuration 2. Conducting additional ground testing with Configuration 2 (a standing FY14 recommendation) would also provide data to address this recommendation.
  2. Conduct electronic warfare testing and analysis (Survivability #3). The MDA conducted preliminary testing during FY13, but additional testing is required.
  3. The program partially addressed the FY14 recommendation to conduct thorough end-to-end testing of the THAAD Configuration 2 that incorporates considerable obsolescence redesigns of hardware and software. The MDA should continue to plan to rigorously ground test the THAAD system to verify that these changes can withstand the range of environments and conditions required.
  4. The program has begun to address the FY15 recommendation that the MDA should prioritize flight and ground testing that involves THAAD and Patriot engagement coordination, to determine if the information passed between THAAD and Patriot does not disrupt organic intercept capabilities and can contribute to reduced

interceptor wastage and threat missile leakage. The MDA and Army are considering a combined THAAD and Patriot test in 2018.

- FY16 Recommendation.
  1. The MDA and BMDS OTA should plan to conduct high-fidelity modeling and simulation runs against longer range threats following the FTT-18 and FTT-15 flight test campaign, to include endgame and lethality analyses for these tests.

Live Fire Test and Evaluation

Live Fire Test and Evaluation

Live Fire Test and Evaluation (LFT&E)

INTRODUCTION

- In FY16, DOT&E executed LFT&E oversight for 132 acquisition programs, 3 LFT&E investment programs (Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME), Joint Aircraft Survivability Program (JASP), and Joint Live Fire (JLF)), and 3 special interest programs (Warrior Injury Assessment Manikin (WIAMan), Home Made Explosives (HME), and Small Boat Shooters' Working Group).
- In support of a range of acquisition decisions and activities, DOT&E published two LFT&E reports and two combined OT&E and LFT&E reports. The reports include recommendations to the Services to further improve the survivability or lethality of the subject systems for a range of operationally relevant scenarios in existing and expected combat environments.

LFT&E Investment Programs Summary

- The Joint Technical Coordinating Group for Munitions Effectiveness:
  - Enhanced the capabilities of its two major products – the Joint Munitions Effectiveness Manual (JMEM) Weaponeering System (JWS) and Joint-Anti-air Combat Effectiveness (J-ACE) – to meet new Combatant Commands' requirements. These efforts equipped the Combatant Commands with added operational targeting, weaponeering data and solutions, and collateral damage estimation capability in direct support of new operations, mission planning, and training. This includes the Digital Precision Strike Suite (DPSS) Collateral Damage Estimation (DCiDE) tool and Digital Imagery Exploitation Engine (DIEE), as well as standalone resources such as the Probability of kill (Pk) Lookup Tools, Collateral Damage Estimation (CDE) tables, and munitions weaponeering guides. These solutions rapidly provide Service members with authoritative weapons effectiveness data when needed, as well as seamless end-to-end strike package development during planning (i.e., weaponeering, collateral damage estimation, and precision point mensuration).
  - Supported the air warfare community – in particular the Naval Strike and Air Warfare Center and the Air Force Weapons School – with its J-ACE tool to develop tactics, techniques, and procedures manuals for air superiority applications and to perform post-shot analysis following exercise and training missions (e.g., Red Flag FY16 exercises at Nellis Test and Training Range, Nellis AFB, Nevada).
  - Worked with DOD, Joint, and Service planners to support force-on-force modeling, mission area analysis, requirements studies, and weapon procurement planning such as the Army's Total Army Analysis, the Air Force's Nonnuclear Consumables Annual Analysis, the Navy's Naval Munitions Requirements Process assessment, and annual Army Capabilities Integration Center simulation exercises.
  - Supported the acquisition community in performance assessments, analysis of alternatives (AoA), and survivability enhancement studies such as the Army's Echelon Above Brigade M113 Family of Vehicles Replacement AoA. This AoA leveraged standard JTCG/ME analytical tools, such as the Joint Mean Area of Effectiveness Model.
  - Developed a preliminary non-kinetic JMEM capability, to include a prototype Cyber JMEM. This provided the analytical foundation for standard processes and data to enable effectiveness estimates for cyber, electronic attack, and directed energy capabilities.
  - Continued work on JWS versions releasable to the United Kingdom, Canada, Australia, Republic of Korea, and other coalition partners for planning, operational weaponeering and collateral damage estimates, support of training and tactics development, and support of force-level analyses.
- JASP funded 47 multi-year projects addressing aircraft survivability enhancement technologies and aircraft survivability evaluation tools. In FY16, JASP made progress in improving:
  - The ability of aircraft to counter near-peer and second-tier threat by 1) developing and testing countermeasure techniques, which included improving both the fidelity of countermeasure simulations and the collection of flight test data on a new chaff design; 2) updating survivability tools such as the Enhanced Surface-to-Air Missile Simulation (ESAMS) with the latest threat types and countermeasures; and 3) investigating new countermeasure concepts for emerging threats.
  - Aircraft force protection by 1) developing improved hostile fire detection; 2) investigating anti rocket-propelled grenade warhead concepts to improve rotorcraft survivability; 3) investigating aircraft hardening against high energy lasers; and 4) improving the accuracy and confidence of vulnerability assessment tools.
  - Aircraft survivability to fires, the primary threat-induced aircraft vulnerability.
- JLF supplemented LFT&E of fielded systems, addressed operational commander's needs, and characterized new survivability and lethality effects of fielded systems either: 1) in response to the exposure of U.S. systems to new threats; 2) as a result of systems being used in new, unanticipated

ways; or 3) as a result of systems being operated in new environments. Specifically, JLF:
- Assessed the effect of fielded system design changes on survivability (e.g., CV-22 add-on armor)
- Assessed weapon lethality of a new ammunition mix for A-10 aircraft as well as behind armor debris of an anti-tank penetrator mine
- Improved the accuracy and fidelity of weapon data used as part of mission planning in order to estimate weapon effectiveness and effects with higher confidence (e.g., improved collateral damage estimates)
- Advanced live fire test methodology to improve collection of fragment velocity and spatial distribution data during arena testing
- Supported the development and improvement of modeling and simulation tools that contribute to survivability and lethality evaluations (e.g., new data to support improvements in predicting weapons effects against aircraft, vehicles, and military structures)

LFT&E Special Interest Programs Summary

- The WIAMan project, an Army-led effort, made significant progress in biomechanics testing and anthropomorphic test device development to design a biofidelic prototype for assessing injuries to vehicle occupants during underbody blast. However, the Army has not programmed the funding for this project in FY18 or beyond, which could adversely affect the delivery of this capability.
- HME-C investigated and tested the repeatability of HME surrogate effects relative to those of TNT and the effects of soil condition and IED emplacement on HME threat performance. DOT&E used the test data to develop LFT&E policy for employing buried underbody blast surrogates that mitigates soil-induced test data variability. This included a new, engineered soil standard for use with underbody blast testing.
- The Small Boat Shooters' Working Group continues to synchronize live fire and other operational test approaches against this growing threat class, which operates in littoral waters.
- DOT&E briefed Congressional staff on helicopter seating system improvements per the House Report to accompany the National Defense Authorization Act for FY16. DOT&E determined that seating system improvements would improve force protection in some crash conditions, but addressing controlled flight into terrain and collision threat avoidance with near-term technology solutions would provide a higher payoff by mitigating leading cause of fatality in helicopter mishap and combat-induced crashes.

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 those platforms or munitions get deployed or enter full-rate production. In FY16, DOT&E executed LFT&E oversight for 132 acquisition programs. Of those, 17 operated under the waiver provision of U.S. Code, Title 10, Section 2366, by executing an approved alternative LFT&E strategy in lieu of full-up system-level testing. DOT&E published two LFT&E reports and two combined OT&E and LFT&E reports in FY16 (see Table 1).

LFT&E Reports	Combined OT&E and LFT&E Reports
Multiple Launch Rocket System (MLRS) M270A1 Launcher Improved Armored Cab (IAC)*	Mine Resistant Ambush Protected (MRAP) Family of Vehicles MaxxPro Long Wheel Base (LWB) Ambulance with Independent Suspension System (ISS) and MaxxPro Survivability Upgrade
Soldier Protection System (SPS) Torso and Extremities Protection (TEP)*	M829A4 120 mm Armor-Piercing, Fin Stabilized, Discarding Sabot – Tracer (APFSDS T)*

* Reports sent to Congress.

- Three reports supported Full-Rate Production decisions:
  - "Multiple Launch Rocket System (MLRS) M270A1 Launcher Improved Armored Cab (IAC)" reported on the protection that the IAC provides to the MLRS crew. The report included three recommendations to improve MLRS crew survivability.
  - "Soldier Protection System (SPS) Torso and Extremities Protection (TEP)," regarding a single soft armor system to replace the Army's Improved Outer Tactical Vest, reported on the protection the TEP provides soldiers against small-arms and fragmenting threats.
  - "M829A4 120 mm Armor-Piercing, Fin Stabilized, Discarding Sabot – Tracer (APFSDS-T)" reported on the lethality of the M829A4 120 mm APFSDS-T. This report included four recommendations to improve operational effectiveness and lethality, and one recommendation to improve test and evaluation practices in future similar lethality test programs. DOT&E continues to observe the follow-on tests and will report on the accuracy problems with the M829A4 service rounds that were observed during the User Beta Test for Version 4.6 of the Abrams software.
- One report provided a system survivability evaluation for use by the Service and Program Office:
  - "Mine Resistant Ambush Protected (MRAP) Family of Vehicles MaxxPro Long Wheel Base (LWB) Ambulance

with Independent Suspension System (ISS) and MaxxPro Survivability Upgrade" reported on the protection against underbody blasts afforded to occupants of the MaxxPro LWB Ambulance MRAP vehicle (also known as the M1266A1). LFT&E made five recommendations to further reduce the underbody vulnerability of the M1266A1 and its crew.
- DOT&E published one classified Special Report, "Market Survey of Active Protection Systems," in response to Senate Committee Report 114-49 (2015).
- DOT&E provided the classified "Assessment of the Performance and Effectiveness Characteristics of the 5.56 mm M855A1 and Mk318 Mod 1 Rounds" to the Under Secretary of Defense for Acquisition, Technology and Logistics in response to Senate Committee Report 114-49 (2015).

LFT&E INVESTMENT PROGRAMS

JOINT TECHNICAL COORDINATING GROUP FOR MUNITIONS EFFECTIVENESS

The Joint Technical Coordinating Group for Munitions Effectiveness (JTCG/ME) continued to update and develop weapons effectiveness and target vulnerability data, standards, and methodologies that are crucial for developing theater commanders' force employment options as well as the resulting execution tasking orders to tactical units. The principal products of the JTCG/ME are the Joint Munitions Effectiveness Manuals (JMEMs). JMEMs enable users to plan the mission adequately by determining the effectiveness of weapon systems against a specified target for a range of weapon delivery modes. JMEMs include: detailed data on the physical characteristics and performance of weapons and weapon systems; descriptions of the mathematical methodologies that employ these data to generate effectiveness estimates; software that permits users to calculate effectiveness estimates; and pre-calculated weapon effectiveness estimates. This information enables a standardized comparison of weapon effectiveness across all Service communities. JMEM products include existing software product lines, such as the JMEM Weaponeering System (JWS) and the Joint Anti-air Combat Effectiveness. Future product lines will include the Joint Non-Kinetic Effectiveness capability. Specialized solutions are driven by the needs of Combatant Commands and lessons learned from current operations. Such solutions include Probability of kill (Pk) Lookup Tools; Collateral Damage Estimation (CDE) tables; munitions weaponeering guides; and enablers for more efficient targeteering (e.g., the Digital Precision Strike Suite (DPSS) Collateral Damage Estimation (DCiDE) tool and the Digital Imagery Exploitation Engine (DIEE)).

Joint Munitions Effectiveness Manual Weaponeering System

- JWS is the DOD source for air-to-surface and surface-to-surface weaponeering, munitions, and target information used daily by the U.S. Central Command (USCENTCOM), U.S. Special Operations Command (USSOCOM), and U.S. Africa Command (USAFRICOM) in the deliberate planning process directly supporting Joint Publication 3-60, "Joint Targeting."
- JWS enables Combatant Commands to prosecute their target sets. JWS incorporates accredited methodologies, certified munition characteristics, delivery accuracy, target vulnerability data, and numerous user aids to support the operational use of JWS to predict weapons effectiveness for fielded weapons and delivery systems.
- JTCG/ME deployed JWS v2.2 in FY16. JWS v2.2 included a total of 220 methodology, functionality, weapons/warheads/fuzes, and target updates. JWS v2.2 included initial connectivity with the DCiDE tool (Figure 1), as well as updates to the Fast Integrated Structural Tool (FIST) (containing building types and a quasi-static blast capability). The connectivity with DCiDE improves both speed and throughput of data.
- JTCG/ME continued to facilitate coalition interoperability. It is currently completing several JWS version releases to key coalition partners in support of current operations under Foreign Military Sales agreements. This capability improves the effectiveness of U.S. fires and targeting personnel working in combined environments.
- JTCG/ME continued development on JWS v2.3 in FY16; fielding is scheduled in 1QFY17. JWS v2.3 will include enhanced data sets and capabilities with a focus on connectivity to other targeting and mission planning capabilities for improved estimates and more seamless planning. More specifically, JWS v2.3 enhanced capabilities include:
  - Connectivity to the Modernized Integrated Database, Joint Targeting Toolbox, and DIEE (currently in finalization for separate fielding). This will permit automatic transfer of data and information between these planning tools.
  - Multiple updates to FIST to incorporate connectivity with DIEE and the Joint Targeting Toolbox, along with updated target options (such as building type, material, and features). These updates will improve weapons effectiveness estimates.
  - Improvements to the Ship Weaponeering Estimation Tool that optimize database use and improve the user interface.
  - Inclusion of a weapon delivery accuracy module along with updates for the Gunship Delivery Accuracy Program, Rotary Wing Delivery Accuracy Program, and Joint Delivery Accuracy Program. This will provide enhanced calculations for F-35 gun munitions and C-130 gunship effectiveness in JWS.

- The Dilution of Precision Tool, which improves the predicted accuracy of GPS/Inertial Navigation System weapons from satellite time and space calculations.
- The Target Location Error Tool, which enables a single JWS tool to provide Target Location Error from airborne and ground based sensors.
- Updates on weapons delivery accuracy and characterization data for multiple systems (e.g. M982 Excalibur satellite-guided artillery shell, M395 Precision Guided Mortar Munition, AGM-65E2/L Maverick air-to-ground tactical missile, M1061 60 millimeter mortar, M120 Towed/M121 120 millimeter mortar, BLU-110 general purpose bomb, AGM-114 Hellfire variant, M31 Guided Multiple Launch Rocket System, M1156 Precision Guidance Kit, and numerous small arms).
- Fifty target vulnerability data sets across ground, aircraft, small boats, ships, and submarines, as well as 352 updated image Quickfacts, which provide the Weaponeer quick-reference characteristics of systems for analysis.

• JTCG/ME will continue development of JWS v2.4 during FY17 to provide enhanced data capabilities and connectivity.

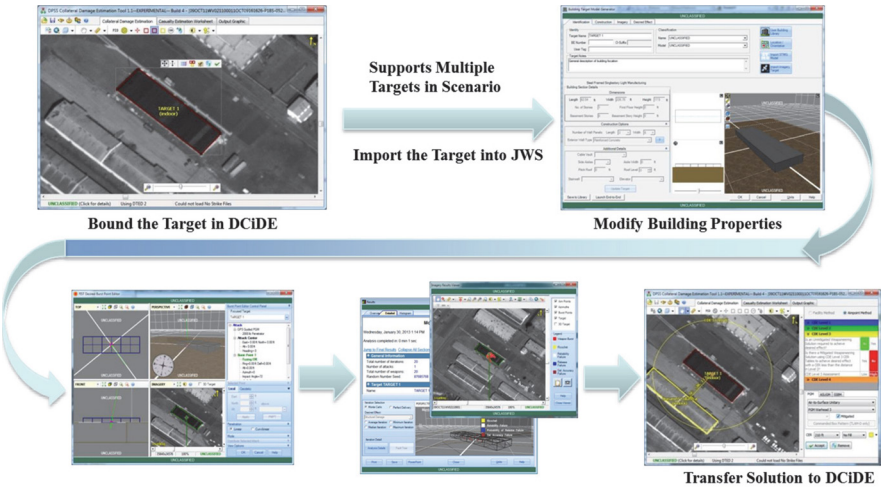


Figure 1. Connectivity between Weaponeering and Collateral Damage Assessment Enables Combatant Commanders to More Rapidly Prosecute Targets

In FY16, JTCG/ME released DCiDE v2.0 to support the Chairman of the Joint Chiefs of Staff Instruction 3160.01B, "No-Strike and the Collateral Damage Estimation (CDE) Methodology." This release provides the latest approved Collateral Effect Radii (CER) and CDE data as of FY16.

- The DCiDE tool is an accredited and automated CDE tool that expedites and simplifies the CDE process. As such, it is critical to the Warfighters' ability to meet urgent operational needs. DCiDE is the only automated CDE tool authorized for use in the USCENTCOM and USAFRICOM Areas of Responsibility Operation (AORs). The JTCG/ME CDE tables are used in every planned kinetic strike in all AORs to meet Commanders' intent and to minimize civilian casualties. DOT&E continues to receive positive feedback on the use of the CER values, collected as part of the Joint Live Fire efforts, as a critical enabler in support of munitions employment against HVTs.
- JTCG/ME updated the accredited CER Reference Tables for selected air-to-surface and surface-to-surface weapons, which are the basic data that support the CDE methodology. Changes included additions for airburst munitions, nomenclature changes, and additional updates for newly fielded/updated systems (e.g., HELLFIRE family). JTCG/ME also developed and accredited the Collateral Effects Library tool in support of advanced CDE mitigation techniques.

• JTCG/ME is working with the Navy's DPSS program based at the Naval Air Weapons Center – Weapons Division in China Lake, California, to provide the Digital Imagery Exploitation Engine (DIEE). DIEE is an enterprise targeting solution that provides both seamless planning with the various planning tools and a direct linkage to mission planning systems in operational units.

- DIEE is a self-contained Government off-the-shelf (GOTS) computer system with internal software. It can derive mensurated coordinates from the Digital Point Positioning Database and will combine applications so that targeting or planning personnel can develop strike plans where the weaponeering, collateral damage estimation, and precision point mensuration conducted during planning is both seamless and linked to mission planning systems for target execution. JTCG/ME began fielding DIEE at the beginning of FY17, and both USCENTCOM and USARFICOM have already committed to using DIEE as their primary targeting planning tool.

Joint-Anti-air Combat Effectiveness

• Joint-Anti-air Combat Effectiveness (J-ACE) provides authoritative air-to-air and surface-to-air weapons effectiveness information, and serves as the primary tool used by the Air Force and Navy to underpin air combat tactics, technics, and procedures development. J-ACE is the umbrella program that includes both the Joint Anti-air Model (JAAM) and Endgame Manager, which provides a full kill chain end-to-end capability. Other users include National Test and Training Ranges for air to air and surface to air shot validation and various members of the analytical community for air combat studies and planning. The U.S. Strategic Command (USSTRATCOM) leverages J-ACE capabilities to support route planning for the execution of strike packages. JAAM supports operational squadrons' mission debrief tools, such as the Personal Computer Debriefing System and several others.

• JTCG/ME is releasing J-ACE v5.3, which will extend and update data sets for missile and aircraft target aero performance, anti-air missile lethality, and air target vulnerability. These data include over 40 air-to-air missile models (blue and threat), over 50 surface-to-air missile models (threat), and approximately 40 aircraft models (blue and threat). New capabilities include:

  - The Hybrid Integration and Visualization Engine computer architecture interface
  - The BLUEMAX6 (six degrees of freedom aero performance) model for increased aircraft aero performance modeling, with Hands-on Throttle and Stick allowing for actual flight control of the aircraft
  - Increased countermeasure capabilities leveraging ESAMS
  - Factoring in the effect of weapon system reliability when calculating the probability of a successful engagement
  - The ability to estimate countermeasure effectiveness
- J-ACE v5.4 is in development to field and add Browse descriptive material to support new weapons in the JAAM and Endgame Manager. The fielding of J-ACE v5.4 in 2017 will facilitate greater connectivity for outbrief capability by units, target detection estimation, counter air defense prediction capability, and enhanced architecture allowing future version growth and compatibility.

Joint Non-Kinetic Effectiveness – Cyber/Electronic Attack and Directed Energy JMEMs

- JTCG/ME is continuing the development of non-kinetic weaponeering tools and methodologies. Joint Non Kinetic Effectiveness is intended to be the single source for operational Warfighters, analysts, targeteers, and planners to analyze offensive cyber capabilities, electronic attack weapons, and directed energy effectiveness.
- In conjunction with DOT&E and the Air Force's 363rd Intelligence, Surveillance, and Reconnaissance Group, the JTCG/ME continued development of a JMEM process for cyberspace operations, electronic attack, and directed energy. FY16 efforts centered on developing the foundational elements for JMEM production, including weapons characteristics, target vulnerability, and effects estimation tools (e.g., U.S. Cyber Command's Cyber Capabilities Registry, Electronic Warfare/Cyber Critical Elements/Weaponeering Guides, and Directed Energy Effectiveness Lookup Tables). These efforts culminated in an initial Cyber JMEM prototype for user review and set the foundation for a full joint non-kinetic suite that includes other non-kinetic effects.

Operational Users Working Group

- The Operational Users Working Group is a critical venue for receiving direct user feedback and development of future requirements from the operational community in regards to needed software enhancements and capabilities to support air-to-surface, surface-to-surface, anti-air, and non-kinetic engagements. Examples of user requirements include the ability to release weaponeering information to coalition partners; connectivity between tools and mission planning systems; current weapon and fuze information; updated training materials; quick weaponeering guides; graphical user interface enhancements; and improved blast/fragment methodologies in support of small precision munitions.
- JTCG/ME continued to chair Operational Users Working Groups with representatives from USCENTCOM, USAFRICOM, USSTRATCOM, U.S. Pacific Command, USSOCOM, the Services, the Defense Intelligence Agency, the Defense Threat Reduction Agency, the Fires Center of Excellence, Service School Houses, the Marine Aviation Weapons/Tactics Squadron, Operations Support Squadrons, Intelligence Squadrons, and numerous operational units.

Joint Aircraft Survivability Program

The mission of the Joint Aircraft Survivability Program (JASP) is to increase military aircraft combat survivability – and, by extension, effectiveness – in current and emerging threat environments. JASP supports the mission through funding and oversight of Research, Development, Test, and Evaluation to develop aircraft survivability technologies and assessment methodologies. JASP also supports the mission through cross-Service coordination, educating the community about aircraft survivability, maintaining and improving core survivability tools, and taking a lead role in combat data collection. In FY16, JASP funded 47 multi-year projects and delivered 27 final reports. In FY16, JASP focused on projects intended to either 1) defeat near-peer and second-tier adversary threats by developing measures to avoid detection and counter engagement of advanced radio frequency and infrared guided threats; 2) improve aircraft force protection; or 3) improve aircraft survivability to combat-induced fires.

Defeat Near-Peer and second-Tier Adversary Threats

To defeat near-peer and second-tier adversary threats, JASP focused on developing: 1) measures to counter adversary radio frequency-guided threats and anti-access/area-denial capabilities, coupled with quantifiable improvements in ESAMS and Hardware-in-the-Loop capabilities; and 2) measures to counter emerging infrared homing threats with advanced counter-countermeasures, coupled with quantifiable improvements in The Modeling System for Advanced Investigation of Countermeasures (MOSAIC) and Hardware-in-the-Loop capabilities.

- 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, in coordination with the Air Force Life Cycle Management Center, developed several upgrades to ESAMS to maintain its relevancy to current and future threat environments. These upgrades include:
  - The capability to model the flow fields around chaff release to more accurately represent chaff bundle dispersion patterns. This capability will be released in ESAMS v5.3 in March 2017.
  - Integration of an advanced naval surface-to-air missile threat, which was developed in cooperation with the Office of Naval Intelligence. This capability will be released in ESAMS v5.3 in March 2017.
  - Improvement of two threat engagement radar models by adding their electronic counter-countermeasure capabilities. These upgrades will be released in ESAMS v5.4 in FY18.
- MOSAIC is the primary digital tool used to develop and assess effective U.S. aircraft infrared countermeasures (IRCM).

- JASP concluded a multi-year effort with Large Aircraft IRCM (LAIRCM) and Common IRCM (CIRCM) program support elements of the Air Force Research Laboratory and the Naval Surface Warfare Center, Crane Division to verify and validate MOSAIC for LAIRCM IOT&E. This effort verified and validated nine threat missile models in MOSAIC for directed energy IRCM supporting LAIRCM, CIRCM, and other future system development, test, and evaluation.

- A continuing need across the DOD is ready access to valid countermeasure characterization model data. The ability to model countermeasures is a critical component in the threat engagement simulations used to develop and optimize tactics, techniques, and procedures (TTPs) in response to near-peer and second-tier adversary threat improvements.
  - JASP funded the Army's Armament Research, Development and Engineering Center in conjunction with Naval Air Systems Command (NAVAIR) to conduct flight tests to collect Radar Cross Section data on a new chaff design. The data will be used to determine the optimum response range of metamaterial for countering radio frequency threats. Initial analysis indicates that the chaff can be utilized from the S through W bands.
  - JASP funded the development of a physics-based model of chaff dispensed in airflow around fixed and rotary wing aircraft. This will improve modeling of the effectiveness of chaff as a countermeasure; current models do not optimize chaff dispersion based on the influences of aircraft flow field vortices. Additionally, chaff models estimate cloud growth based on empirical test data rather than physics-based modeling of individual particles on the Radar Cross Section or Doppler effects. NAVAIR conducted flight testing to collect chaff dispense characteristics in various fixed and rotary-wing aircraft flow fields. NAVAIR, the Army Aeroflightdynamics Directorate, and the Office of Naval Intelligence are working together to develop the Computational Fluid Dynamics model to include flow field effects.
- Helicopter loss rates during Operation Iraqi Freedom, Operation Enduring Freedom, and subsequent counterinsurgency operations were significantly reduced by employment of Missile Warning Systems and effective countermeasures. JASP funded the following efforts to develop technologies and techniques to counter newer classes of infrared-guided seekers:
  - Naval Research Laboratory development of missile warning algorithms using two-color infrared imagery for early identification of threat missiles to enhance countermeasure effectiveness. The main goals are to develop missile identification algorithms capable of exploiting two-color infrared imagery, determine the ability to perform missile identification in urban clutter, and characterize jamming performance for Distributed Aperture IRCM (DAIRCM).
  - Testing threat system Infrared Counter-countermeasures' performance against current countermeasure technologies using a two-color tracker to understand how color ratio is used to discriminate between flares and the target; the results will be used to develop more effective countermeasures.
  - Development of a new capability to field test missile seekers against model aircraft with countermeasures including paints and directed energy to optimize electro-optical/infrared countermeasures. The countermeasure effectiveness of various aircraft paints and paint schemes is determined by testing with a surrogate threat infrared seeker. The scale model test facility at the Naval Research Laboratory's Blossom Point Research Facility is a bridge in test capability between laboratory tests and field tests with full scale aircraft. Validation of seeker results provides a surrogate advanced threat seeker for use in countermeasure development and evaluation.
  - Investigation of the feasibility of using Ultra-Short Pulse lasers for aircraft IRCM. The results of the study will support an Office of Naval Research initiative to further test and develop Ultra-Short Pulse IRCM.
  - Completed design and testing of a standardized test set to measure expendable countermeasure launch setback forces. Developed a standard operating procedure to generate expendable countermeasure setback force data and created a database for tri-Service use. Standardizing the testing of expendable launchers (i.e., flare buckets) across the tri-Service community will minimize test duplication and reduce development costs.

Improve Aircraft Force Protection

To improve the ability of U.S. aircraft to avoid threat detection and to mitigate damage when hit, JASP funded several projects focused on the following objectives: improve situational awareness; counter unguided threats; harden aircraft systems; and improve the accuracy and confidence of vulnerability assessments.

- Improve Situational Awareness. JASP funded the Naval Research Laboratory to develop a sensor package that incorporates both mid-wave infrared (MWIR) and acoustic waveforms for detecting hostile fires and determining the location of the shooter. In FY16 (the second year of a three year program), the project enhanced the baseline approach to further reduce false alarms and improve shock wave propagation predictions. Shock-wave generation propagation simulation models and detection algorithm updates were provided to the DAIRCM program. The algorithm update achieved a 2.5X detection improvement in forward flight/maneuver and a greater than 10 percent improvement in hover over previous algorithms. Analysis of hostile fire detection system noise and performance on HH-60 corrected detection issues in forward flight maneuver.
- Counter Unguided Threats. Aircraft and crew losses to rocket-propelled grenades (RPGs) and other unguided threats are a concern for rotary-wing aircraft. JASP funded NAVAIR and the Army Armament Research, Development and Engineering Center (ARDEC) to develop an anti-RPG warhead. ARDEC

and NAVAIR developed four anti-RPG warhead concepts that could launch from a helicopter expendable countermeasure launcher. Testing of prototypes will begin testing in FY17, and the results will aid the Navy's Helicopter Active RPG Protection program.

- Harden Aircraft Systems. In FY16, JASP vulnerability reduction efforts focused on three major areas to improve aircraft force protection: RPG defeat, innovative opaque and transparent armors, and aircraft hardening against high-energy lasers (HEL). During FY16, JASP:
  - Determined, by compiling existing test data, that there is insufficient data on the response of the PG-7 piezo fuze to high-velocity impacts of common aircraft materials at oblique angles to model potential defeat mechanisms. Since RPG-7 testing has primarily focused on heavy track and ground vehicles there is little data to define constraints in designing solutions to mitigate RPG effects on aircraft.
  - Integrated low-power laser mitigation technology into the highly successful Multi Impact Transparent Armor System. For this initial JASP HEL hardening effort, the focus was to mitigate dazzling from a common, commercially available Nd:YAG (neodymium-doped yttrium aluminum garnet) laser at a wavelength of 1,064 nm. The technology blocked the targeted wavelength while maintaining a 97.2 percent transmission rate in the visible spectrum compared to the pre-notched baseline system with minimal transmission effect in the night vision goggle performance band. However, the system multi-hit capability was compromised due to the ceramic strike face de-bonding on the first hit. Additional development and testing is required before fielding.
  - Initiated a project to determine composite material loss of strength (under mechanical load) as a function of time when exposed to short-duration, high-intensity, thermal loads typical of HEL impingement. From this data, time-dependent probabilities of component damage (Pcd/h) curves can be developed for use in system-level vulnerability assessments.
- Improve the Accuracy and Confidence of Vulnerability Assessments. In FY16, JASP funded efforts to improve the accuracy and confidence of the prediction of projectile and warhead fragment penetration used to assess aircraft vulnerability.
  - JASP developed, implemented, and verified standard formats for the 11 threat projectiles and the 12 single fragments that are most often used in system-level aircraft vulnerability assessments and fire prediction studies. These files will provide consistency across studies performed by different organizations and will be incorporated into the unified threat characterization database that was released in the Air Force Vulnerability Toolkit v6.8 in December 2016.
  - JASP continued to improve projectile penetration predictions by converting the ProjPen projectile penetration model to a six degrees of freedom model with the goal of predicting residual yaw within five degrees and reducing the error in the prediction of system-level vulnerable area.

Improve Aircraft Survivability to Combat-Induced Fire. Threat-induced fire is the largest potential contributor to fixed-wing aircraft vulnerability and the greatest source of uncertainty in aircraft vulnerability analysis. In FY16, JASP focused on developing solutions to maximize residual flight capability in the event of threat-induced onboard fires.

- JASP compiled and began evaluating data from across the Services to determine if self-sealing fuel bladders are performing as expected and whether military-standard qualification test methods adequately address threshold survivability requirements. JASP presented the results at the Tri-Service Fuel Bladder Roundtable and will document them in a final report.
- Developed and optimized, with a statistical design of experiments, next-generation self-sealing fuel bladder materials and construction layups. The next-generation bladders are lighter, more responsive to alternative aviation fuels and blends, and better at preventing fuel loss. Testing will continue during FY17.
- JASP continued work to optimize fire-resistant resin formulations for use as barrier ply on polymer matrix composites used in military aircraft. Integration of this type of resin could increase protection against internal fires and HELs. Coupon testing against heat flux conditions representative of small dry bay fires and HEL radiation is underway.

Combat Damage Assessment

- JASP enforced aircraft combat damage incident reporting in the Services and the DOD by continuing to support 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. JCAT ended its operation in Afghanistan in October 2014 with the return of deployed assessors to the United States. The team has continued to support assessments remotely from the continental United States and is ready to deploy rapidly outside of the United States if necessary.
- The JCAT started 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.
- 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, J8, on an Aircraft Combat Damage Reporting (ACDR) Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Policy (DOTMLPF-P) Change Request (DCR) proposal that would institutionalize ACDR through changes in joint doctrine, training, information technology infrastructure, and policy. The DCR completed the Joint Staff review and comment process and was submitted for Joint Requirements Oversight Council approval.

- The JCAT trained the U.S. aviation community on potential aircraft threats and combat damage. This training includes but is not limited to: capabilities briefs, intelligence updates, recent "shoot-down" briefs to discuss enemy TTPs, and the combat damage collection and reporting mentioned above. The attendees include aircrews, maintenance personnel, intelligence sections, Service leaders, symposia attendees, and coalition partners.

The Joint Live Fire Program

In FY16, Joint Live Fire (JLF) funded 27 projects and delivered 21 reports. Focus areas for JLF included projects that either 1) characterized new survivability issues; 2) characterized new lethality issues; 3) improved accuracy and fidelity of weapon data; 4) improved test methods; or 5) improved modeling and simulation methods.

Characterization of New Survivability Issues

- Military Combat Eye Protection (MCEP) systems (spectacles, goggles) help protect soldier's eyes from debris and fragments associated with explosive munitions and IEDs. MCEP systems typically use lenses made from polycarbonate. JLF is assessing whether another material, Trogamid CX, is also a suitable lens material. Limited prior ballistic testing indicates Trogamid CX has superior ballistic impact resistance at room temperature.
  - JLF conducted testing to assess the ballistic performance of polycarbonate and Trogamid at various temperatures and to compare and contrast the ballistic performance of both materials.
  - The test data were used to develop curves that illustrate ballistic performance versus temperature for polycarbonate and Trogamid lenses, enabling a comparative assessment of the ballistic performance.
  - The data are currently being evaluated. The U.S. Army Natick Soldier Research, Development, and Engineering Center will use the results to assess the suitability of using Trogamid to manufacture protective eyewear in the future.
- Crew survivability in the event of a propellant fire onboard a M109A7 155 mm self-propelled howitzer is a concern. Unlike a fuel fire, a propellant fire is self-oxidizing and cannot be extinguished by the integral automatic fire extinguisher system; it has the potential to be more lethal to crewmen than a fuel fire.
  - JLF conducted a fire test focusing on the adequacy of various design solutions to improve crew survivability from a propellant fire prior to M109A7 full-rate production.
  - The data obtained during this test have been analyzed and will provide a basis for recommendations to improve M109A7 crew survivability. The recommendations will be included in the Live Fire Test and Evaluation Report provided as input to the March 2017 M109A7 full-rate production decision review.
- The U.S. military operates the C-12 aircraft in a number of roles including intelligence, surveillance, and reconnaissance; medical evacuation; and passenger and light cargo transport for the Army, Navy, Air Force, and Marine Corps in both hostile and non-hostile environments. However, the survivability of the C-12 aircraft in hostile environments has not been fully characterized. In FY16, JLF assessed the survivability of the C-12 due to direct ballistic engagements to the aircraft fuel system.
  - The results of this project will provide the information necessary to make informed operational and acquisition decisions based on an understanding of the likelihood and resulting damage levels from small arms threat engagements.
  - Since the fuel system is one of the largest contributors to aircraft ballistic vulnerability, this project examined ullage reaction to a variety of ballistic engagements. Data analysis is ongoing.
- JLF investigated the effectiveness of an improved ballistic armor system to protect CV-22 Osprey crewmembers from ballistic threats. The project used threats not previously tested as part of LFT&E to investigate the armor system performance when challenged along different shotlines. The results of this project will help guide future development efforts for the Osprey's next generation ballistic protection systems.
- Emerging High Energy Lasers (HELs) represent an emerging threat to aircraft and unmanned aerial vehicles (UAVs). The fuel systems of many UAVs have a large presented area which makes them vulnerable to HEL engagements. JLF obtained baseline damage-effects data for both fuel-backed dry bay and adjacent subsystems subjected to HEL thermal flux, and assessed both suppression of laser-induced dry bay fires and laser hardening methods. JLF will use the data to support modeling and simulation of HEL engagements and the improvement of hardening methods to reduce vulnerabilities from HEL engagements.

Characterization of New Lethality Issues

- JLF funded the Army Research Laboratory to characterize the behind armor debris (BAD) of an anti-tank penetrator mine. BAD consists of fragmentation from both the target vehicle's armor and the residual penetrator that spreads out as it is ejected into the vehicle's interior.
  - The additional BAD data for this threat will provide empirical data to support the design of protection systems against this threat.
  - The Army Research Laboratory will also use the test results to construct BAD models for use in vulnerability/lethality analyses. The Army Research Laboratory uses these BAD vulnerability/lethality analyses to support acquisition programs and the planning and evaluation of vehicle vulnerability testing.
- JLF funded the Air Force's 780th Test Squadron (780 TS) to conduct a modeling and simulation analysis to evaluate the lethality of a mix of 30 mm target practice ammunition and high-explosive incendiary (HEI) ammunition to determine the most effective alternative for the A-10's current combat mix.
  - The original A-10 combat load included a mix of both armor-piercing incendiary ammunition with depleted uranium penetrators and HEI ammunition. Environmental

health concerns with depleted uranium and aging-related reliability concerns have resulted in commanders using only HEI ammunition instead. This use of 100 percent HEI ammunition has demonstrated reduced lethality and effectiveness in engagements with combatants shielded by light armor vehicles, soft-skinned vehicles, or structures such as adobe brick walls.
  - This project has the potential to introduce an Urban Combat effective Mix (UCM) using target practice and HEI ammunition that provides an increased lethality over a 100 percent HEI combat load. Lessons learned from this application of target practice ammunition could later be applied to 20 mm and 25 mm weapon platforms for all users throughout the DOD. The results of this effort will also provide the Joint Munition Effectiveness Manual with 30 mm target practice round lethality data.
  - Live ammunition testing will occur in FY17 following the results of this modeling and simulation analysis.

Weapons Data Accuracy

- JLF was resourced to obtain new arena test data on the MK 84 general purpose bomb (Figure 2) due to concerns about the quality of existing MK 84 characterization data. JTCG/ME will incorporate the results of this test into JTCG/ME products. This testing complements similar testing done in FY15.
  - Initial examination of the fragment speeds from the test indicated a variance from the current characterization data. This variance has a strong potential to influence weapon usage for lethality, collateral damage estimates, and risk assessment.
  - In addition to the direct application of the characterization by the warfighter, JTCG/ME will compare the data with the output of shock physics predictive tools to improve the warhead detonation model in order to produce high fidelity results, potentially reduce the number of tests required for characterization of other warheads, and provide a better understanding of the fragment cloud.
  - Sandia National Laboratories utilized the test to explore optical fragment tracking techniques. These tracking techniques have the potential to provide additional data that will improve physics-based modeling.

Figure 2. Still photograph from MK 84 vertical arena test

- Mk 82 and Hellfire vs Adobe Walls. JLF funded the Naval Surface Warfare Center, Dahlgren Division to evaluate the effects of the blast and fragmentation from a MK 82 MOD 1 General Purpose bomb and HELLFIRE R9E warhead on adobe block structures.
  - JLF will collect critical data to determine a threshold radius for wall destruction.
  - The results will be used to improve collateral damage estimates and safe engagement distances for targets in close proximity to adobe buildings with civilian occupants. There currently exists no test data to support these estimates.
- Building Debris Characterization. JLF funded the Naval Surface Warfare Center, Dahlgren Division to conduct a test to characterize the secondary debris produced by detonation of a 105 mm PGU-44/B high-explosive projectile within a concrete masonry unit structure target (Figure 3).
  - JLF will collect critical information to characterize building debris in a manner similar to that of warhead fragments.
  - The results will be used to improve risk estimates of personnel injury resulting from both weapon fragments and building debris. No test data exists to support these estimates.

Figure 3. Concrete masonry unit for characterizing building debris

Improvements of Live Fire Test Methods

- Penetration Profiles of Ballistic Backing Material. JLF is investigating a test procedure to improve the characterization testing of materials currently being evaluated for use as backing material during ballistic testing of Personal Protective Equipment. The current clay backing material is subject to variations that can influence test results.
  - The current characterization tests for backing materials do not replicate the dynamic deformation rates those materials experience during ballistic testing.
  - The results of this effort will permit selection of backing materials based on testing at deformation rates closer to those experienced during ballistic testing. The technique will permit comparisons between emerging prototype backing materials as well as with historical data on the current clay backing material.
  - Testing was recently completed, and the results will be used to screen potential new backing materials and compare their behavior with the current clay backing material.
- Optimization of Arena Test Data Collection Methodology. JLF is investigating the use of a new methodology, based on

techniques developed by NASA, to improve collection of fragment velocity and spatial distribution data during arena testing.

- The technique utilizes piezoelectric film panels for detection, which immediately reports fragment impact locations to a data recorder and requires no additional work for locating the fragments.
- JLF will use the data collected during this program to assess the feasibility incorporating piezoelectric film sensors as a standard method of collecting fragmentation impact location and velocity data during arena testing. The initial results from this project should be available in early FY17.

Improvements of Live Fire Modeling and Simulation

- Enhanced Modeling of BAD Velocity Field for KE Penetrators. JLF supported the improvement of the behind armor debris (BAD) algorithm by collecting unprecedented, high-speed images of kinetic energy warhead BAD using the pulsed laser illumination system (Figure 4).
  - Three-dimensional analyses of these images produced fragment speeds as a function of the fragment's angle from the residual jet.
  - The test data indicate the scatter of kinetic energy BAD fragments may not be a simple function of cone angle, however the Gaussian velocity field used in the BAD algorithm is an improvement over the previous function. Based on the results of this project, the Gaussian velocity filed will be used to represent kinetic energy BAD fragment velocities.

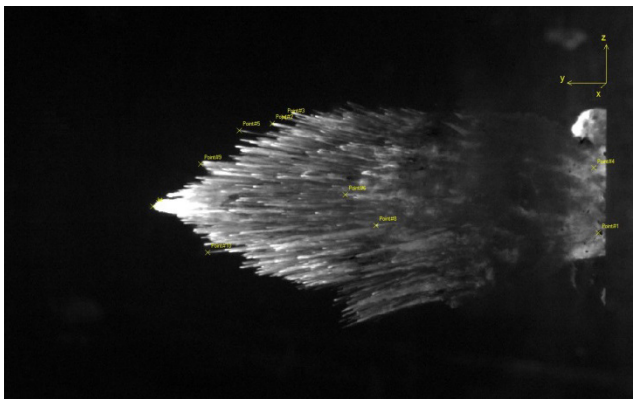


Figure 4. High-speed image of BAD fragments

- Joint Light Tactical Vehicle (JLTV) Underbody Blast Vulnerability Assessment. JLF is investigating the use of high-fidelity computational physics models to simulate vehicle underbody blasts at multiple vehicle locations with several threat sizes. This approach will improve the ground survivability community's understanding of vehicle structural response and occupant injury risk for various threat size and blast location scenarios.
  - JLF will perform system-level underbody blast simulations on the JLTV in at least 12 blast locations using up to 3 sizes of threat and assess the results against the DOT&E survivability criteria used for the JLTV program (see Figure 5). The high fidelity mesh model to support these simulations is in development.
  - This modeling approach would represent a new assessment capability: a multi-threat and multi-location methodology for mapping vehicle structural response and occupant injury risk of combat systems. Performing simulations at multiple threat locations should show the changes in vulnerability across different regions of the underbody, while simulating different charge sizes will help identify the estimates of most vulnerable underbody areas to increasing threat size.

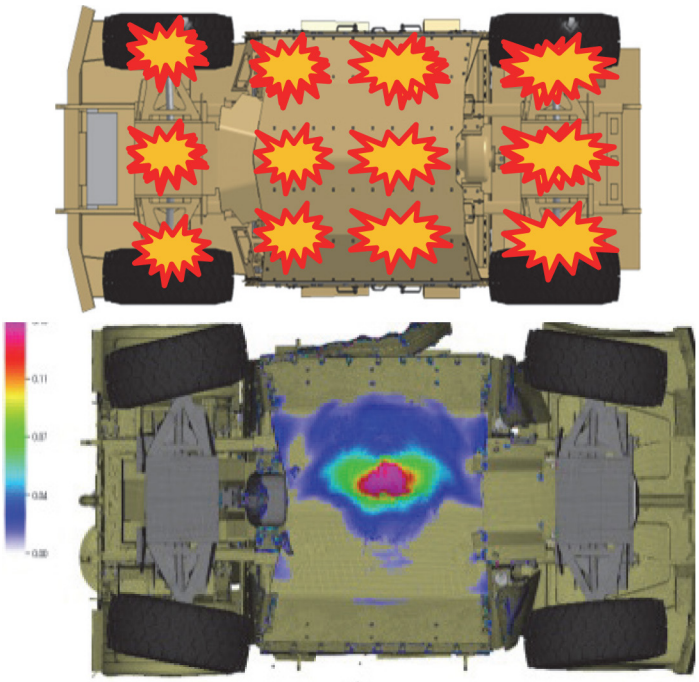


Figure 5. Shotline selection for simulations (top) and structural response of vehicle underbody (bottom)

- JLF supported the development of a shaped charge jets effects model.
  - Initiation of stowed 25 mm ammunition is one of several lethal mechanisms that can impart catastrophic levels of damage to a ground vehicle. Testing on stowed 25 mm training rounds with shaped-charge jets of varying size and velocity collected quasi-static pressure versus time data that will be used to develop a new ammunition compartment vulnerability model.
- JLF continued a joint effort with Germany to develop and validate the Dynamic Systems Mechanical Advanced Simulation (DYSMAS) hydrocode used to model bottom and near-bottom underwater explosions effects.
  - In FY14, several tests were conducted in the Briar Point test pond at the Aberdeen Test Center, Maryland, using a floating shock platform to collect data on platform response from charges located at mid-depth, near-bottom, and on the bottom.
  - The analysis of those test results was completed in FY15, providing additional validation for the use of DYSMAS in vulnerability assessments for the modeling of underwater

explosion loading and ship responses in littoral or harbor environments, where bottomed or tethered mines are likely to be encountered. DYSMAS predictions are improved with the use of sea-bottom data for the location of interest.

- JLF continued to investigate sea-based weapons effects phenomena to improve the fidelity of modeling and simulation used to assess both platform survivability and weapon effects.
  - In FY16, work continued to improve the understanding of combined shock and submergence effects from underwater explosions on unique submarine structural configurations when at deep depths. Scaled test models were fabricated in preparation for FY17 testing. The data from these tests will be correlated with modeling and simulation results to determine which models are best for assessing underwater explosion shock loads in combination with submergence pressure loadings on submarines.
  - In FY16, JLF developed a plan to conduct a collaborative research and test effort with the Canadian Navy to improve the ability to model the effects of near-field underwater explosions and the resulting bubble and bubble jetting loading on structural damage. The data gathered will validate modeling and simulation tools used to evaluate the survivability of Navy platforms against torpedo and mine threats and to improve weapon lethality estimates.

LFT&E SPECIAL INTEREST PROGRAMS

Warrior Injury Assessment Manikin

- The Warrior Injury Assessment Manikin (WIAMan) Engineering Office (WEO) is currently leading the WIAMan project (Figure 6) on behalf of the Army Research, Development, and Engineering Command (RDECOM), with the Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) supporting acquisition-related preparation activities. RDECOM and PEO STRI signed a memorandum of agreement defining the leadership, responsibilities, and funding relationships between these two organizations.
  - The WIAMan project will enter the acquisition cycle as a post-Milestone A program of record via a Materiel Development Decision in FY17. The WEO will transition leadership of the WIAMan project to PEO STRI at Milestone B, but will continue to support PEO STRI in certain non-severable activities related to the WEO's expertise in biomechanics, anthropomorphic test device (ATD) development, and Live Fire Test and Evaluation (LFT&E).
  - The Army developed and validated a Test Capability Requirements Document (TCRD) for the WIAMan project. The Army Test and Evaluation Command, RDECOM, and DOT&E all signed the TCRD. The TCRD identifies the key performance parameters, key system attributes, and requirements for the WIAMan ATD system. In addition to the development of a validated TCRD, the WIAMan project held an Industry Day in June 2016 in order to gauge the level of interest and available competition in the ATD industrial base.
  - The WEO continued to demonstrate that the current ATD used in LFT&E, the Hybrid III, lacks biofidelity in the underbody blast (UBB) test environment, meaning it does not exhibit a human-like response when exposed to UBB loading conditions. ATD biofidelity is assessed via compliance with biofidelity response corridors (BRCs) for the human body regions and response parameters of interest.
  - In FY16, the project delivered the remaining 13 component-level BRCs. These BRCs are focused on the human response in the head/neck, lumbar spine, pelvis, and lower leg/foot and ankle body regions.
  - The project delivered 6 of 12 whole-body BRCs. These BRCs focused on human response to different combinations of parameters that vary in LFT&E, such as loading rate inputs, occupant posture, and Personal Protective Equipment. The remaining whole-body BRCs will be developed in FY17.
  - The project generated initial data on the tolerance of bones to severe loading conditions and developed a notional human injury probability curve (HIPC) for foot and ankle fractures. The WEO also conducted a prioritization exercise that benefitted from updated analyses of injuries experienced by soldiers in combat; this exercise resulted in an executable biomechanics test plan that will result in no less than 36 unique HIPCs, spanning the head, neck, lumbar spine, pelvis, leg, and foot/ankle body regions.
- In FY16, the WEO initiated a 3-year, $3 Million pilot study to investigate the effects of the UBB environment on female soldiers. The objective of this study is to determine if UBB loading conditions affect females differently than males and, if so, for what reasons. 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. A total of 5 whole body female biomechanics tests were executed in FY16, with an additional 13-17 planned for FY17.
- The WEO continued to implement emerging biomechanics data into the development of a WIAMan ATD through new task order awards to Diversified Technical Systems (DTS). In FY16 DTS delivered a Technology Demonstrator ATD that demonstrated improved biofidelity and usability in the UBB test environment when compared to the Hybrid III ATD. Test results to date indicate that the WIAMan Project is on track to achieve a Technology Readiness Level 6 prior to program transition at Milestone B. DTS also delivered the first data acquisition system (DAS) units for benchtop testing in September 2016, and will deliver four fully integrated first generation WIAMan ATD prototypes for verification and validation testing in June 2017.

- The WEO continued its refinement of an optimized ATD finite element model. This model supported analyses to accelerate the redesign of the ATD to achieve strength-of-design, biofidelity, and usability goals. A full three-dimensional description of the ATD has been created and validated in accordance with the current Technology Demonstrator design and performance.
- The WEO continues to accomplish its technical goals regarding establishing human body response to the UBB load regime, to include expanding its investigation into potential gender-based differences. The Assistant Secretary of Defense for Health Affairs has committed to fully funding the medical research required to meet the WEO's scientific goals. However, the planning and execution of the formal acquisition program envisioned by the Army is behind schedule, while incurring significant overhead costs. Despite the Army's and the Department's large investment in this project, the Army's concerns about the cost of procuring and incorporating this much-needed technological advancement into UBB LFT&E have resulted in no acquisition funding programmed for the project after FY18.

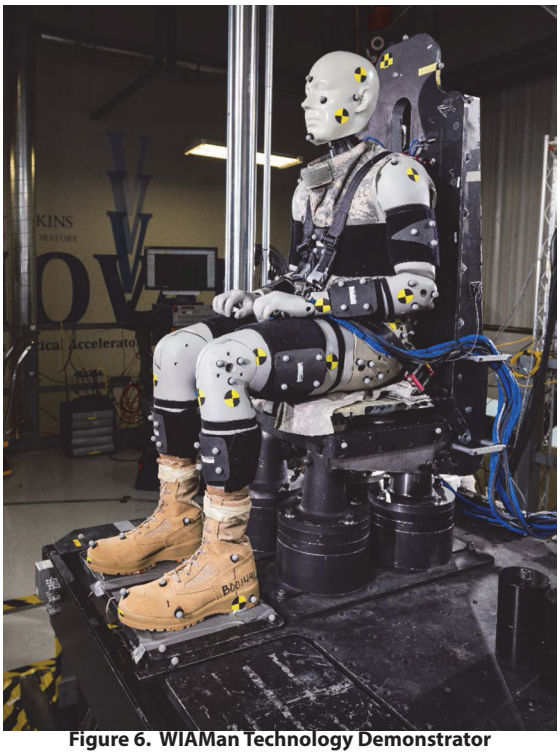


Figure 6. WIAMan Technology Demonstrator

Homemade Explosives

DOT&E continued to participate in the Army-led, multi-Service effort known as the Homemade Explosives Characterization (HME-C) working group. The HME-C effort originated to address concerns regarding the Department's ability to test operationally significant scenarios involving underbody blast threats, and to ensure adequate LFT&E of military vehicles now and in the future. In FY16:

- The HME-C working group completed the planned scope of test and evaluated the data resulting from all of the program's test phases.
- DOT&E used the information and data to develop LFT&E policy for employing buried underbody blast surrogates. This included a new soil standard for use with underbody blast testing.
- The Army Test and Evaluation Command developed operating procedures to implement this policy.

Small Boat Shooters' Working Group

Small boats represent a growing threat class to ships operating in littoral waters and are targeted by a wide variety of weapons systems.

- In FY16, DOT&E sponsored the fifth annual Small Boat Shooters' Working Group, which examined the general nature of the small boat threat in littoral waters; summarized the threat classes and available targets and models available for ammunition, rocket, and tactical missile weapon systems; and attempted to synchronize various LFT&E and other operational test approaches among the various programs/Services by sharing the breadth of test and evaluation options available to evaluators.
- The working group assessed the nature of the small boat threat; the availability of targets and lethality models representing those threats; the data collection, test techniques, and instrumentation that have been applied to small boats; and the performance of shipboard and aircraft weapons against small boat threats. The group also reviewed results from DDG-1000 gun tests, a test concept for HELLFIRE longbow missiles vertically fired from a ship against High-Speed Mobile Surface Targets (as part of the Littoral Combat Ship (LCS) program), and results from tests of special 30 mm gun ammunition under development specifically to counter the small boat threat.

Helicopter Seating Systems

The House Report accompanying the National Defense Authorization Act for FY16 required a briefing describing any plans for improvements to current helicopter seating systems. DOT&E briefed Congressional staff that, while improved helicopter seating would improve force protection, it is just one aspect of the overall helicopter force protection/survivability improvement effort. Addressing leading causes of fatalities in mishaps and combat-induced crashes with near-term technology solutions such as controlled flight into terrain collision and threat avoidance would provide a higher payoff.

- The leading causes of mishaps and combat-induced casualties cannot be mitigated via improved helicopter seating systems.
  - The leading cause of mishaps is controlled flight into terrain due to loss of situational awareness. These events are typically not survivable but could be mitigated through implementation of crash avoidance technologies. Crash avoidance technology has been demonstrated on the UH-1N at technology readiness level 9 (use in operational conditions). If crash avoidance requirements are set, solutions could be fielded on existing systems.
  - The leading causes of helicopter combat-induced casualties are aircraft vulnerabilities leading to catastrophic crashes that are not survivable. These crashes could be mitigated through improved situational awareness, adaptive flight

control, and countermeasure technologies. Additional RDT&E investments in these areas are warranted.

- In many survivable crashes, helicopter seating systems provide adequate protection for the pilot/crew but not for troops and passengers. The troop seating system standard has been waived to enable mission performance. Therefore, existing troop seating systems do not meet the military standards, resulting in preventable casualties.
- Current helicopter seating system ergonomics may be detrimental to mission effectiveness and result in long term disability, but the extent and exact causes have not been determined. Additional analysis is warranted to determine the root cause of casualties, especially to troops and passengers, and the root cause of long-term disabilities.
- DOT&E recommended identifying and addressing the root causes of crew casualties in mishaps and combat-induced crashes and funding the systems that have the greatest return on investment for avoiding or reducing fatalities and injuries.

Cybersecurity

Cybersecurity

Cybersecurity

SUMMARY

DOT&E provides cybersecurity evaluations of DOD acquisition programs as part of the programs' operational test and evaluation. In addition, Congress directed DOT&E to perform cybersecurity assessments of live, operational DOD networks and systems during Combatant Command (CCMD) and Service training exercises. This report includes results from FY16 assessments, but pays particular attention to the trends and changes that have occurred since 2009, when DOT&E updated and improved the requirements and procedures for cybersecurity test and evaluation. Key observations follow, and additional details are in the classified cybersecurity report DOT&E issued in July 2016:

- Over the last 7 years, the Department has increased its focus on cybersecurity, and allocated additional resources to cyber capabilities, expertise, and associated activities. As a result, in recent years some DOD programs and networks have demonstrated, for the first time, effective defenses against attacks from cyber Red Teams emulating threats with limited cyber capabilities. In recent years, DOT&E's cybersecurity assessment program has helped CCMDs address major cybersecurity vulnerabilities through its focus on finding vulnerabilities, helping the CCMD to fix the vulnerabilities, and independently verifying that the vulnerabilities have indeed been fixed. This "find-fix-verify" approach has proven to be an effective way to rapidly improve the cybersecurity of DOD programs and networks.
- Despite this progress, during major exercises critical CCMD missions remain at risk when subjected to cyber-attacks emulating an advanced nation-state adversary. Cyber-attacks are clearly a part of modern warfare, and DOD networks are constantly under attack. However, DOD personnel too often treat network defense as an administrative function, not a warfighting capability. Until this paradigm changes, and the change is reflected in the Department's approach to cybersecurity personnel, resource allocation, training, accountability, and program and network management, the Department will continue to struggle to adequately defend its systems and networks from advanced cyber-attacks.
- DOT&E issued more explicit policy and guidance regarding cybersecurity testing over the past 7 years, resulting in a significant increase in the cybersecurity component of OT&E for major programs. Most operational tests have found significant vulnerabilities and limitations in the system's ability to sustain missions or rapidly restore capabilities when compromised.
- Over the past 7 years, Red Team operators have become high-demand, low-density assets, and requests for Red Team services increasingly go unsatisfied. DOD had an enviable share of master-level operators 7 years ago, but a significant number of these cyber experts accepted positions in the private sector in the ensuing years, often because of the increased wages and more relaxed work environment. Simultaneously, demand within DOD for Red Team services has more than doubled. The new congressional requirement to conduct cybersecurity assessments of all major DOD programs (Section 1647 of the FY16 NDAA) will increase further the demand on DOD Red Teams. Additionally, Red Team capabilities and expertise must increase so that the teams can emulate more advanced and realistic adversaries during testing and training.
- Over the last 3 years, DOT&E refined and expanded the use of long-duration cyber Red Teaming in CCMD networks, including U.S. Pacific Command (USPACOM) and U.S. Northern Command (USNORTHCOM). Such long-duration Red Teaming, conducted by a Persistent Cyber Opposing Force (PCO), is far better at emulating advanced, persistent nation-state cyber threats, while at the same time more efficiently utilizing scarce Red Team resources. PCO activities have identified, and rapidly addressed, serious vulnerabilities that had not previously been discovered during more than a decade of short-duration, less realistic exercise events.
- To effectively fight a war in cyberspace, the focus of cyber defense needs to expand beyond the traditional approaches of system protection and intrusion detection to encompass a broader view of system resilience. DOD has focused a great deal of attention and resources on the defense of outward-facing boundaries. As a result, these boundaries have shown significant improvement in protecting against nascent- and limited-level attacks. However, Red Teams emulating a moderate-level adversary – or below – routinely demonstrate the ability to intrude DOD networks and operate undetected within DOD networks for extended periods of time. The Department needs to put more emphasis on preventing lateral movement by network intruders and improved detection of anomalous network activity.
- In recent years, CCMDs and Services have provided better opportunities for DOT&E-sponsored assessments to inject limited cyber-attacks and observe the resulting effects and responses. However, exercise and network authorities seldom allow fully representative cyber-attacks, and complete assessments of protection, detection, and response capabilities.
- Cyber ranges can be effective venues to fully evaluate realistic cyber-attacks and defenses in a safe and secure environment, without any risk to DOD operations and missions. Cyber ranges may be the only acceptable environment where Red Teams can fully execute attacks representative of an advanced nation-state cyber adversary. Over the last 7 years, DOD has matured its cyber range capabilities, but existing ranges will not be able to fully support the anticipated near-term requirements, including: needed training for the Cyber Mission Forces (CMF), more realistic CCMD and Service exercises and assessments, and rapidly increasing acquisition

program cyber testing requirements. Recent investments in the Persistent Training Environment and Cyber Test Ranges should help remedy these shortfalls, but improvements are likely to remain sub-optimized due to lack of a single Executive Agent for cyber ranges.

- While some Cyber Protection Team (CPT) elements have successfully defended DOD networks during our assessments, many of the 68 CPTs have not received adequate training or equipment to provide effective and timely support to defend networks and critical missions. The initial staffing of the CPT included personnel without the requisite skills and training, and with many current CPT members scheduled to depart in the next year, DOD needs to focus on attracting, training, and retaining skilled individuals for the CPT. DOT&E has provided excellent training opportunities for CPT members during our assessments, and we plan to work with U.S. Cyber Command (USCYBERCOM) to identify more opportunities to do so in the future.
- Over the last 7 years, CCMDs have become increasingly interested in Offensive Cyber Operations (OCO) capabilities. However, CCMDs often have little confidence in available OCO capabilities because the OCO developers have not tested the capabilities in a realistic environment. DOT&E sponsored several test events in FY16 to demonstrate that more realistic testing of OCO capabilities can be both expeditious and low-cost. These events demonstrated that realistic testing of OCO can reveal significant operational problems which do not surface during limited lab testing. The OCO developers can then address these problems to make the capability more likely to succeed when it is deployed. Realistic OCO testing also enabled DOT&E to provide CCMDs with an improved understanding of the scope and duration of OCO effects.
- In recent operational tests, DOT&E has frequently encountered two components that are prevalent across many DOD acquisition programs: Programmable Logic Controllers (PLC), and Cross-Domain Solutions (CDSs). These components can introduce cyber vulnerabilities to the system under test and the associated network(s). DOT&E provided guidance in 2015 and 2016 for testing industrial control systems that contain PLCs and CDSs. DOT&E also sponsored testing to help identify vulnerabilities, potential mitigation strategies, and rigorous methods for testing these components.

Table 1 below shows the operational tests involving cybersecurity, and the DOT&E-funded cybersecurity assessments conducted during FY16. Table 2 shows the cybersecurity test organizations that supported the conduct of the activities shown in Table 1.

TABLE 1. CYBERSECURITY OPERATIONAL TESTS AND ASSESSMENTS IN FY16		
EVENT TYPE	**SYSTEM OR ORGANIZATION**	
Cybersecurity Operational Test	Automated Biometric Information System	F-35 Joint Strike Fighter – Central Point of Entry
	AC130-J Ghostrider	F-35 Joint Strike Fighter – Squadron Kit
	Aegis Ashore	Joint Stand-Off Weapon
	Advanced Field Artillery Tactical Data System	Joint Warning and Reporting Network
	Army Integrated Air and Missile Defense	Littoral Combat Ship
	Acoustic Rapid Commercial-off-the-Shelf Insertion	LHA 6 - America Class - Amphibious Assault Ship
	Airborne Warning and Control System	MQ-9 Reaper
	Aegis Weapons System	Mobile User Objective System
	Common Aviation Command and Control System	Next Generation Diagnostic System
	Consolidated Afloat Network and Enterprise Services	Network Integration Event
	CV-22 Osprey	Navy Advanced Extremely High Frequency Multi-band Term.
	Defense Agency Initiative	Near Real Time Identity Operations
	Distributed Common Ground System – Navy	Pueblo Chemical Agent Destruction Pilot Plant
	Defense Medical Information Exchange	Paladin Integrated Management
	E-2D Advanced Hawkeye	Public Key Infrastructure
	Expeditionary Sea Base	RQ-4 Global Hawk
	Global Broadcast Service	Space-Based Infrared System
	Global Command and Control System - Joint	Spider XM7 Network Command Munition
	High Mobility Artillery Rocket System	Theater Medical Information Program – Joint
	F-35 Joint Strike Fighter – Air Vehicle	Warfighter Information Network – Tactical
	F-35 Joint Strike Fighter – Autonomic Logistics Operating Unit	
Exercise Assessments	U.S. Africa Command Epic Guardian 2016	U.S. Special Operations Command Jackal Stone 2016
	U.S. Central Command Marine Forces Central	USMC Large Scale Exercise 2016
	U.S. European Command Jackal Stone 2016	U.S. Strategic Command Global Thunder 2016
	U.S. Pacific Command Pacific Sentry 2016	U.S. Strategic Command Global Lightning 2016
	U.S. Southern Command PANAMAX 2016	U.S. Navy Valiant Shield 2016
Cyber Readiness Campaigns	U.S. Northern Command	
	U.S. Pacific Command	

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 Corp 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 and Lethality Analysis Division
Navy	Navy Information Operations Command
	Space and Naval Warfare Systems Command
	Navy Operational Test and Evaluation Force
Marine Corps	Marine Corps Information Assurance Red Team
Defense Agencies	National Security Agency
	Defense Information Systems Agency Risk Management Executive Red Team

RECOMMENDATIONS

- The Combatant Commands and Services should reduce restrictions that prevent testing and training against realistic cyber threats, and perform "fight-through" events to demonstrate that their critical missions are resilient in contested cyber environments.
- The Joint Staff should sponsor a cyber-focused exercise with a different CCMD each year, where cyber training and mission resiliency are the primary training objectives.
- The Services should upgrade their cyber Red Teams with additional capacity, capabilities, training, and threat assessments to ensure that the certified Red Teams can portray relevant and representative adversaries, including advanced nation-state threats.
- The DOD Chief Information Officer and USCYBERCOM should issue policy and instructions to require implementation of the following as soon as possible; vulnerabilities in these areas often jeopardize CCMD and acquisition program missions during cybersecurity assessments and operational tests:
  - Secure credential use and storage
  - Segregation of network privileges, to include role-based allocation of privileged accounts and responsibilities, and network segmentation based on the segments' mission criticality
  - Reduction of cross-connections between networks, and effective, active defense of cross-connections which cannot be eliminated
  - Encryption of data at rest and in transit
  - Centralized logging and audit log correlation to enable rapid detection and tracking of threats inside a system or network
  - Effective anomalous behavior detection, and cyber-attack response tactics and procedures for attacks inside the system or network, as well as at the system/network boundary
  - A consolidated reporting and analysis tool for cyber incidents
  - Locking down SharePoint websites based on "need-to-know"
  - Authentication and verification procedures for chat room participants
- The Joint Staff and USD(AT&L) should require systems and networks to support essential missions even when compromised, and cyber defenders should be able to quickly reset and restore systems and networks following a successful cyber-attack.
- DOD should designate a single Executive Agent for cyber ranges with the authority to oversee funding and personnel

for all DOD-funded ranges, and the authority to identify and certify commercial cyber range resources for DOD use, as appropriate. The leadership for the Persistent Training Environment and the Cyber Test Range should collaborate to identify priority requirements for range environments in support of testing, training, as well as CCMD and Service exercise assessments.
- DOD should field new cyber capabilities (e.g., Joint Regional Security Stacks, OCO capabilities) only after realistic operational testing confirms the capabilities will be effective and suitable for use by representative users.
- CCMDs and Services should routinely conduct long-duration cyber assessments using a PCO, to enable more threat-representative cyber Red Team activities on DOD networks and to more rapidly discover and address critical cyber vulnerabilities.
- USCYBERCOM, the Services, and Defense Information Systems Agency should conduct "hands-on" training in realistic networks using realistic cyber threats, and effective tools and procedures, for Cyber Mission Force (CMF) personnel and Cybersecurity Service Providers.
- USD(AT&L) and DOD CIO should sponsor the development of test tools and procedures for evaluating cybersecurity in non-Internet Protocol applications, including CDSs, PLCs, system-unique data buses and protocols, radio and acoustic frequencies, and tactical datalinks.

EVOLVING GUIDANCE AND TEST/ASSESSMENT TRENDS

In FY03, the Congress directed DOT&E to perform annual operational evaluations of information assurance with each of the CCMDs and Services; develop a process to similarly consider systems on the DOT&E oversight list; and report to Congress on the Information Assurance (IA) posture of the DOD. DOT&E has performed the required assessments annually since that time, and has in recent years issued and enforced new policy for cybersecurity OT&E.

Early assessments were generally network-focused, with extensive limitations on the supporting Red Teams. Today DOT&E observes fewer limits and restrictions on cybersecurity testing and assessments, but actual impacts to networks and systems are still limited due to safety, security, or other training requirements. The result is that warfighters generally train and conduct cyber assessments in a relatively benign cyber environment.

DOT&E issued the first guidance on cybersecurity requirements for OT&E in 2009, establishing requirements and procedures for testing cybersecurity. Over the past 7 years, that focus has expanded from information-handling systems to encompass a variety of weapons and weapons platforms, and the missions they support.

In 2011, ADM Mullen, the CJCS, issued an Execute Order (EXORD) that directed all CCMDs perform threat-representative assessments of critical CCMD missions in cyber-contested environments within a 3-year period. This EXORD charged exercise authorities and CCMD leadership to conduct major training exercises in a non-benign cyber environment. Exercise authorities now expected cyber Red Teams to participate during exercises, but CCMDs did not consider cyber to be a training objective, and hence cyber activities were severely limited. The Secretary of Defense Leon Panetta re-emphasized the CJCS EXORD in 2012, but this emphasis was soon diluted due to the downsizing and cancelation of exercises due to sequestration.

In 2013, DOT&E and USPACOM agreed that the Department needed to break from the notion that cyber training and assessment performed once a year was acceptable. As a result, DOT&E developed a new approach that includes multiple building-block events in a given year – a Cyber Readiness Campaign – that leads to a culminating event (e.g., a full CCMD exercise), and employs a PCO to emulate a realistic nation-state cyber adversary.

In 2013, USCYBERCOM created the Cyber Mission Force (CMF), consisting of 133 teams. USCYBERCOM and the Services did not have mature plans for training and equipping the CMF. This became evident during DOT&E-sponsored cyber assessments when CCMDs requested Cyber Protection Team (CPT) support, and CPTs were often slow to deploy and unable to provide much support when they arrived. This is still the case for many of the CPTs; however, more recently, DOT&E observed several instances where the CPTs working with hunt teams performed well in detecting and responding to Red Team intrusions. DOT&E will continue to encourage participation of CPT personnel in DOT&E-sponsored Cyber Readiness Campaigns and cybersecurity assessments, where CPTs receive much-needed "hands-on" network training while defending against a realistic cyber adversary.

Concerned with the lack of cybersecurity guidance for acquisition programs, in 2014 DOT&E recommended that the Department develop a cybersecurity requirement. In response, in November 2014 the Deputy Secretary directed the Joint Staff to develop such a requirement within 90 days. Over the past 2 years, the Joint Staff drafted a Cybersecurity Endorsement to the Survivability Key Performance Parameter. The Joint Staff also developed an implementation guide, which identifies a number of key attributes pertaining to cybersecurity that the Services must address in the requirements documentation for systems that handle digital data transfers. These attributes include the ability of the system to control access, reduce detectability, harden attack surfaces, encrypt data, detect anomalies, and recover from a cybersecurity incident. Although the cybersecurity endorsement has been in a draft form for months, the JROC has not yet formally approved and issued it.

In 2015, Secretary Carter issued the DOD Cyber Strategy. This coincided with a number of well-publicized cyber-attacks of government and private organizations, including the breach of

the Office of Personnel Management records involving millions of federal personnel. These cyber-attacks helped DOD senior leadership understand the importance of cybersecurity and created opportunities for DOT&E to portray more realistic cyber adversaries during operational tests and exercises.

Despite progress, operational test and exercise planners need to encourage the use of realistic cyber actions that could require restoration of systems or implementation of alternative means of operations. The reluctance to permit debilitating cyber-attacks is appropriate when there are personnel safety concerns, but the DOD needs to routinely assess the ability of missions and systems to either operate through cyber-attacks or restore operations afterwards. Training in a benign environment is not acceptable in any other warfighting domain, nor should it be for cyber.

The DOD should continue to lessen restrictions that prevent testing and training against realistic cyber threats in order to improve the resistance and resilience of mission and systems under conditions that increasingly are part of the daily operational environment.

PROGRESS AND CHALLENGES

Cyber Defenses Continue to Lag Cyber Threats

Over the last 7 years, DOT&E observed and reported on the gradual improvement of defensive capabilities within the Department. The levels of compliance with key cybersecurity practices and controls improved steadily for several years, and test events show that the majority of DOT&E-assessed systems and networks meet key cybersecurity compliance criteria. Nonetheless, DOD cyber Red Teams continue to compromise DOD systems and networks and jeopardize critical DOD missions during exercises. This is because mere compliance with cybersecurity controls is not enough to provide an effective cyber defense. An effective cyber defense requires well-trained, well-equipped cyber defenders, operating in a secure network environment, in conjunction with other warfighters, to maintain critical missions.

Focus Shift to Cyber Resilience: "Assume Breach"

Most cyber defense tools and systems focus on hardening network and system boundaries. When network configurations are up to standard and patches are current, DOD networks can usually withstand cyber-attacks from Red Teams using limited cyber-attack capabilities. Over the past 7 years, the DOD has hardened many of its networks and systems against cyber-attacks by more rapidly installing security patches and improving the security of credentials (such as passwords). This has helped prevent Red Teams using novice techniques from penetrating network and system boundary defenses and disrupting missions during exercises. However, Red Teams using more advanced techniques continue to demonstrate the ability to bypass boundary protections, intrude into DOD networks, and operate undetected for extended periods.

Once they have gained access to a network, Red Teams frequently use tools native to the network and stolen credentials. These two tactics seriously challenge defenders, as they do not currently have sensors or tools to determine that an adversary is using tools or credentials approved for that network; in order to identify an adversary presence, they must detect some anomalous activity or behavior. Anomalous behavior detection is a critical element of cybersecurity, but few DOD cyber defenders have the tools needed to accomplish this.

Coordination and communication among the many agencies and activities charged with providing cyber defenses is often inefficient or ineffective. This lack of coordination contributed to missed opportunities to detect Red Team activities.

DOD should prepare for potential adversaries who may employ advanced capabilities and techniques by developing "fight-through" capabilities. CCMDs and Services should perform frequent training in cyber-contested environments that emphasizes well-coordinated cyber responses, the ability to reset or restore networks and systems to operation following an attack, and the ability of the warfighter to complete assigned missions while under cyber-attack.

Maturing the Cyber Ranges

The DOD Enterprise Cyber Range Environment is a collection of four independent cyber-range assets where classified training and testing can occur. In 2011, these ranges were experiencing budget cuts and were becoming unsustainable. DOT&E proposed enhancements for these cyber ranges and the establishment of an Executive Agent in 2012; as a result, the cyber ranges received additional funding during the FY13 Program Review, but there was no decision for an Executive Agent.

The FY15 NDAA directed DOD to establish an Executive Agent for cyber training ranges and an Executive Agent for cyber testing ranges. In FY16, the DOD allocated funds separately for a Persistent Training Environment, and for cyber test ranges. As combined testing and training are necessary for efficient use of the ranges, and to help address the rapidly increasing demand for cyber range resources, the creation of two separate Executive Agents—with separate responsibilities and funding—may hinder the Department's ability to effectively respond to rapidly evolving and increasingly sophisticated cyber threats. The DOD should designate a single Executive Agent for cyber ranges with the authority to oversee funding and personnel for all DOD-funded ranges, and the authority to identify and certify commercial cyber range resources for DOD use, as appropriate.

Over the past 2 years, the Test Resources Management Center (TRMC) delivered multiple Regional Service Delivery Points (RSDPs) to key geographical locations, including USPACOM and MIT Lincoln Labs. RSDPs bring cyber range capabilities to local users to permit cost effective testing and training, and they provide a variety of capabilities (instrumentation, traffic

generation, environments, etc.) on the local "mini cloud" to reduce the bandwidth requirements for distributed range events. The TRMC also upgraded the National Cyber Range (NCR), and plans to build additional NCR facilities to help meet the rapidly growing demand for cyber test and training resources.

Assisted by DOT&E funding, over the last few years several of the National Labs demonstrated advances in the creation of realistic range environments, including environments that can be quickly built and deployed to an RSDP, the NCR, or other suitable range locations to support testing, training, and CCMD assessments that are not suitable for operational networks. DOD needs more of these environments to adequately test and train against advanced cyber threats.

Joint Information Environment Testing Shortfalls

In 2013, the Chairman of the Joint Chiefs of Staff signed a white paper entitled "Joint Information Environment" identifying "IT efficiencies" as a key goal. This white paper proposed a "shared Information Technology (IT) infrastructure with a common set of enterprise services, under a single security architecture." Subsequently, the DOD CIO established the Joint Information Environment (JIE) as a "concept." The DOD CIO intends all DOD networks to eventually conform to the JIE concept. Hence, the cybersecurity of the JIE concept is critical to the future security of the entire Department. Unfortunately, there is little evidence that JIE will improve cybersecurity, especially if Services field JIE components without adequate preparation in order to meet IT efficiency targets.

JIE is not a formal program of record, and it lacks a unified program executive to manage cost and schedule, monitor performance metrics, and plan and conduct testing. Furthermore, DISA and the Services are pursuing a non-traditional acquisition approach for major JIE components such as the Joint Regional Security Stack (JRSS), and both the Army and Air Force have fielded JRSS without conducting operational testing, despite developmental tests that showed cyber defenders could not use JRSS effectively to defend their network. See the JIE section elsewhere in this annual report for more details.

Although cyber defenders need improved tools to meet the evolving cyber threats, the DOD should not field tools such as JRSS until testing confirms that the tools are effective and usable by representative defenders.

Testing Offensive Cyber Capabilities

Combatant Commands are increasingly interested in Offensive Cyber Operations (OCO) capabilities either as a complement or as an alternative to traditional military capabilities. Factors that prevent CCMDs from adopting OCO capabilities into plans and operations include:

- Timelines for OCO approval that are unacceptably long;
- Waived testing or tests with limited operational realism, and;
- Lack of confirmed and well-characterized knowledge of OCO effects and potential risks.

OCO developers may waive tests because they consider testing as an unacceptable cost in terms of time and money. Waiving such tests occurs despite the fact that extended approval timelines for OCO result in part from the failure to conduct testing to rigorously characterize OCO effects and risks. What policy and guidance does exist for OCO capabilities emphasizes technical specifications, rather than the operational performance and suitability of the tool in a realistic environment. Many OCO capabilities undergo only limited testing, and seldom do any of these tests approach the rigor or realism of an operational test.

DOT&E sponsored several test events in FY16 for selected OCO capabilities at the request of Combatant Commands who had interest in advertised capabilities, but were unsure how much confidence to place in the scope and duration of the desired effects. These events demonstrated that testing of OCO capabilities can be both expeditious and low-cost. The test findings based on end-to-end employment with a cognitive cyber adversary differed greatly from the limited lab testing results. DOT&E-sponsored test results motivated improvements to OCO capability performance and reductions in undesirable second- and third-order effects.

OCO development and release authorities should conduct rigorous operational testing on OCO capabilities when the capabilities are complex and likely to be employed, and/or the risks of failure are unacceptable. DOD should take advantage of the recent advances in high-fidelity cyber ranges to perform more rigorous testing of OCO capabilities. OCO development teams should include test experts in the capability development phase to help validate requirements, focus performance metrics, and expedite a range environment that can support development, testing, and mission rehearsal.

DOT&E will continue to work with US Cyber Command, the Joint Staff, and the Services to enable rigorous OT&E of OCO capabilities. DOT&E will also stand up a cyber element within the Joint Technical Coordinating Group to perform subsequent analysis and reporting of test results to warfighters and DOD leadership.

PATH FORWARD FOR CYBERSECURITY TESTING

Improve Strategic Test Planning

DOT&E has reviewed over 800 documents related to cybersecurity OT&E in the last four years, including Test and Evaluation Master Plans, Operational Test Plans, Emerging Results, and test reports. DOT&E reviewed 240 of these documents in the last calendar year, supporting operational test and evaluation of over 100 systems.

While the quality of cybersecurity test planning continues to improve, program offices and operational test agencies need to place greater emphasis on the following areas in preparing test plans:

- Development and documentation of complete system architectures

- The means for testing non-Internet Protocol technologies
- A description of how cybersecurity tests will demonstrate active defense from attacks, measure the effectiveness of the cyber defenses, and assess the mission impacts resulting from cyber-attacks
- End-to-end testing, to include key subsystems, peripherals, and plug-ins
- Identification of resources (including cyber ranges) to be used for testing
- The role of cybersecurity service providers.

Similarly, test agencies and CCMDs require better master plans to improve the management and objectives of exercise assessments. An acquisition program's TEMP should include and describe the overall plan for cybersecurity test and evaluation. A Cyber Assessment Master Plan (CAMP) is a multi-year plan that identifies the strategic cybersecurity priorities for each CCMD or Service participating in the DOT&E Cybersecurity Assessment Program. CAMPs should focus assessment activities on critical missions that CCMDs must be able to sustain in contested cyber environments, and should motivate fight-through demonstrations in exercises or high-fidelity range events.

As the capabilities of cyber adversaries continue to grow, so must our ability to accurately portray and account for cyber threats in our OT&E and CCMD assessments. To achieve this we will work with the Combatant Commands and Services, and in particular USCYBERCOM, to develop long-term Standing Ground Rules that enable PCO activities. These standing agreements are key to the realistic threat portrayal of advanced adversaries, and offer efficiencies in the application of limited Red Team assets.

Meeting the Need for Cyber Red Teams

The DOD Cyber Strategy and DOT&E policy mandate that operational tests and exercise assessments include representative cyber-threat portrayal. Attainment of this mandate requires sufficient numbers of expert Cyber Red Team operators and supporting cyber planners to assist in the development and execution of operationally realistic cybersecurity tests, the planning and assessment of CCMD exercises and missions, and to support remediation efforts for identified vulnerabilities. The demand on DOD Cyber Red Teams has increased significantly in the past 3 years, and in the same timeframe, the private sector has hired away many members of Cyber Red Teams. As a result, Red Teams are unable to meet current DOD demand. This shortage has caused delays in cybersecurity operational testing, and reduced Red Team capabilities during some CCMD assessments. More critically, the personnel shortage has drastically increased the operational tempo of Red Team members, reducing their training opportunities to the extent that they are not able to keep pace with the tool and skill sets of advanced cyber adversaries. To address this critical situation, the Services should increase the hiring and retention of qualified Red Team personnel, and upgrade their Red Teams with new tools and training to ensure that their teams can portray advanced nation-state adversaries.

DOT&E has created two initiatives to mitigate the impact of Red Team personnel shortages and address the need for more advanced Cyber Red Team support. The PCO organizes existing DOD-certified Red Teams to support long-duration cyber activities that more closely resemble advanced persistent cyber adversaries. USPACOM and USNORTHCOM have signed Standing Ground Rules to implement the PCO construct to provide year-round cyber opposing force support for training and assessment events. The PCO has helped USPACOM find and remediate significant cyber vulnerabilities that might have otherwise gone undetected. Other Combatant Commands are developing agreements to permit PCO activities in their theaters, and DOT&E is coordinating with USCYBERCOM to develop the process and authorities for a global PCO.

DOT&E also created the Advanced Cyber OPFOR (ACO) concept to augment DOD Red Teams with more advanced nation-state capabilities. The ACO enables developers of advanced cyber capabilities and practitioners of advanced techniques to assist in planning and execution of PCO operations.

Testing Fielded Operational Systems

The cybersecurity posture of systems reflects aspects inherent to the system itself, but also aspects that reflect the surrounding operational environment, systems, and cyberspace. Operational testing of acquisition programs enables the evaluation of cybersecurity for systems in development, but fielding of the system following operational testing can result in changes to its cybersecurity posture.

Cybersecurity is a continuing and iterative process, but the DOD has no established mechanism for examining cybersecurity posture of systems following fielding. The DOT&E Cybersecurity Assessment Program examines fielded systems during CCMD and Service exercises, but most are headquarters command and control systems.

Congress recognized this cybersecurity shortfall with the FY16 NDAA Section 1647 language that directed USD AT&L to examine the cybersecurity posture of fielded systems. DOT&E is assisting this effort by providing access to all assessment results and partnerships, and identifying opportunities to conduct Section 1647 assessments in conjunction with CCMD and Service assessments and range events. To develop the Section 1647 assessment plans, the 1647 team used best practices DOT&E developed for cybersecurity operational testing and network assessments.

Resolving Legacy Problems

In conducting tests of already-fielded systems as well as new systems under acquisition oversight, DOT&E has encountered several classes of components (e.g., Programmable Logic Controllers (PLC), and Cross-Domain Solutions (CDS)), which could introduce cyber vulnerabilities to the system. Focused cybersecurity testing of such components will identify methods and analytical approaches to apply test results across multiple

acquisition programs and achieve potentially significant test efficiencies.

DOT&E provided guidance in 2015 and 2016 for testing industrial control systems that contain PLCs and CDSs. DOT&E also sponsored testing at Sandia National Laboratory, Pacific Northwest National Laboratory, and the MITRE Corporation to help identify rigorous methods for cyber testing these components, vulnerabilities, and potential mitigation strategies for developers and users of systems with these components.

Additionally, DOT&E provided guidance to the Operational Test Agencies regarding areas where cybersecurity OT&E should expand. These include:

- Non-Internet Protocol data buses and formats, to include the Military Standard 1553 bus, the Aeronautical Radio Standard 429, the Controller Area Network bus, and the 700 and 800-series avionics data buses
- Radio frequency, acoustic, radar data, and tactical datalink formats

TABLE 3. PLANNED CYBERSECURITY ASSESSMENT PROGRAM ASSESSMENTS IN FY17

EVENT TYPE	ORGANIZATION	
Exercise Assessments	U.S. Africa Command Judicious Response 2017	U.S. Pacific Command Pacific Sentry 2017
	U.S. European Command Austere Challenge 2017	USMC Large Scale Exercise 2017
Cyber Readiness Campaigns	U.S. Central Command	U.S Air Force Air Operations Centers (to be selected)
	U.S. Northern Command	U.S. Navy Amphibious Ready Group/Marine Expeditionary Group
	U.S. Southern Command	U.S. Army Reserve Command
	U.S. Special Operations Command	U.S. Army Civil Affairs Physiological Operations Command
	U.S. Strategic Command	White Sands Missile Range
	U.S. Transportation Command	

Test and Evaluation Resources

Test and Evaluation Resources

Test and Evaluation Resources

Public law requires DOT&E to assess the adequacy of operational and live fire testing conducted for programs under oversight. This assessment must include comments and recommendations on resources and facilities available for OT&E and LFT&E and on levels of funding made available for these activities. DOT&E monitors and reviews DOD- and Service-level strategic plans, investment programs, and resource management decisions so that capabilities necessary for realistic operational 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. FY16 focus areas include:

- Adjustments to the DOT&E FY16 Budget Request
- Army Support of OT&E
- Cybersecurity Red Team Personnel and Capability Shortfalls
- Threat Representation for OT&E of Space Systems
- High-Altitude Electromagnetic Pulse Test Capability
- Joint Strike Fighter Advanced Electronic Warfare Test Resources
- Point Mugu Sea Test Range Enhancements to Support OT&E of Air Warfare Programs
- Electronic Warfare for Land Combat
- Navy Advanced Electronic Warfare Test Resources and Environments
- Equipping the Self-Defense Test Ship for Aegis Combat System, Air and Missile Defense Radar, and Evolved SeaSparrow Missile Block 2 Operational Testing
- Multi-Stage Supersonic Targets
- Fifth-Generation Aerial Target
- Torpedo Surrogates for Operational Testing of Anti-Submarine Warfare Platforms and Systems
- Submarine Surrogates for Operational Testing of Lightweight and Heavyweight Torpedoes
- Missile Warning and Infrared Countermeasure Test Capability Gaps
- Threat Modeling and Simulation to Support Aircraft Survivability Equipment Testing
- Foreign Materiel Acquisition Support for T&E
- Tactical Engagement Simulation with Real Time Casualty Assessment
- Warrior Injury Assessment Manikin
- Testing in Urban Environments
- Biological Defense Testing at West Desert Test Center
- Range Sustainability and Radio Frequency Spectrum

Adjustments to the DOT&E FY16 Budget Request

Action by the House Armed Services Committee (HASC), the Senate Armed Services Committee (SASC), the House Appropriations Committee, and the Senate Appropriations Committee on the FY 2016 budget request included:

- HASC and SASC approval of the President's Budget request in the National Defense Authorization Act for FY16.
- Appropriations increases for:
  - Joint T&E ($10 Million)
  - Threat Resources Analysis ($8 Million)

The Congressional increase for Joint T&E is on track to provide six additional Quick Reaction Tests beyond the six Quick React Tests that were included in the base budget. The increase for Threat Resource Analysis improved threat realism for testing, focusing on the following areas:

- Increased cyber intelligence analyses for characterizing emerging cyberspace threat representations and threat environments
- Analysis for converging electronic warfare (EW) and cyber threats
- Standardized methods for documenting and cataloging cyber threats
- Extended support for development and validation of threat models and simulations to improve their fidelity and availability for T&E

Army Support of OT&E

Beginning with the 2014 Annual Report, DOT&E has expressed concern with the continued budget and staffing reductions at the Army Test & Evaluation Command (ATEC) and the office of the Army Test & Evaluation Executive. During the FY16 DOT&E review of the Army's T&E budget and resources, the Army indicated that there would be further staffing reductions at ATEC's Army Evaluation Center and Operational Test Command through FY19. The Army acknowledged that this may cause increased customer billing rates, the inability to conduct simultaneous operational test events, and longer timelines for the release of test reports. Substantial growth in the areas of autonomy, electronic warfare, cybersecurity, and big data analysis continue to put new demands on the Army T&E workforce and infrastructure. Current funding levels do not support growing T&E analysis capability needs. In addition to staffing reductions, the Army must contend with competition from industry as it struggles to recruit, retain, and grow an analytical and technically competent workforce. DOT&E is concerned that this may impact test planning, execution, and reporting and may result in delayed acquisition decisions. DOT&E will continue to monitor the Army T&E workforce to ensure that it is able to support and not hinder the outcomes of the Army's acquisition programs.

Cybersecurity Red Team Personnel and Capability Shortfalls

DOT&E guidance establishes data and reporting requirements for cybersecurity Red Team involvement in both operational tests of acquisition systems and exercise assessments. The demand on DOD-certified Red Teams, which are the core of the cyber opposing force (OPFOR) teams, has increased significantly in the past 3 years. In the same timeframe, the Cyber Mission Force and private sector have hired away members of Red Teams, resulting in staffing shortfalls at a time when demand is likely to continue to increase. This trend must be reversed if the DOD is to retain the ability to effectively train personnel and assess DOD systems and protective measures against realistic cyber threats. In FY16, the almost non-stop pace of events for all Red Teams challenged their ability to provide complete data sets and complete reports. Without these data and reports, network defenders and trainers will not have the critical inputs they need to develop effective mitigations or perform effective training on new procedures.

DOT&E has already seen instances in which tests were rescheduled or could not be performed as planned due to a lack of available cyber teams authorized to conduct cyber operations on live networks and enclaves. The high operational tempo of the Red Teams has reduced or eliminated opportunities for the teams to train, thereby eroding their ability to ensure their skill level is commensurate with advanced nation state cyber threats. The high operational tempo has also induced a number of experienced Red Team members to seek higher paying, less demanding jobs outside of the Department, further exacerbating the personnel shortfalls.

A number of initiatives would help address the increasing shortfall of qualified cybersecurity Red Team personnel:

- Create pay and other incentives for cybersecurity personnel – such as those afforded to other highly-trained, critical DOD personnel (e.g., pilots) – in order to retain talented Red Team operators
- Expand the number of master-level and journeyman-level Red Team operators, and develop performance-based certification standards to ensure each Red Team is manned with sufficient numbers of qualified operators
- Expand the Persistent Cyber Opposing Force (PCO) to global authorities to provide more long-duration, efficient, flexible, and threat-realistic cyber effects
- Grow Red Team capabilities and infrastructure to better and more efficiently portray advanced cyber threats, and automate the capture of required data
- Develop automated Red Team capabilities that can perform mid-level cyber exploits and identify common cybersecurity vulnerabilities

Threat Representation for OT&E of Space Systems

U.S. adversaries are working to diminish and overcome U.S. military advantage by threatening our space superiority. Although the military Services normally subject space systems to representative natural hazards and space phenomena during the course of integrated testing campaigns, they often inadequately represent a hostile wartime environment during space systems testing. Potential adversaries are relentlessly pursuing offensive space control capabilities. Therefore, the OT&E of space systems must realistically reflect the hostile threats that U.S. space systems will face, and the military Services must provide the additional resources required to conduct such OT&E.

In March 2016, DOT&E provided guidance to military Service acquisition officials and Service operational test agencies (OTAs) to ensure adequate representation of realistic threats in the OT&E of all segments of space systems, including ground control, space-borne, and user equipment. Military Service acquisition officials and OTAs must identify and address the resource and infrastructure limitations that currently constrain our ability to conduct adequate operationally realistic testing of space systems. In addition to the persistent cyber threats which could target all segments of our space systems, our space forces face electronic warfare, kinetic, and directed energy threats. OTAs must insist on current, validated threat assessments for their space systems, and must adequately and realistically represent each of these threats during OT&E.

To ensure operational realism, OTAs must employ actual threat systems when possible in OT&E. If the required threat resources are not available, then the military Service acquisition official and OTA should act in advance of OT&E to develop or procure those resources. If acquisition and employment of actual threats is not practical, would violate U.S. or DOD policy, or would introduce unmitigated and unacceptable operational, security, or safety risks, then OTAs should use realistic, accredited threat surrogates during OT&E in lieu of the actual threat system. If the actual threat system or realistic threat surrogate is not available for OT&E – despite military Service efforts to develop or procure it – then the OTA should employ accredited threat M&S.

To employ actual threat systems and threat surrogates against satellites for OT&E, in cases where risk or policy will limit adequate on-orbit testing, the military Services should fund pre-launch, thermal vacuum chamber (TVAC) testing of either first articles or non-flight, identical "test satellite" articles for cyber, electronic warfare, and directed energy threats. Representative operational crews should operate satellites being threat tested in TVAC for OT&E, using the control segment and capabilities intended for operational employment. If a Service cannot demonstrate realistic threat intensities in a TVAC, the chamber testing should be supplemented by subcomponent testing at realistic threat intensities, with analyses to correlate observed results to system-level effects.

The acquisition and test communities should leverage the space-related expertise and resources of the many U.S. space-related organizations and individuals to mitigate the infrastructure and resource limitations which currently impede DOD's ability to portray realistic space threats in OT&E. For example, test planners should make use of the expertise and resources of organizations such as NASA, the National Reconnaisance Office, the Joint Navigation Warfare Center, the Space Security and Defense Program, the Test Resource Management Center

(TRMC), and adversary tactics organizations such as the 527th Space Aggressor Squadron.

The March 2016 DOT&E guidance recommends the OTAs take immediate steps to improve their ability to adequately represent space threats by: identifying and tracking space threat representation capabilities, including their availability, location, and connectivity; identifying and prioritizing space threat representation gaps, and requesting funding to fill those gaps; documenting space threat operational and system-level concepts of operations (CONOPS) and blue system defensive CONOPS; designating OPFORs for space threat representation in OT&E; and developing M&S capabilities which support the assessment of system- and mission-level impacts of space threats.

TRMC is conducting an assessment to identify the threat environment, current T&E capabilities, and gaps in those T&E capabilities that are needed to support space system T&E requirements. This assessment will provide an estimate of resources required for acquisition programs to sustain operations in a contested space environment. DOT&E requested each Service T&E Executive to brief their plans for threat representation of space systems during the FY16 budget review process. Finally, all space system TEMPs and test plans submitted to DOT&E for approval must include the resources for a thorough representation of potential threats.

High-Altitude Electromagnetic Pulse Test Capability

Military Standard 4023 (MIL-STD-4023), "High-Altitude Electromagnetic Pulse (HEMP) Protection for Military Surface Ships," requires full-ship electromagnetic pulse (EMP) testing to support surface vessel survivability assessments. In addition, since the DDG 51 is expected to be capable of operating in an EMP environment, DDG 51 Ship Specification, Section 407 establishes requirements for DDG 51 EMP Protection. Section 407 states that during the guarantee period of the ship, the Government will conduct a full-ship EMP test to determine the performance of the ship's electronic systems under simulated EMP conditions.

The Navy currently does not have a capability to conduct a survivability assessment of a full ship subjected to EMP effects. Current Navy practice is to conduct limited testing on ship systems and sub-systems, and then extrapolate these results to the entire ship. This testing method does not provide the data needed to adequately assess full ship EMP survivability at sea in an operational mode. Existing EMP modeling and simulation capabilities provide very limited information on ship survivability, with significant uncertainties.

In FY15, the OSD Chemical Biological Radiological and Nuclear Survivability Oversight Group – Nuclear identified a full-ship EMP Threat Level Simulator (TLS) for warships as their most important test capability gap. The Tri-Service Technical Working Group, responsible for the development of MIL STD-4023, agreed that a full-ship EMP TLS is required for warship EMP threat survivability assurance. The Defense Threat Reduction Agency also determined that testing using a full-ship EMP TLS is the best approach to demonstrate ship threat-level EMP protection and mission assurance in accordance with standing Navy requirements. Currently, surface vessel acquisition programs (e.g., DDG 51) have no plans to conduct a full-ship EMP test because the Navy has no capability to do so. In order to address this testing capability shortfall, in FY16 the Naval Sea Systems Command (NAVSEA) has directed the Navy's EMP Program Office to develop a method of using a Low-Level Continuous Wave Illuminator to conduct EMP testing on one to be determined test ship. Evaluation of this trial will help determine the way forward for the development of a full-ship EMP TLS.

In conjunction with NAVSEA, the Defense Threat Reduction Agency has estimated the costs to build a full-ship EMP TLS capability to be $49 – 54 Million. Once operational, the total cost to conduct nine tests is estimated at $17.5 – 18.6 Million. Full-ship EMP TLS testing at sea will support mission assurance by providing test data for EMP modeling and realistic EMP training scenarios for ship crews. At-sea testing using this capability will demonstrate full-ship EMP survivability and support the U.S. nuclear deterrent posture. DOT&E supports all efforts to address current EMP testing shortfalls as soon as possible.

Joint Strike Fighter Advanced Electronic Warfare Test Resources

In February 2012, DOT&E identified significant shortfalls in EW test resources – in particular threat representation on the open-air ranges. This resulted in nearly $500 Million of funding for the Electronic Warfare Infrastructure Improvement Program (EWIIP). EWIIP intended to buy both open- and closed-loop threat emulators for the open-air ranges, provide upgrades to anechoic chambers and the F-35 mission data file reprogramming lab, and provide intelligence products to support the development of the threat emulators.

Significant progress has been made in some instances, while progress is lacking in other areas. The open- and closed-loop threat emulators – in addition to the lab upgrades – are key to the development, testing, and timely fielding of numerous U.S. systems that are critical for operating successfully against near-peer adversary threat systems that exist, are proliferating, or are undergoing an accelerating pace of significant upgrades. The U.S. aircraft and EW systems include the F-35, F-22 Increment 3.2 A/B, B-2 Defensive Management System, Long Range Strike Bomber, and the Next Generation Jammer for the EA-18G. The status of these EW upgrades is displayed in Table 1.

TABLE 1. RECOMMENDATIONS ON ELECTRONIC WARFARE TEST RESOURCES	
DOT&E Recommendation	**Current Status**
Develop a combination of open- and closed-loop emulators in the numbers required for operationally realistic open-air range testing of the Joint Strike Fighter and other systems beginning in 2018.	Both the open- and closed-loop efforts are underway. The open-loop systems are called Radar Signal Emulators (RSEs). EWIIP was scheduled to deliver the first 2 systems in 2016, 12 systems during 2017, and the final 2 in early 2018, for a total of 16 RSEs – in time to support F-35 IOT&E and other testing in 2018 and beyond. Acceptance and integration testing will be conducted during 2016 and 2017; this testing will establish procedures for use of the RSEs in the F-35 IOT&E and provide validation data for the accreditation of the systems for use in OT&E. Two closed-loop systems are in development but are not scheduled to be available until mid to late 2019, after completion of the planned F 35 IOT&E. The integration architecture developed for the open-loop RSE systems will provide adequate test capabilities for F-35 Block 3F IOT&E, in lieu of closed-loop systems.
Upgrade the Government anechoic chambers with adequate numbers of signal generators for realistic threat density.	Initial studies of materiel solutions to achieve realistic densities have begun. • The Navy chamber has procured improved, interim signal generation capabilities and initial test support equipment for direct signal injection capability for the F-35. Further, the Navy chamber executed F-35 electronic warfare testing for spec compliance and simulation validation in September and October 2016. The facility will introduce a much more substantial upgrade in the summer of 2017 that will allow high-fidelity replication of very high signal density threat environments. • The Air Force chamber has completed one stage of significant hardware upgrades, greatly improving its ability to replicate high signal density environments and has identified a path forward covering more extensive upgrades through 2020.
Upgrade the Joint Strike Fighter mission data file reprogramming lab to include realistic threats in realistic numbers.	A Joint Strike Fighter Program Office-sponsored study to determine upgrade requirements was completed in December 2014. It confirmed the shortfalls identified by DOT&E in February 2012, but also identified many other critical shortfalls preventing effective and efficient mission data file development and reprogramming. Unfortunately, inexplicable delays by the program since this study was completed have ensured that upgrades will not be completed in time to affect mission data file production for Block 3F IOT&E and fielded operations. Also, the program plans to procure fewer signal generators than the study recommended, further jeopardizing the program's ability to generate effective mission data in the future.
Provide Integrated Technical Evaluation and Analysis of Multiple Sources intelligence products needed to guide threat simulations.	Products have been completed and delivered, and are being used to support development of the open- and closed-loop threat radar emulators.

Due to delays and inaction by the F-35 Joint Program Office, the situation at the Joint Strike Fighter mission data file reprogramming lab has resulted in the failure to upgrade the lab before IOT&E of Block 3F capability.

DOT&E believes additional funding of $268 Million is needed for additional range infrastructure for testing, training, and readiness of U.S. aircraft and airborne EW systems. This funding would enable the test ranges and the models and simulations (that must be validated with test data) to assess the performance of U.S. systems against the key challenges of near peer threat air defense networks of the 2020s. These capabilities include: conventional radars with advanced digital signal generation and processing, networked together via advanced track fusion processing systems; multi-static radar networks; passive detection systems; and passive coherent radars. The proposed enhancements are constrained to materiel solutions that can be procured rapidly and off the shelf where possible in order to be available for testing of critical systems such as the Next Generation Jammer.

Point Mugu Sea Test 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 the integration of the Air Warfare Battle Shaping (AWBS) system and the open loop RSEs at Point Mugu Sea Test Range (STR), California. AWBS is a variant of the Air-to-Air Range Instrumentation system at the Air Force Western Test Range (WTR), Nevada, where it is essential for scoring as well as post-mission reconstruction and analysis of OT&E missions. The use of the RSEs at the STR for the F-35 IOT&E provides key operationally realistic scenarios and off-loads some of the F-35 IOT&E trials from the WTR, which can only allocate a few range periods per week for the F-35. Conducting test trials at the STR could considerably shorten the duration of F-35 IOT&E.

In 2016, Navy and Air Force personnel participated together in RSE range integration working groups throughout the year and together with DOT&E observed initial acceptance testing of the first two RSEs. Navy personnel are planning to take part in fall 2016 training for operations, maintenance, and programming of

the RSEs. Two RSEs are planned to be temporarily transferred from the Nevada Test and Training Range (NTTR) to the STR during 2017 to complete integration testing at the STR. Eventually, all 16 RSEs will be stationed at NTTR for F-35 IOT&E trials. Once those scenarios are completed, 12 RSEs will move to the STR for additional F-35 IOT&E trials.

Electronic Warfare for Land Combat

Networked mission command systems that support the commander's mission execution across the Brigade Combat Team (BCT) are a cornerstone of the Army's modernization plan. These integrated network capabilities are distributed throughout a combat formation and its support elements, from the brigade command posts down to the individual dismounted soldier. The Army intends commanders, using tactical network systems, to have the ability to transfer information such as voice, video, text, position location information, and high-resolution photographs throughout the BCT, and provide individual commanders access to information needed to complete their mission. The expanded use of radio frequency spectrum to support mission command systems with supporting data networks exposes the BCT to contemporary EW threat vectors available to a broad range of potential enemies. Recent conflicts have demonstrated the mission effects that EW can have on the modern battlefield. As the Army becomes more dependent on these sophisticated network technologies, it is critical that the developmental and operational test communities continue to identify and assess vulnerabilities of these systems. Decision makers must understand the inherent vulnerabilities, as well as the ways in which an enemy may choose to exploit and/or degrade the tactical network.

During operational testing, threat EW is part of a broader combat force that is made available to the opposing force (OPFOR) commander. When possible, the EW systems, tactics, techniques, and procedures employed by the OPFOR during test should represent those of potential adversaries. The Threat Systems Management Office (TSMO) is responsible for developing, operating and sustaining the Army's suite of threat EW capabilities. In early FY17, TSMO will complete the development of three new EW capabilities – to include an upgraded injection jammer, airborne EW payload, and GPS jammer system – demonstrating a continued commitment to providing realistic threat EW for operational test and mitigating limitations when possible. Since they support increased operational realism in testing, these developing threat test capabilities are critical to support future testing of Warfighter Information Network – Tactical Increment 2, Nett Warrior/ Rifleman Radio, Mid-Tier Networking Vehicular Radio, Manpack Radio, Joint Battle Command – Platform, and Assured Positioning Navigation and Timing.

Navy Advanced Electronic Warfare Test Resources and Environments

Capability for Realistic Representation of Multiple Anti-Ship Cruise Missile Seekers for Surface Electronic Warfare Improvement Program Operational Testing

This gap in test capability was initially identified in DOT&E's FY13 Annual Report as "Additional Electronic Warfare Simulator Units for Surface Electronic Warfare Improvement Program (SEWIP) Operational Testing." The Navy addressed it with development of a programmable seeker simulator that could represent different Anti-Ship Cruise Missile (ASCM) seekers by specifying the 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," needs to be modified such that its ERP more realistically represents the second ASCM of a dual ASCM stream raid.

The next SEWIP Block 2 OT&E is projected for FY19. This is to be followed by FOT&E on a Product Line Architecture-compliant DDG 51 with Block 2 actually integrated with the Aegis Combat System. This integration was not part of the Block 2 IOT&E. Subsequent FOT&E would be with the DDG 1000 and CVN 78 combat systems. The estimated cost to add the ERP improvement is $5 Million. The Navy has not planned for or funded this improvement.

Long-Term Improvement in the Fidelity of Anti-Ship Cruise Missile Seeker/Autopilot Simulators for Electronic Warfare Testing

This gap in test capability was initially identified in DOT&E's FY13 Annual Report due to the continued reliance on manned aircraft for captive-carry of the ASCM seeker simulators. Such simulators will be unable to demonstrate a kinematic response to electronic attack by SEWIP Block 3 nor demonstrate the effect that such kinematic responses will have on ships' hard-kill systems (e.g. missiles, guns). Manned aircraft fly too high and too slowly for credible ASCM representation and are unable to represent ASCM maneuvers. Credible ASCM representation requires a vehicle that can fly at subsonic ASCM speeds and lower altitudes than the current Learjets; can home on a platform representing a SEWIP Block 3-mounted ship, using a threat-representative radar seeker and autopilot; and can respond realistically to Block 3 electronic jamming. An approach to satisfy this requirement is to use a recoverable, unmanned aerial vehicle (UAV) that is equipped with embedded, miniaturized simulators. The UAV should be able to maneuver at ASCM

speeds and altitudes with encrypted telemetry to track seeker/autopilot responses to electronic attack. A human-controlled override capability would be required for safe operation. The remotely controlled Self-Defense Test Ship (SDTS) would tow a ship target for the UAVs to home on. SEWIP Block 3 would be mounted on the SDTS along with hard-kill systems such that the integrated hard-kill and soft-kill (i.e., SEWIP Block 3) combat system capability could be demonstrated. Currently, such testing is at the discrete combat system element level, leaving integrated combat system capability unknown.

SEWIP Block 3 IOT&E is projected for FY19. FOT&E of Block 3 integrated with the DDG 1000 combat system, as well as FOT&E with the CVN 78 combat system, should occur subsequent to the IOT&E. The cost for the development of these UAVs (with simulators and telemetry) is estimated to be approximately $120 Million for development, testing, and acquisition. The estimated unit cost of each vehicle is not expected to exceed $15 Million. The Navy has not planned for or funded this improvement.

Equipping the Self-Defense Test Ship for Aegis Combat System, Air and Missile Defense Radar, and Evolved SeaSparrow Missile Block 2 Operational Testing

The close-in ship self-defense battle space 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 weapons 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 place great stress on 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 the 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. These restrictions were imposed following a February 1983 incident on the USS *Antrim* (FFG 20), which was struck with a subsonic BQM-74 aerial target during a test of its self-defense weapon systems, killing a civilian instructor. The first unmanned, remotely controlled SDTS – the ex USS *Stoddard* – was put into service that same year. A similar incident occurred in November 2013, in which two sailors were injured when the same type of aerial target struck the USS *Chancellorsville* (CG 62) during what was considered to be a low-risk test of its combat system. This latest incident underscores the inherent dangers of testing with manned ships in the close-in battlespace.

While the investigation into the USS *Chancellorsville* incident has caused the Navy to rethink how it will employ subsonic and supersonic aerial targets near manned ships, the Navy has always considered supersonic ASCM targets a high risk to safety and will not permit flying them directly at a manned ship. The Navy has invested in a current at-sea, unmanned, remotely-controlled test asset (the SDTS) and is using it to overcome these safety restrictions. The Navy is accrediting a high-fidelity modeling and simulation (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 non-Aegis ships can be completely and affordably conducted. The Navy recognizes that 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). However, it has not made a similar investment in an SDTS equipped with an Aegis Combat System, Air and Missile Defense Radar (AMDR), and ESSM Block 2 for adequate operational testing of the DDG 51 Flight III Destroyer self-defense capabilities. The current SDTS lacks the appropriate sensors and other combat system elements to test these capabilities.

On September 10, 2014, DOT&E submitted a classified memorandum to USD(AT&L) with a review of the Design of Experiments study by the Navy Program Executive Office for Integrated Warfare Systems. The Navy study attempted to provide a technical justification to show that the test program did not require an SDTS to adequately assess the self-defense capability of the DDG 51 Flight III Class Destroyers. DOT&E found that the study presented a number of flawed justifications and failed to make a cogent argument for why an SDTS is not needed for operational testing.

On December 10, 2014, the Deputy Secretary of Defense (DEPSECDEF) issued a memorandum directing the Director of Cost Assessment and Program Evaluation (CAPE) to identify viable at-sea operational testing options that meet DOT&E adequacy requirements and recommend a course of action (with cost estimates, risks, and benefits) to satisfy testing of the AMDR, Aegis Combat System, and ESSM Block 2 in support of the DDG 51 Flight III Destroyer program. The CAPE study evaluated four options to deliver an at-sea test platform adequate for self-defense operational testing of the DDG 51 Flight III, AMDR, and ESSM Block 2 programs. Each option requires funding beginning in FY18 to ensure support of operational testing of these systems in FY22. A decision on whether to fund the procurement of the needed equipment is pending.

DOT&E continues to recommend equipping an SDTS with capabilities to support Aegis Combat System, AMDR, and ESSM Block 2 OT&E to test 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. The CAPE-estimated cost for development and acquisition of these capabilities over the Future Years Defense Program is approximately $350 Million. Of that, approximately half could be recouped after the test program completes by installing the hardware in a future DDG 51 Flight III Destroyer hull. The Navy previously agreed with this "re-use" approach in their December 2005 Air Warfare/Ship Self-Defense Test and Evaluation Strategy stating that "… upon completion of testing and when compatible with future test events, refurbish and return the test units to operational condition for re-use."

On February 10, 2016, DEPSECDEF directed the Navy to adjust funds within existing resources to procure long lead items to begin procurement of an SDTS equipped with the Aegis Combat System and AMDR. He further directed the Navy to work with DOT&E to develop an integrated test strategy for the DDG 51 Flight III, AMDR, Aegis Modernization, and ESSM Block 2 programs. DEPSECDEF required the Navy to document that strategy in a draft TEMP for those programs and submit the TEMP to DOT&E by July 29, 2016. The Navy has complied with the funding direction but has not complied with the DEPSECDEF direction to provide an integrated test strategy for those programs. Despite budgeting for the long lead AMDR components, the Navy has not programmed funding in the Future Years Defense Plan to complete all other activities and equipment required to modify the SDTS to support adequate operational testing of the self-defense capabilities of the DDG 51 Flight III, AMDR, and ESSM Block 2 in FY 2023 as planned.

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 Destroyer, CVN 78 Aircraft Carrier, DDG 51 Flight III Destroyer, LHA(R), 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 in order to address technical deficiencies as well as cost and schedule breaches, which would have postponed its initial operational capability 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 very costly (the Navy estimates $739 Million), very difficult to implement, dependent on the results of highly segmented tests, and would suffer from severe artificialities that would hopelessly 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 models and simulation capabilities for assessing the probability of raid annihilation for Navy ships.

Fifth-Generation Aerial Target

DOT&E has been investigating the need for an aerial target to adequately represent the characteristics of Fifth Generation threat aircraft in light of the emergence of threat aircraft like Russia's PAK-FA and China's J-20. The Fifth Generation Aerial Target (5GAT) study effort began in 2006 and examined the design and fabrication of a dedicated 5GAT that would be used in the evaluation of U.S. weapon systems effectiveness. 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. Also, the team built one full-scale, flight-representative wing that will be used for structural load tests and a system integration laboratory. The Department provided funding to complete the final design, tooling, fabrication and flight tests. The prototyping effort will provide cost-informed alternative design and manufacturing approaches for future air vehicle acquisition programs. This data can also be used to assist with future weapon system development decisions as well as T&E planning and investment, and will support future T&E analysis of alternative activities. It will also demonstrate reduced signature, basic aerodynamic performance, and provision for special mission systems.

Torpedo Surrogates for Operational Testing of Anti-Submarine Warfare Platforms and Systems

Operational testing of anti-submarine warfare (ASW) platforms and related systems includes the ability to detect, evade, counter, and/or destroy an incoming threat torpedo. The determination of system or platform performance is critically dependent on a combination of the characteristics of the incoming torpedo (e.g., dynamics, noise, fusing, sensors, logic, etc.). Due to differences in technological approach and development, U.S. torpedoes are not representative of many highly proliferated torpedoes, particularly those employed in anti-surface warfare by other nations. Contractor, developmental, and operational testing that is limited to U.S. exercise torpedoes will not allow the identification of existing limitations of ASW and related systems against threat torpedoes, and will result in uninformed decisions in the employment of these same systems in wartime. A January 9, 2013, DOT&E memorandum to the ASN(RDA) identifies specific threat torpedo attributes that the threat torpedo surrogate(s) must be evaluated against. A June 18, 2015, DOT&E memorandum to ASN(RDA) reiterated the need for representative threat torpedo surrogates in operational testing and emphasized understanding threat torpedo behavior, including tactics and countermeasure logic, when evaluating the adequacy of torpedo surrogates. A May 24, 2016, DOT&E memorandum

to the ASN(RDA) further emphasized the importance of resolving the surrogate shortfall in advance of evaluating the Navy Torpedo Warning System and Countermeasure Anti-torpedo Torpedo acquisitions systems. The non-availability of threat-representative torpedo surrogates will prevent adequate development and operational testing for ASW platforms and related systems, as well as adversely affect tactics development and validation of these tactics within the fleet.

Naval Undersea Warfare Center (NUWC) Division Keyport conducted a study of threat torpedo surrogates in FY14. The $480,000 study was jointly funded by the Navy and DOT&E. The completed study, dated September 4, 2015, confirmed DOT&E concerns that current torpedo surrogates have significant gaps in threat representation for operational testing and provided recommendations for improving current threat torpedo emulation. The Navy has since taken the following actions to address the gaps in threat representation of torpedo surrogates:

- NUWC Division Keyport is currently pursuing a prototype technology development project that will deliver a threat-representative, high speed, quiet propulsion system. The development of a propulsion system prototype is intended to overcome a critical gap identified in the torpedo threat surrogate capability gap analysis, discussed in the preceding paragraph. This effort is funded as an FY16 Resource Enhancement Program project at approximately $1 Million. This project is focused on the propulsion power system but will not address reducing the cavitation noise caused by the surrogate executing operationally realistic threat profiles.
- The Navy proposed development of a General Threat Torpedo (GTT) as a Resource Enhancement Program project for FY17 to provide a torpedo surrogate that better represents threat torpedos in dynamic and acoustic performance, as well as tactical logic. The $6.2 Million project will incorporate the technology developed in the high-speed, quiet propulsion system prototype and is supported by DOT&E. However, the ability of GTT to adequately support operational testing, if developed, will depend on future Navy decisions to procure sufficient quantity of GTT.

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 stratum 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 the fact 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. During the MK 50 lightweight torpedo operational test in May 1992, the Navy conducted some limited set-to-hit testing against manned submarines, which included impact against the target hull, but that practice has been discontinued.

In preparation for the 2004 MK 54 lightweight torpedo operational test, DOT&E supported the development and construction of the unmanned Weapon Set-to-Hit Torpedo Threat Target (WSTTT) using Resource Enhancement Project funding. The WSTTT was a full-sized steel mock-up of a small diesel-electric submarine, with an approximate program cost of $11 Million. As a moored stationary target, the WSTTT could not emulate an evading threat, but its use in the MK 54 operational test demonstrated the value of such a dedicated resource. Unfortunately, the Navy did not properly maintain the WSTTT and abandoned it on the bottom of the sea off the California coast in 2006. In subsequent years, the Navy was able to make some limited use of the WSTTT hulk as a bottomed target for torpedo testing.

In a separate effort, the Navy built the Mobile Anti-Submarine Training Target (MASTT), designed to serve as a full-sized threat surrogate for use in training by surface and air ASW forces. The Chief of Naval Operations initiated the program in 2010 with the goal of achieving operational capability by late 2011. An engineering assessment of the MASTT reveales the surrogate cannot be used as a set-to-hit target for torpedo testing. After 5 years and an expenditure of approximately $15 Million, the Navy has started using the MASTT in limited search training. The Navy resisted design input from the operational test community and made it clear that the MASTT was not intended to support torpedo testing.

In support of a 2010 Urgent Operational Need Statement, the Navy funded the construction of the Steel Diesel-Electric Submarine (SSSK), a full-sized, moored, set-to-hit target consisting of an open steel framework with a series of corner reflectors to provide appropriate sonar highlights. This surrogate does provide a basic sonar signature. The Navy used the SSSK as a target for the MK 54 torpedo in a 2011 Quick Reaction Assessment and 2013 FOT&E. As part of the TEMP approval for the latter, DOT&E sent a memorandum indicating that the Navy must develop an appropriate mobile target to support future MK 54 testing.

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 mobile depth changes and high speeds, autonomous, 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. Cost estimates range from under $10 Million for a towed target to over $30 Million for a full-sized submarine simulator. The Navy has not funded the additional efforts.

Missile Warning and Infrared Countermeasure Test Capability Gaps

Aircraft Survivability Equipment (ASE) is an integral part of military fixed and rotary wing platforms to provide aircraft and crew protection, and is vital to mission effectiveness in hostile environments. DOT&E and TRMC co-lead the Infrared Countermeasure Test Resource Requirements Study (ITRRS), which is designed to identify shortfalls in infrared countermeasure (IRCM) testing and develop a prioritized investment roadmap of projects to mitigate current test gaps. However, the resultant roadmap is historically underfunded to a considerable degree. The roadmap has projects to address gaps for ground-based missile plume simulators, airborne missile plume simulators, hardware in the loop test facilities, installed system test facilities, surrogate threat missiles, instrumentation suites, open air test range improvements, and threat system acquisition and storage.

One of the high priority projects on the ITRRS list is the ability to measure threat signature data for the development or improvement of the threat models for heat seeking missiles and unguided hostile fire munitions used for the T&E of ASE. These models drive a large number of T&E simulation tools listed above. The DOT&E Center for Countermeasures serves as the executing activity for a TRMC Central T&E Investment Program (CTEIP) Resource Enhancement Project – the Joint Standard Instrumentation Suite (JSIS) – in order to mitigate this shortfall as well as provide ground truth for live missile firing and hostile fire tests of IRCM systems. When available, the JSIS initial operational capability (IOC) will support Advanced Threat Warner and Department of the Navy (DON) Large Aircraft Infrared Countermeasure (LAIRCM) operational testing. JSIS IOC capability is scheduled to be delivered in early FY17. JSIS can be deployed to static live fire venues outside the continental United States, where opportunities exist to measure and collect data for threat assets that are either not available, or of insufficient quantities domestically.

However, the JSIS IOC capability only partially addresses the needs identified by the ITRRS team. For example, it will not provide the capability to measure missile attitude information for the entire missile fly out, nor will the JSIS IOC capability meet all needs related to signature collection fidelity (i.e., frame rates and resolution). Full operational capability is required to meet the needs of the Army's Common Infrared Countermeasures (CIRCM) program, Navy's Advanced Threat Warner, Air Force's LAIRCM program, and the Naval Research Laboratory's Distributed Aperture Infrared Countermeasure (DAIRCM) program. JSIS full operational capability is also needed to collect signature data in support of T&E of advanced IRCM systems, currently in development, which operate in other wavelength bands. JSIS requires an additional investment of $43 Million to provide the full operational capability needed for IRCM T&E.

Both open-air test ranges and indoor test facilities require upgrades to test the latest missile warning systems and IRCM. The open-air test range improvements include additional firing points for multi-threat environments and angular separation, upgrades to improve test efficiency, improved instrumentation, and DAIRCM jitter and atmospheric distortion measurement capability. Hardware-in-the-loop and installed system test facilities are in need of upgrades to represent the latest threats in an operational simulated environment. Additionally, these facilities are heavily utilized and in need of expansion to meet program test schedules.

Threat Modeling and Simulation to Support Aircraft Survivability Equipment Testing

Acquiring actual threat systems for widespread testing is not always possible. To address this challenge, DOT&E funded standard, authoritative threat M&S for systems T&E. These may be coupled with U.S.-built threat representations. Although threat M&S capabilities have been used in T&E for many years, they were not always accurate representations, and different M&S instantiations of the same threats often produced different results. DOT&E's objective is to improve the fidelity and consistency of threat M&S at various T&E locations while reducing overall test costs.

Throughout the T&E process, M&S representations of threat systems can be used when actual threat components are not available. Use of these M&S representations may provide a more complete assessment of system operational performance than is possible using open-air facilities alone. M&S representations of threat systems also support testing when flight safety precludes live fire testing, such as missile launches against manned aircraft. For example, test programs may only conduct 10 – 20 live missile firings events; however, using a threat M&S test program may extend those results across a broader range of test conditions (typically 20,000) with different threats, ranges, altitudes, aspect angles, atmospheric conditions, and other environmental variables affecting weapon system performance.

DOT&E developed a T&E Threat M&S Configuration Management System to implement controls and distribution management for threat M&S to ensure integrity for realistic T&E and to ensure M&S consistency of test results among various T&E regimes. This system provides mechanisms to identify and correct anomalies between a threat and its M&S representations. It also assists in controlling model configuration changes, maintains critical documentation such as interface descriptions and validation documents, and provides updated threat M&S to multiple T&E facilities for developmental and operational test needs. The T&E Threat M&S Configuration Control Board (CCB), comprised of representatives from the T&E community and intelligence organizations, prioritizes existing threat M&S developments and changes to ensure updates are provided efficiently to T&E user facilities. Requests for T&E threat M&S, anomaly reports, and change requests are managed through an interface on DOD's Secret Internet Protocol Router Network. DOT&E is in the process of expanding the breadth of control by this CCB.

During FY16, the T&E Threat Resource Activity provided standardized authoritative threat M&S to multiple T&E facilities

operated by the Army, Navy, and Air Force. The Services integrated and used this M&S to support ASE testing. DOT&E engaged the United States' closest allied nations to implement the same authoritative threat M&S for allied T&E. This allows the United States and its allies to use each other's ranges and facilities, leveraging this worldwide implementation for T&E.

DOT&E also developed and updated a threat M&S roadmap for ASE T&E to provide a comprehensive plan for future threat M&S. A good example is JSIS, which will capture threat data from live fire test events. The roadmap identifies projects to conduct systematic analyses of JSIS data to feed the development of threat-representative M&S to support U.S. and allied missile warning and infrared countermeasure systems.

DOT&E completed a threat radio-frequency (RF) M&S study which collected, analyzed, and presented information regarding the design, distribution, integration, and use of RF-related threat M&S across multiple organizations and the Services. The RF study provided a consolidated list of authoritative threat models developed by the Intelligence Production Centers (IPCs). The RF study team surveyed subject matter experts (SMEs) at the IPCs and T&E facilities to determine common issues with the implementation of M&S for T&E. The RF study provided the following list of recommendations to stakeholders for T&E M&S improvements:

1. Assist IPCs with RF threat M&S configuration management (CM) using the existing IR configuration management system
2. Maintain an up-to-date catalog of RF Threat M&S
3. Provide periodic RF threat M&S feedback between IPCs and T&E facilities
4. Sponsor and assist threat RF M&S hardware acceleration programs
5. Develop a roadmap for RF M&S threat representations and technology

DOT&E, in conjunction with TRMC, is developing a T&E threat M&S capability/investment roadmap. This comprehensive roadmap will address threat M&S investment needs to adequately evaluate airborne combat systems. The roadmap will also coordinate new development and sustainment programs to address EW test capability shortfalls. These new programs will require additional funding in the next five years.

Foreign Materiel Acquisition Support for T&E

DOT&E is responsible for ensuring U.S. weapons systems are tested in realistic threat environments, using actual threat systems to create these threat environments whenever possible and appropriate. DOT&E develops an annual prioritized list of foreign materiel required by upcoming operational tests. These requirements are submitted to the 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) to address significant threat shortfalls that affect testing for IRCM programs like CIRCM, LAIRCM, and 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. During FY16, ongoing Foreign Materiel Acquisition efforts have continued to lead to new opportunities to acquire assets for IRCM equipment testing.

DOT&E's Test and Evaluation Threat Resource Activity (TETRA) – in collaboration with the Office of the Under Secretary of Defense for Intelligence and Department of State Weapons Removal and Abatement – has made significant progress in raising awareness of the critical shortfalls of MANPADS for T&E. TETRA briefed the National Security Council (NSC) Counter-Terrorism Task Force and the MANPADS Task Force. These efforts led to NSC tasking the organizations responsible for developing sources, which in turn led to the creation of more opportunities for acquisition to meet T&E requirements.

There is an extreme shortfall of foreign materiel for operational testing, particularly MANPADS and anti-tank guided missiles. This shortfall has become critical, as exemplified in the U.S. Special Oeprations Command's 2015 Joint Urgent Operational Needs Statement. 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 very lengthy and unpredictable, making it difficult to identify appropriate year funding. DOT&E recommends adding a staff position within the Joint Foreign Materiel Program Office dedicated to developing and executing foreign materiel acquisition opportunities for operational testing. The funding requirement for this staff position is $300,000 per year. DOT&E also recommends a no-year or non-expiring funding line for foreign materiel acquisitions, funded at a level of $10 Million per year.

Tactical Engagement Simulation with Real-Time Casualty Assessment

Realistic operational environments and a well-equipped enemy intent on winning are fundamental to the adequate operational test of land and expeditionary 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. Simulated force-on-force battles must contain realism to cause commanders and Soldiers to make tactical decisions and react to the real-time conditions on the battlefield. 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 based on the lethality and survivability characteristics of both the systems under test and the opposing

threat systems. TES/RTCA systems must 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 in the test event as an integrated part of the test control and data collection architecture. Post-test playback of these data provides a critical evaluation tool to determine the combat system's capability to support soldiers and marines as they conduct combat missions.

In FY15, the Army initiatied the Integrated Test Live, Virtual, and Constructive Environment (ITLE) project to address the known TES/RTCA capability shortfalls and future Army requirements. There was little progress made on the ITLE project in FY16; consequently, funding for the effort has been realigned. DOT&E is concerned that because of delays, ITLE may not be able to accomplish the TES/RTCA upgrades needed to support upcoming operational testing of the Army's major modernization programs.

The Marine Corps' current force-on-force training system, the Instrumented Tactical Engagement Simulation System II (ITESS II), does not support combat vehicle engagements. The Marine Corps Operational Test and Evaluation Activity had planned a substantial upgrade of ITESS II beginning in FY16 to support the upcoming operational testing of combat vehicles, but it was unable to secure the required funding. The estimated cost of the ITESS II upgrade was $9 Million.

DOT&E, beginning with its 2002 annual report, has emphasized the need for continued investment in TES/RTCA capabilities. Further, DOT&E requires these capabilities for testing systems such as Amphibious Combat Vehicle, Bradley and Abrams Upgrades, Armored Multi-purpose Vehicle, AH-64E Block III, Joint Light Tactical Vehicle, and Stryker Upgrades.

Warrior Injury Assessment Manikin

DOT&E has been the advocate for an Army-led project to enhance the Department's ability to assess injuries from under-vehicle IED and mine blasts by creating a military-specific anthropomorphic test device (ATD) and associated injury criteria tailored to the underbody blast environment. The need for this was first documented in 2009 as a result of a SECDEF-directed evaluation of the Department's underbody blast modeling and simulation capabilities, and the need has been validated repeatedly since then. The evaluation concluded that automotive crash test dummies used in LFT&E and the consequent injury criteria – designed and developed for forces and accelerations in the horizontal plane, as seen in automotive frontal impact-induced injuries – were not adequate to assess the effects of the forces and accelerations in the vertical plane typically seen in combat-induced unerbody blast events. To address this limitation in 2010, DOT&E championed initial funding for the Army to lead the effort that became known as the Warrior Injury Assessment Manikin (WIAMan) project. Under this project, the Army initiated critical biomechanical research and the anthropomorphic test devices (ATD) development program to increase DOD's understanding of the cause and nature of injuries incurred in underbody blast combat events.

The science and technology (S&T) and ATD development aspects of the project are being executed by the Army Research Laboratory's WIAMan Engineering Office (WEO). In 2015, the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)) determined that the WIAMan project is an Acquisiton Category II program of record and, as such, ASA(ALT) has determined that the Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) will be responsible for the project's execution post Milestone B. The WEO continues to accomplish its technical goals for S&T and ATD development research, but as a result of the acquisition approach, the WEO is now also supporting PEO STRI, as required by a memorandum of agreement signed by the Army Research, Development, and Engineering Command and PEO STRI. However, no additional personnel or funding has been procured for the WEO to address these additional duties. This has the potential to tax the resources of the WEO and shift the emphasis of the subject matter experts within WEO from S&T to acquisition. The planning and execution of the formal acquisition process is behind schedule, while incurring significant overhead costs.

In FY15, the Assistant Secretary of Defense for Health Affairs committed S&T funding for the program post Milestone B to ensure critical injury biomechanics research is completed. However, the Army had not provided a similar committment to fund this program's acquisition. Consequently, in FY15, DOT&E supported fully funding the acquisition side of the project. As a result, the Army was directed to allocate $16.2 Million over FY17 and FY18 "to continue RDT&E activities and further the acquisition process." However, the critical funding required to continue and complete the execution of this program past FY18 has not yet been resolved.

Some within the Army have questioned whether DOD still needs a combat-specific injury assessment capability. In the view of DOT&E, it is entirely appropriate for DOD, and in particular for the Army, to accord the same high priority to testing and verifying the protection provided to soldiers by their combat vehicles that the commercial automotive industry accords to testing and verifying the protection provided to the U.S. public by their automobiles.

Testing in Urban Environments

Operations in urban environments present unique challenges to the military Services and their equipment. Degraded mobility, maneuver, communications, and situational awareness; a large civilian presence; the risk of collateral damage; reduced stand-off distances; and unique threat profiles are some of the conditions present during urban operations. These challenges – and a world population that is becoming increasingly urban – reinforce the requirement that systems be tested in realistic urban environments. DOT&E, beginning with its 2002 annual report,

has been highlighting the need for larger and more complex urban test environments.

With the cancellation of the Army's Joint Urban Test Capability in 2015, the long-standing urban environment operational and developmental test capability shortfall is not being addressed. DOT&E recommends that the Army revisit the urban test capability requirement to capture current and future T&E requirements, and develop a new approach to addressing this shortfall.

Biological Defense Testing at West Desert Test Center

In late FY15, DOD suspended the production of and testing with biological select agents and toxins (BSAT) and derivatives of BSAT materials at the West Desert Test Center (WDTC) on Dugway Proving Ground, Utah. On October 16, 2015, the Secretary of the Army approved the reassignment of the WDTC Life Science Division to the Edgewood Chemical Biological Center (ECBC) in Edgewood, Maryland. On July 1, 2016, ECBC took control of the Life Science Division and changed its name to the WDTC Biological Testing Branch (BTB). In August 2016, the Army completed a review of safety and surety protocols and procedures at WDTC and approved the resumption of field test activities using biological simulants that are safe for open-air use. The Army requested a withdrawal of the Dugway Proving Ground Biosafety Level Three (BSL 3) Centers for Disease Control and Prevention (CDC) permits and plans to apply for a new BSL 3 CDC permit for WDTC BTB facilities. The Army's current projection for achieving WDTC BTB BSL-3 certification is late 2019. WDTC and the BTB have unique biological testing facilities and capabilities that are essential to operationally realistic T&E of biological defense systems. DOT&E continues to monitor the requirement for BSL-3 and work with the Army to develop mitigation plans until the full biological test capability comes back online.

Range Sustainability and Radio Frequency Spectrum

Adequate land-, air-, and sea-space are critical for DOD's capability to test weapon and associated systems in operationally realistic conditions under which performance data can be collected, public safety can be ensured, and physical security and cybersecurity can be protected. Range sustainability is the preservation of, and advocacy for, those spaces. Sustainability is challenged by encroachment factors such as incompatible infrastructure, urban development, natural resource constraints, and frequency spectrum losses. Each of these factors may limit the use of land-, air-, and sea-space for DOT&E to execute its operational test and evaluation mission.

Despite DOT&E's best efforts there are a number of continuing challenges to both preserving current test capabilities and ensuring that there are avenues available to support testing of future weapon systems. Future testing will require expanded footprints, networked sensors, and advanced range capabilities which address complex cybersecurity environments.

Two primary strategies are essential to protect range space and test capabilities. The first is data-driven compatibility analysis – based on weapon system performance requirements – to ensure that evaluations conducted are credible. The second is outreach to other Federal agencies, state and local governments, and non-governmental organizations, to address issues early and to develop solutions that benefit all participants.

A recurrent theme in the evaluations performed for range sustainability is that while most of the challenges have either no compatibility risks or have risks that can be mitigated, there are a few cases that do have adverse impacts on test capabilities. Ongoing vigilance is required to ensure that DOT&E knows about projects that may pose risks to operational testing capabilities, now and in the future, and that DOT&E is in a position to mitigate risks early in the review cycle.

Current major areas of concern are:

- Energy infrastructure projects
- Natural resource protections
- National monuments and marine sanctuaries
- Frequency spectrum reallocation
- Foreign investment
- Privately owned and operated drones

Energy infrastructure projects can adversely affect instrumentation essential for obtaining data on weapon systems being tested, and can create physical obstructions that limit the use of test space. Under the provisions of Public Law 111 383, Section 358, as amended by Public Law 112 81, Section 331, DOD conducts compatibility evaluations of energy infrastructure to ensure that adverse impacts to national security can be identified and mitigated. DOT&E is an active participant in the DOD process to ensure that test capabilities required for realistic testing of current and future weapon systems are available for use. The process enables review and approval or disapproval of projects based upon risk to operational test capabilities. However, the tools available to the Department to require mitigation of problematic aspects of proposed energy infrastructure projects are not currently sufficient to prevent all adverse impacts to test capabilities. The DoD can only directly control development on DOD owned, leased, or withdrawn property. In all other circumstances, the Department must rely on a mix of authorities available to other Federal agencies, or to state and local government intervention. Yet these authorities have proven to be problematic in certain instances. For example:

- DOD relies on the FAA obstruction to flight notification requirements in section 44718 of title 49, U.S. Code (49 USC 44718), to receive notification of energy infrastructure projects. However, the statute gives DOD no authority to evaluate structures not covered by 49 USC 44718, nor does it prescribe any mechanism for DOD to ensure that unacceptable risks do not occur. The FAA does not currently have the authority to withhold approval for projects that do not pose a hazard to flight safety, but are objectionable to DOD. DOT&E has been researching options by which DOD can object to renewable energy and associated infrastructure projects on the basis of adverse impact to national security and will continue to explore and shape policies and procedures that can be

used to ensure that required operational test capabilities are available for use.

- Developers proposing energy infrastructure projects on Federal land must go through the National Environmental Protection Act (NEPA) process. While DOD can be a participating agency on those projects which have the potential to constrain the conduct of operational testing, current rules do not allow the Department to object to projects that would impact its ability to satisfy reasonably foreseeable future testing requirements; the processes are focused on consideration of documented requirements. As mentioned earlier in this report, the Department is confident that the expanded capabilities of new weapon systems will drive operational testing requirements for test spaces with larger footprints than are currently available. DOT&E will work with Federal agencies to ensure that NEPA procedures provide for consideration of reasonable and foreseeable actions to support mid- and long-term weapon systems test requirements.
- For many of the test ranges, particularly those in the Southwest, Federal land is withdrawn for specified periods of time. DOT&E conducts test missions using airspace that is restricted as regulatory, special use airspace through the FAA, and sea-space that is designated as non-regulatory, special use air-space by the FAA. For land withdrawal extensions, test ranges prepare range planning documents to support continued withdrawal. These plans integrate planned test requirements for the individual test range; however they may not adequately consider requirements for integrating requirements with those of other test ranges to allow for combined land and air resources to support future tests of longer range and networked weapon systems. DOT&E will investigate mechanisms to provide for sufficient air- and land-space to support this expanded envelope testing.

The Department requires that its weapon systems be capable of operating in a wide variety of environments, and its ranges are designed to allow testing and training across these environments. However, DOD ranges contain environmentally sensitive flora and fauna, including those that migrate from external disturbed areas. The U. S. Fish and Wildlife Service list of threatened and endangered species and Reports to Congress on the Recovery of Threatened and Endangered Species indicate that the total number of U.S. plant and animal species that are identified as threatened or endangered has more than doubled from 581 in 1990 to 1604 as of September 2016. The growing list of threatened and endangered species, and their proximity to DOD ranges, places significant pressure on the Department to safeguard areas where protected species and habitat exist while testing weapons systems in operationally realistic environments. The DOD challenge is to integrate weapons systems testing needs with environmental restrictions that prevent use of areas designated for operational testing. Accordingly, DOT&E will actively engage other Federal, state, local, and private organizations to reach mutually agreeable arrangements on means to accommodate test disturbances while conserving natural resources.

The declaration of a new or expanded national monument and marine sanctuary has the potential to encroach on existing test ranges, or to preclude expansion of ranges in the future. The challenge is to allow for testing activities, which require vehicle and personnel transit on or above these areas and which may result in damage from test objects, while preserving natural resources. To ensure that use of these areas to satisfy national security requirements, to include test and evaluation, is not precluded, it is essential that the proclamations establishing national monuments and marine sanctuaries include specific language permitting continued DOD use.

Frequency spectrum is required to conduct test operations, and is vital for controlling autonomous vehicles, sending and receiving test data, and ensuring range safety. However, there are continuing pressures to repurpose spectrum currently allocated to DoD to support national broadband expansion. The challenge is how to accommodate approved spectrum repurposing while retaining required spectrum for use by DoD when it is needed. The strategies employed include working to preserve essential frequency spectrum currently available for DoD use and supporting research initiatives for technologies and equipment that makes the most efficient use of available spectrum. DOT&E will continue to monitor frequency spectrum issues related to operational test requirements, review policies and procedures ensuing from DoD's Spectrum Strategy, and engage in other issues that may adversely impact use of spectrum for T&E.

Foreign investment in resources and facilities proximate to test ranges may create undesirable opportunities for intelligence gathering on weapons capabilities. Foreign purchases of U.S. companies that provide test and telemetry equipment used on our ranges and test facilities may likewise create operational security challenges. DOT&E reviews projects referred by the Committee on Foreign Investment in the United States (CFIUS) for possible security risks for foreign data collection. During the past twelve months, 207 cases – with more than 3,500 supporting documents – were reviewed. Sixteen cases were assessed to pose a potential threat to test or training ranges and required further investigation and development of mitigation strategies. However, as currently constituted, CFIUS provides only for the review of projects voluntarily submitted by applicants; there is a potential risk that other, unrecorded transactions may create operational security vulnerabilities. DOT&E will exercise vigilance in this area to ensure that data from weapon system tests are not compromised.

The advent of inexpensive drones, and the institution of public licensure policies, creates potential risks from drones intruding into sensitive DoD airspace, either inadvertently or with malicious intent. This creates safety of flight dangers, and opens potential adversaries to collect information on weapons characteristics. At present, DoD has very few legal avenues to prevent such intrusions, or to act when intrusions are detected. DOT&E will actively work within the Department and with other Federal agencies to ensure that adequate procedures are in place to ensure that drones do not create impediments to effective operational testing.

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 submit these products to the appropriate Service or Combatant Command 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 through 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 has two test methods available for customers: the Joint Test and the Quick Reaction Test (QRT). Additionally, a Special Project is available for command directed or customer funded test projects.

The Joint Test is, on average, a two-year project, preceded by a six-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 periodic feedback and useable, interim test products. The JT&E Program charters two new Joint Tests annually. The JT&E Program managed seven Joint Tests in FY16 that focused on the needs of operational forces. Projects annotated with an asterisk (*) were completed in FY16:

- Digitally Aided Close Air Support (DACAS)
- Four Pillars of Integrated Air and Missile Defense (4-PI)*
- Joint Advanced Zensor to Zhooter (JAZZ)
- Joint-Base Architecture for Secure Industrial Control Systems (J-BASICS)*
- Joint-Fiber Laser Mission Engagement (J-FLaME)*
- Joint Pre-/Post-Attack Operations Supporting Survivability And Endurability (J-POSSE)
- Joint Tactical Air Picture (JTAP)*

QRTs are intended to solve urgent issues in less than a year. The program managed 18 QRTs in FY16:

- Civil Military Engagement Development-Joint Targeting/ Non-Lethal (CMED-JT/NL)*
- Cyber Degraded Training (CDT)
- Homeland Underwater Port Assessment Plan (HUPAP)
- Joint Accelerated Collaborative Targeting (J-ACT)
- Joint Air Operations Center Command and Control in a Contested Degraded Environment (JADC)
- Joint Biological/Radiological Mortuary Affairs Contaminated Remains Mitigation Site (JBRM)*
- Joint-Cyber Synchronization into Air Tasking Order (J-CAT)*
- Joint Cyber Integration of DOD Information Network Operations (J-CID)
- Joint Intelligence Surveillance and Reconnaissance in a Contested Area (JICA)*
- Joint Interagency-Cyber Enhanced Detection and Monitoring (JI-CEDM)
- Joint Laser Anti-Satellite Mitigation Mission Planning (J-LAMMP)*
- Joint Personnel Recovery Information Digital Exchange (J-PRIDE)
- Joint Sniper Performance Improvement Methodology (JSniPIM)*
- Joint Talon Thresher Theater Integration (JT3I)
- Joint Target Development: Target System Analysis Standards and Procedures (T-SaP)*
- Joint Unmanned Aerial Vehicle Swarming Integration (JUSI)*
- Theater Joint Land Forces Component Commander Common Operational Picture (T-COP)*
- Optimization of Social Media and Open Source Information Support (OSMOSIS)

As directed by DOT&E, the program executes Special Projects that address DOD-wide problems. Special Projects generally address emergent issues that are not addressed by any other DOD agency, but that need a rigorously tested solution. The program managed two Special Projects in FY16:

- Joint and Community Attributes-Based Access Control Authorization for Transportation Services (J-CAATS)*
- Joint National Capital Region Enhanced Surveillance Tactics, Techniques, and Procedures (J-NEST)

JOINT TESTS

DIGITALLY AIDED CLOSE AIR SUPPORT (DACAS)

Sponsor/Start Date: Joint Staff J6/February 2016

Purpose: To develop, test, and evaluate standardized TTP so Joint Terminal Attack Controllers (JTAC), Joint Fires Observers (JFO), and Close Air Support (CAS) aircrew can realize the advantage of DACAS capabilities, including shared situational awareness, increased confidence prior to weapons release, and improved kill chain timeliness.

Products/Benefits:
- Enable JTAC and aircrew to access existing networks and exploit DACAS benefits
- Decrease human input error through machine-to-machine data exchange
- Instill confidence prior to weapons release

FOUR PILLARS OF INTEGRATED AIR AND MISSILE DEFENSE (4-PI)
(CLOSED AUGUST 2016)

Sponsor/Start Date: U.S. European Command (USEUCOM), U.S. Army Space and Missile Defense Command, and U.S. Air Forces Europe-Air Forces Africa/August 2014

Purpose: To develop and test TTP that enable sharing of existing sensor data to enhance the concurrent execution of integrated air and missile defense (IAMD) active defenses, passive defenses, attack operations, and battle management command, control, communications, and intelligence (BMC3I) in response to ballistic missile attacks across Combatant Command areas of responsibility (AOR) in a coalition environment.

Products/Benefits:
- TTP on sharing data to support concurrent offensive and defensive counter-air operations in order to better defend against, and mitigate the effects of, a ballistic missile attack across Combatant Command boundaries with coalition partners (USEUCOM, U.S. Central Command (USCENTCOM) and NATO)
- Enabled cross-AOR data sharing of Joint Automated Deep Operations Coordination System information, which allows communication of USEUCOM priorities and real-time engagement monitoring and established persistent capability that can be easily turned on when operational need arises
- Developed cross-AOR attack operations Joint Planning Team construct and Collaborative Planning Environment TTP, which serves as a baseline for Joint Staff cross-AOR planning orders to resolve potential cross-AOR gaps and seams
- Standardized BMC3I capabilities and Global Command and Control System – Joint configurations to maximize efficiencies, support command and control collaboration, and enable sharing of IAMD sensor data
- Enhanced civil-military passive defense/missile warning process for NATO nations, extensible to other Shared Early Warning System partners

JOINT ADVANCED ZENSOR-TO-ZHOOTER (JAZZ)

Sponsor/Start Date: U.S. Pacific Command (USPACOM)/ August 2015

Purpose: To develop, evaluate, and validate TTP to more efficiently and effectively gain and maintain battlespace awareness through integration of rapidly developed capabilities to support combat operations in anti-access/area denial environments.

Products/Benefits:
- A sensor to shooter TTP that enables sharing of advanced sensor and National-Tactical Integration (NTI) data between 5th and 4th generation fighters, resulting in increased situational awareness, improved engagement opportunities, and better utilization of weapon systems
- Documented roles and responsibilities for the Operational Air Component Commander and the tactical datalink network designers to plan and execute integration of advanced sensors and NTI into any theater of operations

JOINT-BASE ARCHITECTURE FOR SECURE INDUSTRIAL CONTROL SYSTEMS (J-BASICS)
(CLOSED DECEMBER 2015)

Sponsor/Start Date: U.S. Cyber Command (USCYBERCOM)/ February 2014

Purpose: To develop, test, and evaluate Advanced Cyber Industrial Control System (ACI) TTP to improve the ability of industrial control system (ICS) network managers to detect, mitigate, and recover from nation-state cyber-attacks.

Products/Benefits: ACI TTP and related ICS network manager training packages provided the following capabilities:

- Resiliency to DOD ICS networks and IT infrastructures
- Increased Command confidence resulting from the ACI TTP, for ICS network managers to: detect nation-state presence in DOD ICS networks, mitigate damage to underlying processes supported by the ICS in the event of a cyber-attack, and quickly recover the ICS network to be mission capable
- Policy and implementation guidance recommendations for ICS network security to Commander, USCYBERCOM and the Assistant Secretary of Defense, Energy, Installations and Environment
- Training package and cyber exercise scenarios that provide ICS operators an understanding of the TTP and its practical application

JOINT-FIBER LASER MISSION ENGAGEMENT (J-FLAME)
(CLOSED AUGUST 2016)

Sponsor/Start Date: Naval Surface Warfare Center, Dahlgren Division/August 2014

Purpose: To develop and test TTP that integrate emerging directed energy laser (DEL) capabilities into joint fires and force protection missions.

Products/Benefits: Improved DEL Operations in the Joint Battlespace:

- Integrated DEL systems into joint fires planning and execution, focusing on actions required for deconfliction, integration, synchronization, and safety of these systems in a complex and congested battlespace

- Addressed force protection mission requirement against asymmetric threats (unmanned aerial systems and small boats), focusing on unique aspects of DELs that impact the joint battlespace (for example, new coordinating measures, Laser Engagement Zones, and Laser Operating Areas) that personnel at both operational and tactical levels need to consider
- Provided laser dwell time versus range graphs for various DEL power classes and mission sets to assist operators to effectively and efficiently employ DELs
- Provided information on risks associated with DEL reflected energy and risk estimate distances for use in minimizing risks to friendly troops in close proximity to DEL targets
- Provided recommendations to assist the Services in DEL system development and acquisition, as well as with integrating DELs into the battlespace common operational picture

JOINT PRE-/POST-ATTACK OPERATIONS SUPPORTING SURVIVABILITY AND ENDURABILITY (J-POSSE)

Sponsor/Start Date: U. S. Strategic Command (USSTRATCOM)/February 2015

Purpose: To develop, test, and evaluate TTP to provide joint operators the ability to survive an electromagnetic pulse (EMP) event in order to ensure continuous mission functionality.

Products/Benefits:
- Standardized procedures that provide overarching guidance for required actions before and after an EMP event in order to survive it
- Results inform future resourcing decisions regarding physical enhancements
- Extensible to other mission systems potentially vulnerable to EMP effects

JOINT TACTICAL AIR PICTURE (JTAP)
(CLOSED FEBRUARY 2016)

Sponsor/Start Date: USPACOM/February 2014

Purpose: To develop, evaluate, and validate TTP to improve the joint air picture and engagement opportunities, which decrease the risks of preemptive hostile attack and fratricide.

Products/Benefits:
- Developed TTP to reduce radio frequency network loading by moving participants to internet protocol architectures resulting in a greater number of timeslots available for participants
- Developed Multi-Service IAMD TTP to enhance integrated fire control/between ground sensors and air shooters for defensive counter-air engagements thereby increasing the number of available tracks containing fire control quality data

---

QUICK REACTION TESTS

CIVIL MILITARY ENGAGEMENT DEVELOPMENT-JOINT TARGETING/NON-LETHAL (CMED-JT/NL)
(CLOSED MAY 2016)

Sponsor/Start Date: U.S. Army Civil Affairs & Psychological Operations Command (Airborne)/February 2015

Purpose: To develop, test, and validate civil-military engagement development (CMED) TTP to improve the non-lethal aspects of the joint targeting process. To increase the Combatant Command staff's ability to integrate civil information and analysis products into the joint targeting cycle and improve basic, intermediate, and advanced joint target folder development, entity-level development, prioritization (phase two of the joint targeting process), and no strike and restricted target lists.

Products/Benefits:
The CMED-JT/NL-developed TTP provided Commanders the ability to integrate civil military information into phase two of the joint targeting process.

CYBER-DEGRADED TRAINING (CDT)

Sponsor/Start Date: USPACOM/Feb 2016

Purpose: To develop, test, and evaluate concept of operations (CONOPS) and TTP that will address the characteristics of cyber-degraded training environments as well as how to select, employ, and overcome these capabilities relative to factors such as military training objectives, Commander's risk tolerance, threat representation, and exercise complexity

Products/Benefits: TTP & CONOPS
- TTP and CONOPS that provide USPACOM with standardized, comprehensive tools to support Commanders at all levels with the ability to function in a cyber-degraded environment
- CONOPS identifies the different types of degraded cyber environments that can be created and options of how trainers, planners, and subject matter experts can employ them for training and exercise activities

HOMELAND UNDERWATER PORT ASSESSMENT PLAN (HUPAP)

Sponsor/Start Date: North American Aerospace Defense Command (NORAD)-U.S. Northern Command (USNORTHCOM)/June 2015

Purpose: To develop and evaluate TTP for underwater port assessments to include specific details about the roles and responsibilities of the stakeholders; identify available local, state, and federal force multipliers; provide data collection, compilation, and sharing guidance; and identify gaps in response considerations.

Products/Benefits:
- Comprehensive TTP that prescribes the standards and activities necessary to gather interagency underwater port

information for homeland ports and internal waterways in preparation for a catastrophic event
- Assists port authorities when developing an Interagency Underwater Port Assessment that will provide DOD and interagency partners with preparation, response, and recovery information necessary to reopen ports and waterways

JOINT ACCELERATED COLLABORATIVE TARGETING (J-ACT)

Sponsor/Start Date: USSTRATCOM/February 2016

Purpose: To develop and assess a CONOPS that uses an accelerated intelligence processing, exploitation, and dissemination (PED) process that streamlines intelligence analysis and coordination with targeteers to increase the speed of potential target object classification and verification.

Products/Benefits:
- A PED CONOPS that accelerates imagery analysis, target object classification, and target verification.

JOINT AIR OPERATIONS CENTER (AOC) COMMAND AND CONTROL (C2) IN A CONTESTED DEGRADED ENVIRONMENT (JADC)

Sponsor/Start Date: USPACOM/February 2016

Purpose: To develop TTP to support joint AOC distributed planning, execution, and assessment in a contested, degraded, and operationally limited environment by distributing authorities and effectively employing airpower and supporting forces.

Products/Benefits:
- TTP that enables delegation of operational airpower C2 from the joint AOC to subordinate Commanders
- Delegation of authorities that empower leaders at lower echelons of command to continue execution of the Commander's intent with limited loss of operational or tactical initiative

JOINT BIOLOGICAL/RADIOLOGICAL MORTUARY AFFAIRS CONTAMINATED REMAINS MITIGATION SITE (JBRM)
(CLOSED SEPTEMBER 2016)

Sponsor/Start Date: U.S. Army Quartermaster School/June 2015

Purpose: To develop TTP for the safe processing, identification, and preparation for evacuation of biologically or radiologically contaminated human remains. To improve the Mortuary Affairs Contaminated Remains Mitigation Site effectiveness and safety for operational mission requirements, including hazard mitigation, preserving forensic evidence, establishing chain of custody, supporting positive identification processes, and preparing remains for evacuation.

Products/Benefits:
- Updates to Army and joint doctrine, with primary focus on Army Techniques Publication 4-46.2, Mortuary Affairs Contaminated Remains Mitigation Site Operations, as related to biological or radiological contaminated human remains
- Verified data and tools to the mortuary affairs community for use in both USNORTHCOM homeland defense missions and DOD's worldwide contingency operations
- Creation of the Mortuary Affairs Contaminated Remains Mitigation Site Tactical Handbook

JOINT-CYBER SYNCHRONIZATION INTO AIR TASKING ORDER (J-CAT)
(CLOSED FEBRUARY 2016)

Sponsor/Start Date: USPACOM/October 2014

Purpose: To develop TTP for Combatant Commands to direct regionally synchronized and globally deconflicted cyber fires and integrate offensive cyberspace operations into air tasking order development and execution processes to synchronize cyber operations with other joint fires and provide coordination and deconfliction of global cyber operations with USCYBERCOM's cyberspace tasking order.

Products/Benefits: An operational TTP for incorporation of cyber fires and effects into the Combatant Command's air tasking order and USCYBERCOM's cyberspace tasking order.

JOINT CYBER INTEGRATION OF DOD INFORMATION NETWORK OPERATIONS (J-CID)

Sponsor/Start Date: USPACOM/June 2015

Purpose: To develop a CONOPS and TTP for the Combatant Commands' Joint Cyber Centers that fully integrates the organization, authorities, and capabilities of DOD Information Network commands in support of joint theater cyber operations.

Products/Benefits: CONOPS and TTP that provide best practices for the support of regional operations, situational understanding, and decision making for cyberspace operations between regional DOD Information Network commands and Joint Cyber Centers.

JOINT INTELLIGENCE SURVEILLANCE AND RECONNAISSANCE IN A CONTESTED AREA (JICA)
(CLOSED FEBRUARY 2016)

Sponsor/Start Date: 25th Air Force/October 2014

Purpose: To develop TTP that improve information flow from national intelligence, surveillance, and reconnaissance (ISR) capabilities to operational and tactical-level users in an anti-access/area denial environment.

Products/Benefits: TTP that establish a 'trigger' for AOC intelligence personnel to request ISR support from national assets by defining and identifying the level of degradation impairing organic theater and tactical ISR capabilities and instructions on how to efficiently request ISR support.

JOINT INTERAGENCY-CYBER ENHANCED DETECTION AND MONITORING (JI-CEDM)

Sponsor/Start Date: Joint Interagency Task Force South (JIATFS)/June 2016

Purpose: To develop TTP to coordinate and utilize interagency cyber domain support from DOD, law enforcement, and intelligence community partners in the conduct of detection and monitoring (D&M) missions.

Products/Benefits: CONOPS and TTP for the timely and efficient use of internal and external cyber resources to support JIATFS requirements, eliminate redundancy, and maximize the impact of cyber domain information in conducting D&M operations

JOINT LASER ANTI-SATELLITE MITIGATION MISSION PLANNING (J-LAMMP) (CLOSED OCTOBER 2015)

Sponsor/Start Date: U.S. Air Force Warfare Center/June 2014

Purpose: To develop TTP to quantify the anti-satellite (ASAT) risk to low-earth and highly elliptical orbit satellites using optical systems and requiring operational and tactical methods to mitigate existing low-power laser threats. The TTP incorporates payload susceptibility information into mission planning to mitigate laser ASAT threats at both the operational and tactical levels of space operations.

Products/Benefits:
- Ability to incorporate payload susceptibility information into the mission planning processes at operational and tactical levels in response to laser ASAT threats
- Formalized established communications processes within the Joint Space Operations Center (JSpOC) and between the JSpOC and subordinate units

JOINT PERSONNEL RECOVERY INFORMATION DIGITAL EXCHANGE (J-PRIDE) (CLOSED OCTOBER 2016)

Sponsor/Start Date: Joint Staff J7/June 2015

Purpose: To develop TTP to pass critical information across existing hybrid networks between isolated personnel, recovery forces, and command and control nodes during joint personnel recovery (PR) missions.

Products/Benefits:
- Formalized mission critical information across operational and tactical PR nodes to enhance mission effectiveness and increase survivability
- Provided a standardized 15-line PR message format across joint forces

JOINT SNIPER PERFORMANCE IMPROVEMENT METHODOLOGY (JSNIPIM) (CLOSED JANUARY 2016)

Sponsor/Start Date: U.S. Marine Corps Weapons Training Battalion/October 2014

Purpose: To develop TTP and training methodologies to improve sniper teams' ability to identify, range, lead, and engage human motion-type moving targets at distances of 300 to 1,000 meters at speeds of up to 10 miles per hour.

Products/Benefits: Developed a sniper-carried memory aid and a training support package with learning objectives, an instructor guide, and student handouts that:
- Enable instructors to teach, test, and qualify students on engaging moving targets at distances of 300 to 1,000 meters at speeds of up to 10 miles per hour
- Update curriculums for all DOD sniper schools

JOINT TALON THRESHER THEATER INTEGRATION (JT3I)

Sponsor/Start Date: USPACOM/October 2015

Purpose: To develop a CONOPS that clearly defines the optimal operating parameters of the Talon THRESHER system and standardizes user operating procedures to enhance air domain awareness within theater command and control nodes, joint AOCs, and national-tactical integration cells.

Products/Benefits:
- Standardized operating parameters and procedures to utilize and disseminate Talon THRESHER data
- Enhanced analysis of air track patterns of behavior
- Timely output of correlated air picture in multiple security formats

JOINT TARGET DEVELOPMENT: TARGET SYSTEM ANALYSIS STANDARDS AND PROCEDURES (T-SAP) (CLOSED MAY 2016)

Sponsor/Start Date: Joint Staff J2/February 2015

Purpose: To develop TTP for targeteers and intelligence analysts to conduct target system analysis (TSA) for joint force operations and to standardize and enhance federated TSA production in support of deliberate and crisis action planning.

Products/Benefits:
- TSA TTP to support joint force planning and update Chairman of the Joint Chiefs of Staff Instruction 3370.01, Target Development Standards
- Provided applicable doctrine change recommendations that will be transitioned to the Joint Staff J2

JOINT UNMANNED AERIAL VEHICLE SWARMING INTEGRATION (JUSI) (CLOSED JULY 2016)

Sponsor/Start Date: USPACOM/February 2015

Purpose: To develop, test, and validate a concept of employment that addresses operational use of swarming unmanned aircraft (UA) carrying electronic attack (EA) payloads against an advanced integrated air defense system (IADS) in an anti-access/area denial environment.

Products/Benefits:
- A concept of employment for UA swarms performing stand-in EA to degrade and deny the hostile IADS kill chain in support of joint air vehicles
- Identified capabilities and limitations of existing planning and modeling and simulation tools for this mission

THEATER JOINT LAND FORCES COMPONENT COMMANDER COMMON OPERATIONAL PICTURE (T-COP)
(CLOSED JUNE 2016)

Sponsor/Start Date: USPACOM/February 2015

Purpose: To develop a TTP and handbook for the USPACOM land forces common operating picture (COP) system to streamline the integration of participating units and various systems into the existing land domain COP.

Products/Benefits:
- Joint TTP that is extensible to other Combatant Commands seeking to enhance or develop similar land domain COPs for their specific needs
- A common processes handbook to effectively maintain the COP and document Service specific practices

OPTIMIZATION OF SOCIAL MEDIA AND OPEN SOURCE INFORMATION SUPPORT QRT (OSMOSIS)

Sponsor/Start Date: USCENTCOM/May 2016

Purpose: To develop TTP to rapidly and effectively gain near-real-time situational awareness using published digital media (new and traditional media sources) available on a global basis to enhance decision-making, planning, and execution of the Civil Affairs, Psychological Operations/Military Information and Support Operations, and Public Affairs missions.

Products/Benefits:
- Improved information gathering from traditional and non-traditional sources to provide the data necessary to create value focused, fused information for analysis to enhance the situational awareness of Commanders at the tactical, operational, and strategic levels.
- Accelerate employment of the Information Volume and Velocity application, a data extraction and aggregation application, across a broad set of missions such as: Defense support of civil authorities, humanitarian aid/disaster relief, strategic communications, counterterrorism, stability and counterinsurgency operations, joint interdiction operations, and peace operations

SPECIAL PROJECTS

JOINT AND COMMUNITY ATTRIBUTES-BASED ACCESS CONTROL AUTHORIZATION FOR TRANSPORTATION SERVICES (J-CAATS)
(CLOSED JULY 2016)

Sponsor/Start Date: U.S. Transportation Command/February 2015

Purpose: To develop TTP and CONOPS for providing secure, yet timely and appropriate, data access for DOD users using an attributes-based access control approach.

Products/Benefits:
- TTP that detailed the technical parameters and provided step-by-step guidance regarding the installation and use of the J-CAATS capability
- CONOPS that describes the overall planning, resources, and timelines required to proceed with usage

JOINT NATIONAL CAPITAL REGION ENHANCED SURVEILLANCE TACTICS, TECHNIQUES, AND PROCEDURES (J-NEST)

Sponsor/Start Date: NORAD/October 2014

Purpose: To develop TTP to incorporate emerging sensor capabilities into the NORAD and USNORTHCOM family of systems to support the air defense mission.

Products/Benefits:
- TTP that enable tactical, operational, and strategic command and control nodes to more fully employ the expanded detection, improved identification, and enhanced engagement of cruise missile threats to the national capital region
- TTP on utilization of advanced equipment capabilities to execute an effective joint engagement sequence for cruise missile defense

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-wing and fixed-wing aircraft
- Determines effectiveness of precision guided weapon (PGW) 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 effectiveness to Service Program Offices, DOT&E, DASD(DT&E), and the Services
- Supports Service member exercises, training, and pre-deployment activities

In FY16 the Center completed 32 T&E activities. These activities included operational/developmental tests for rotary- and fixed-wing ASE, PGWs, threat data collection, experimentation tests, and pre-deployment/exercise support using CM/CCM. The Center conducted analysis of more than 30 DOD systems or subsystems – with special emphasis on rotary-wing survivability – and reported the results.

The Center provided T&E support throughout the year as follows:

- ASE testing, primarily in support of Joint Urgent Operational Needs Statement (JUONS) and Urgent Universal Needs Statement (UUNS) (approximately 40 percent)
- PGW, foreign system, and other types of field testing not related to ASE (approximately 22 percent)
- Realistic Man Portable Air Defense System (MANPADS) threat environment for Service member aircrew training (approximately 8 percent)
- Internal programs to improve test capabilities and develop test methodologies for new types of T&E activities (approximately 26 percent)
  - The Center continued to improve, develop, and validate multiple test tools for evaluating ASE infrared countermeasure (IRCM) systems.
  - In addition, the Center is improving its electronic warfare capability by developing and validating the Portable Range Threat Simulator (PRTS), which will provide a more comprehensive, integrated ASE T&E environment.
- Subject matter expertise to numerous working groups (WGs) and task forces (approximately 4 percent)

The Center's FY16 activities are summarized in the following subsections.

JUONS SUPPORT

Army: Advanced Threat Warning (ATW) Flare Interference Tower Test

- Sponsors: Technology Applications Program Officer (TAPO) and the 160th Special Operations Aviation Regiment (SOAR) Systems Integration Management Office (SIMO)
- Activity: The Center provided one Multi-Spectral Sea and Land Target Simulator (MSALTS) to perform two color, infrared (IR) missile simulations and jam beam data collection. The Center also provided missile warning sensor (MWS) subject matter expertise. This test focused on the ATW Directed Infrared Countermeasure (DIRCM) capabilities to maintain track of a MANPADS in the presence of flares.
- Benefit: The Center's participation in this test was in direct support of ongoing TAPO JUONS efforts. The data the Center collected during this test helped TAPO evaluate the ATW DIRCM's tracking capabilities in the presence of flares.

Army: Project Management Office Aircraft Survivability Equipment (PMO ASE) Formal JUONS Demonstration Pallet Test

- Sponsor: PMO ASE
- Activity: The Center provided one MSALTS to perform simultaneous ultraviolet (UV) and IR missile simulations and jam beam data collection. The Center also provided MWS subject matter expertise. This test evaluated the ATW system. The ATW system was on a pallet installed on the UH-60M. UV simulations were used to assess Common Missile Warning System (CMWS) responses; IR simulations were used to assess ATW responses; and jam beam radiometers were used to assess ATW jam return.
- Benefit: The Center's participation in this test was in direct support of ongoing PMO ASE JUONS efforts. The data the

Center collected during this test helped PMO ASE assess the performance of the integrated ATW/CMWS.

Army: TAPO JUONS Demonstration Test
- Sponsors: TAPO and the 160th SOAR SIMO
- Activity: The Center provided two MSALTS to perform two-color IR missile simulations. The Center also provided MWS subject matter expertise. This test evaluated the ATW system. The ATW system was on a pallet installed on the UH-60A. This test familiarized TAPO with IR MWS testing. The Center provided an independent assessment of ATW detection and angle-of-arrival (AOA) capabilities. After the test, the Center provided an independent assessment analysis report.
- Benefit: The Center's involvement in the program was in direct support of ongoing TAPO JUONS efforts. The Center's independent assessment and the data it collected during this effort helped TAPO determine the ATW system's detection and threat AOA capabilities, which in turn will help them plan future JUONS test activities.

Army: PMO ASE JUONS Hostile Fire Indication Tower Test
- Sponsor: PMO ASE
- Activity: The Center provided one MSALTS – to perform simultaneous UV and IR missile simulations – and jam beam radiometers. This test assessed the capability of the ATW/CMWS-integrated system to track and place laser energy on the true target (MSALTS) with competing sources in the ATW DIRCM tracker field of view. The Center provided near real-time data reduction and analysis of simulations quality and jam onset times to assist the sponsor in test decisions.
- Benefit: The data the Center collected during this test helped PMO ASE assess the integrated ATW/CMWS's performance capabilities in the presence of competing sources.

Army: PMO ASE Formal JUONS IT3 Phase 2 Test
- Sponsor: PMO ASE
- Activity: The Center provided one MSALTS and one Joint Mobile Infrared Countermeasure Test System (JMITS) to perform simultaneous UV and IR missile simulations along with jam beam radiometers. The Center provided simulators for single and dual threat engagements against the integrated ATW/CMWS system as installed on the AH-64E.
- Benefit: The data the Center collected during this test helped PMO ASE assess the integrated ATW/CMWS system declaration, as well as threat AOA performance and DIRCM slew and pointing accuracy.

Army: PMO ASE Formal JUONS IT3 Clutter Flight Testing
- Sponsor: PMO ASE
- Activity: The Center provided one MSALTS – to perform simultaneous UV and IR missile simulations – and jam beam radiometers. The test evaluated the integrated ATW/CMWS system as installed on the AH-64E. The AH-64E flew in the Houston area with MSALTS placed in an urban/industrial environment. The objective was to determine the integrated ATW/CMWS's capabilities to detect and declare the MSALTS simulations in the presence of clutter.
- Benefit: The data the Center collected during this test helped PMO ASE assess the AH-64E integrated system's capability to declare, track, and respond when presented with simulated missiles in a clutter environment.

Army: Army Special Operation Aviation JUONS Phase 1a and 1b Flight Test
- Sponsors: TAPO and the 160th SOAR SIMO
- Activity: The Center provided one JMITS to perform two-color IR missile simulations. The test evaluated the ATW, which was on the MH-60M upturned exhaust system (UES) for Phase 1a testing and on the MH-47F for Phase 1b testing. The test assessed the ATW system's declaration and threat AOA performance, as well as DIRCM slew and pointing accuracy.
- Benefit: The Center's participation in this test was in direct support of ongoing TAPO JUONS efforts. The data the Center collected during this test allowed TAPO to investigate the use of smart dispensing for IRCM flare sequences (i.e., dispense the best pattern based on threat AOA).

Air Force: Air Force Special Operations Command JUONS CV-22 ATW Sensor Flight Test
- Sponsor: 413th Flight Test Squadron Special Systems, Air Force Life Cycle Management Center
- Activity: The Center provided two MSALTS missile simulators to perform two-color IR simulations, as well as a laser van to conduct laser illuminations. The Center also provided test support to include consultation regarding test preparation, planning and execution, as well as data reduction, analysis and reporting for the missile simulations and laser illuminations. The test evaluated the Large Aircraft Infrared Countermeasure (LAIRCM) ATW system as integrated on the CV-22 platform.
- Benefit: The data the Center collected during this test helped the Air Force assess the performance of the ATW system as integrated on the CV-22 platform.

UUNS SUPPORT

Navy: Department of the Navy (DON) LAIRCM ATW MV-22 UUNS IT2A and B Flight Testing
- Sponsors: Program Executive Officer, Advanced Tactical Aircraft Protection Systems (PMA-272) and Commander, Operational Test and Evaluation Force (COTF)
- Activity: The Center provided two MSALTS to perform two-color IR missile simulations, threat-representative lasers, PRTS, and consultation regarding test preparation, planning and execution for the missile simulator and laser test events. This test was an end-to-end, open-air test and evaluation of the

UUNS for integration of the DON LAIRCM ATW system onto the MV-22. After the test, the Center provided an independent assessment analysis report.
- Benefit: The Center's independent assessment and the data it collected during this effort helped PMA-272 evaluate the integration of the DON LAIRCM ATW system onto the MV-22 and test the new ATW software upgrades.

Navy: DON LAIRCM ATW MV-22 Quick Reaction Assessment Flight Testing
- Sponsors: PMA-272 and COTF
- Activity: The Center provided two MSALTS (to perform two-color missile simulations), threat-representative lasers, and consultation regarding test preparation, planning and execution for the missile simulator and laser test events. This test was an operational test and evaluation of the UUNS for integration of the DON LAIRCM ATW system onto the MV-22.
- Benefit: The Center's participation in this test was in support of MV-22 ATW quick reaction operational testing. The data the Center collected during this test helped PMA-272 evaluate the integration of the DON LAIRCM ATW system onto the MV-22.

ASE ACTIVITIES

Army: Seeker Performance in a Cluttered Environment Test
- Sponsors: Army Research Laboratory (ARL) and Utility Helicopters Project Office (UHPO)
- Activity: The Center provided the Seeker/Radiometric Test System (SRTS) with eight preemptive-configured IR surface-to-air missile (SAM) seekers, IR radiometric imagers, and SAM subject matter expertise during acquisition testing. This test evaluated the ability of MANPADS to acquire Army rotary wing aircraft flying against a cluttered terrain background. The radiometric and imagery data collected were used to quantify the background. After the test, the Center provided an independent assessment of the SAMs for incorporation into a briefing for ARL and UHPO.
- Benefit: The Center's involvement in this activity was in support of ARL's modeling and simulation efforts. The Center's independent assessment and the data it collected during this effort will help validate modeling and simulation of rotatory wing aircraft flying in a cluttered background environment against MANPADS.

Army: Reduced Optical Signature Emissions Solution IRCM IX Test
- Sponsors: TAPO and the 160th SOAR SIMO
- Activity: The Center provided the SRTS with eight post-reactive-configured IR seekers and subject matter expertise during the IRCM effectiveness test for the MH-60M and MH-47G aircraft. These tests evaluated new flare CM sequences and variations of current flare CM sequences using improved flares, different flares, and/or flare timing within the sequences. 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 sponsor was able to make decisions on flare sequence performance during the course of the test. After the test, the Center provided an independent assessment analysis report and a briefing of test results to TAPO leadership.
- Benefit: The Center's involvement in this activity helped TAPO determine a final IRCM flare solution. The Center's independent assessment and the data it collected during this effort allowed TAPO to procure the new flares needed to enhance the protection of the MH-60M and MH-47G aircraft against MANPADS.

Army: Seeker Bowl XI IRCM Test
- Sponsor: Armament Research, Development and Engineering Center (ARDEC), Pyrotechnics Division, Countermeasure Flare Branch
- Activity: The Center provided the SRTS with eight post-reactive-configured IR seekers and subject matter expertise during the IRCM effectiveness test for the AH-64E ASPI, UH-60M UES, UH-60L UES, UH-60L HIRSS, and CH-47F IRSS aircraft. 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 sponsor was able to make decisions on flare sequence performance during the course of the test. After the test, the Center provided an independent assessment analysis report.
- Benefit: The Center's involvement in this activity helped ARDEC determine a final IRCM flare solution and prepare its post-test briefing for its higher headquarters. The Center's independent assessment and the data it collected during this effort allowed ARDEC to change the fielded flare sequence for all but the CH-47F IR Suppression System, thus providing better protection for those aircraft against MANPADS. ARDEC also briefed the test results to PMO ASE and platform program managers.

Air Force: U-28 ATW Sensor Flight Test
- Sponsor: 46th Test Wing Test Squadron, Defensive Systems and Mobility Directorate, Air Force Life Cycle Management Center
- Activity: The Center provided one JMITS missile plume simulator and personnel to perform two-color IR simulations in support of flight testing. The Center also provided test support to include consultation regarding test preparation, planning, and execution, as well as data reduction, analysis, and reporting for missile plume simulations. After the test, the Center provided an independent assessment analysis report.

- Benefit: The Center's independent assessment and the data it collected during this effort helped the Air Force assess the performance of the ATW system installed on the U-28 platform.

Navy: KC-130J DON LAIRCM Integration Test
- Sponsor: PMA-272
- Activity: The Center provided two MSALTS and subject matter expertise during the planning and execution of integration testing of the DON LAIRCM ATW onto the KC-130J.
- Benefit: The Center's participation in this test helped support integration of the ATW system onto the KC-130J and testing of new ATW software upgrades. The data the Center collected during this test helped the Navy assess the performance of the ATW system as installed on the KC-130J.

FOREIGN EVENTS

Foreign: Static Burn Test/NATO Trial KANERVA
- Sponsors: The Joint Countermeasures Test and Evaluation (JCMT&E) WG and the Naval Research Laboratory (NRL)
- Activity: The Center, along with the Arnold Engineering Development Complex and the NRL, collected radiometric signature data on static rocket motor burns at Niinisalo, Pohjankangas, Finland. Participation was under the provisions of existing NATO agreements and data analysis was coordinated within the provisions of the four-nation Multinational Test and Evaluation Program's Air Electronic Warfare Cooperative Test and Evaluation Project Arrangement. Data was collected on five types of threat rocket motors. Model updates resulting from this effort will be used to improve JMITS/MSALTS simulations.
- Benefit: The data the Center collected during this test supports refinements to MWS threat algorithms.

RESEARCH AND DEVELOPMENT ACTIVITY

USD(AT&L)/Air Force: Space-based Hypertemporal Imaging Research and Development
- Sponsors: USD(AT&L) Coalition Warfare Program and Air Force Research Laboratory, Advanced Missile Warning Technologies
- Activity: The Center deployed and operated the Towed Airborne Plume Simulator (TAPS) to Woomera, Australia. This risk reduction activity supported research and development associated with space-based sensor detection of IR sources through varying cloud layers.
- Benefit: The Center's TAPS provided the sponsors with the ability to present a controlled IR source (i.e., location and signature) within a space-based sensor's field-of-view at desired weather conditions. The Center provided self-assessment quick-look reports within 24 hours of each mission, summarizing the simulator's performance for each event.

PGW CM ACTIVITIES

Navy: JSOW C-1 OT-IIIB Land IRCM Live Fire Flight Test
- Sponsor: COTF
- Activity: The Center supported a live-fire test of the JSOW C-1 missile against a stationary target. The Center provided a CM environment consisting of camouflage nets and IR smoke to obscure and modify the signature of the stationary target while the JSOW C-1 attempted to acquire, track, and hit the target. After the test, the Center provided an independent assessment analysis report.
- Benefit: The Center's independent assessment and the data it collected during this test helped COTF determine if the JSOW C-1 missile had retained its stationary land target mission capability in a CM environment given the recent addition of a moving maritime target mission capability.

Army: Joint Air-to-Ground Missile (JAGM) System
- Sponsor: Joint Attack Munition Systems Project Office
- Activity: The Center, in conjunction with the Edgewood Chemical and Biological Center, Smoke and Target Defeat Branch, provided various battlefield atmospheric obscurants for test and evaluation of the JAGM in tower and captive flight environments.
- Benefit: These tests were conducted to characterize the performance of the JAGM guidance section and collect scene data for the guidance section sensors in the presence of CMs for the verification of Integrated Flight Simulation results.

TRAINING SUPPORT FOR SERVICE MEMBER EXERCISES

Red Flag 16-1 (January 25 – February 12, 2016) Nellis AFB, Nevada

Red Flag 16-2 (February 29 – March 11, 2016) Nellis AFB, Nevada

Emerald Warrior (May 2 – 13, 2016) Hurlburt Field, Florida
Advanced Integration/Joint Forcible Entry (June 7 – 21, 2016) Nellis AFB, Nevada
Red Flag 16-3 (July 11 – 29, 2016) Nellis AFB, Nevada
Red Flag 16-4 (August 15 – 25, 2016) Nellis AFB, Nevada

- Sponsors: Various
- Activity: The Center provided personnel and equipment to simulate a threat environment, as well as subject matter expertise, to observe aircraft ASE systems and crew reactions to this environment. Specifically, the Center simulated MANPADS threat engagements for participating aircraft. Additionally, the Center provided MANPADS capabilities and limitations briefings to pilots and crews and conducted familiarization training at the end of the briefings.
- Benefits: The Center's participation in these exercises provided realism to the training threat environment and enhanced the Service member pilots' and crews' understanding and use of CM equipment, especially ASE. The data the Center collected and provided to the trainers helped the units develop/refine their tactics, techniques, and procedures to enhance survivability.

T&E TOOLS

The Center continues to develop tools for T&E of ASE. The Joint Standard Instrumentation Suite (JSIS) and the MSALTS Ultraviolet Emitter Enhancement (MUVEE) projects were funded by USD(AT&L), the Test Resource Management Center; and the Central T&E Investment Program.

JSIS

JSIS is a transportable, fully-integrated instrumentation suite that will be used to collect signature; Time, Space, Position Information; and related threat missile and hostile fire munitions metadata. The transportability of JSIS will 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 Navy (PMA-272), Army (PMO ASE), and Air Force (LAIRCM System Program Office) have endorsed JSIS, and it will be an integral part of each program office's ASE development. The Center deployed and operated JSIS during a risk reduction activity at Redstone Arsenal, Alabama, in February 2016. The Center exercised the system in an operationally realistic environment and verified the performance of key system capabilities. Some anomalies were identified that could not be detected in a laboratory environment. Post-event analysis discovered the root cause of these anomalies and the engineering changes needed to resolve them prior to acceptance testing. Early detection and resolution of any anomalies mitigates the risk of such anomalies arising when JSIS is used to collect data during actual acquisition program events.

The JSIS Initial Operational Capability is expected to be completed in FY17. As part of the JSIS project, the Center managed a contract to develop a Doppler Scoring Radar to support missile and hostile fire signature data collections and model developments. It is a 10.08 – 10.56 GHz tunable continuous wave and frequency modulated continuous wave radar, providing three degrees of freedom information (X, Y, Z) in time and range rate information on acquired and tracked targets. The Doppler Scoring Radar radar is capable of acquiring 128 targets and tracking 3 targets. The radar supported JSIS Risk Reduction tests. Its TrackVue software – which supports radar configurations, calibration, operational functionality, and data analysis – was updated to version 1.5.1. Sixteen high-power amplifiers within the radar and one spare were repaired to reduce noise floor fluctuations.

JSIS initial operational capabilities were driven by near-term needs for operational testing with the Navy's Advanced Threat Warner. While it represents a significant step forward in fielding data collection capabilities, significant gaps and shortfalls remain to include expanded missile attitude data collection and additional signature instrumentation to support emerging ASE programs with associated modeling and simulation needs. The Center has been actively formulating a technical approach, cost estimate, and acquisition strategy to produce JSIS Phase II with the intent of securing sponsorship beginning in FY17.

MUVEE

The MUVEE is an engineering improvement to MSALTS that incorporates the Army's T-MALUS emitter and software. The MUVEE will improve UV performance to enhance support of Army operational testing of Common Infrared Countermeasure (CIRCM) integrated with CMWS. Acceptance testing of the MUVEE was completed on May 20, 2016. The system was deployed to Redstone Test Center during the week of May 23 to collect signature data in support of system validation, as well as conduct some field regression testing. Corrective actions for deficient items and documentation updates were completed the first week of June 2016, followed by delivery of the system to the Center.

TEST VANS

- The Center procured a new van to replace a legacy, off-road test van which is no longer field-worthy. The van will be used for video and radiometric data collection at remote test sites.
- The Center is modifying one of its existing vans for use as the JSIS control van. This van will allow rapid and efficient deployment of JSIS to test sites.
- The Center is developing a new van to serve as the Center's Remote Launcher System control and instrumentation van. This van will be capable of controlling up to two launch trailers simultaneously.

THREAT SIGNATURE GENERATION

In support of Army's PMO ASE, the Center is generating up to 60,000 threat signatures for the CIRCM program. Initial planning meetings and coordination with the threat integration laboratories have occurred. The Center briefed its threat signature generation

process to the program, Army Test & Evaluation Command, and Army Validation WG. The Center submitted the standard operating procedure to the PMO ASE for review and signature. The signatures will be used in labs and open-air testing for evaluating CIRCM performance.

PRTS AND HIGH-POWERED PRTS (HPRTS)

The Center is internally funding the procurement of two RF threat emitters: PRTS and HPRTS. This was prompted by the Center's FY13 electronic warfare internal study and the increasing demand for test tools that support multi-spectral, integrated ASE threat environments. The low-powered PRTS system completed validation data collection in FY16, and an HPRTS capability is scheduled for delivery in FY17. These systems are designed to replicate short-range acquisition and targeting radar systems. Both systems will be validated to support operational testing of the APR-39D(V)2 Radar Warning Receiver/Electronic Warfare Management System.

JCMT&E WG

DOT&E and DASD(DT&E) co-chartered the JCMT&E WG to measure, test, and assess the following:

- 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
- Overseas threat and air electronic warfare systems performance and effectiveness data collection in coalition warfare environments

DOT&E, DASD(DT&E), all four of the U.S. Services, Australia, Canada, New Zealand, the UK, and the 22-nation NATO Air Force Armaments Group Sub-Group 2 participate in the JCMT&E WG. The WG is tasked with actively seeking mutually beneficial T&E opportunities to measure performance and suitability data, which are necessary to provide relevant operational information to deploying joint/coalition Service members and to U.S. acquisition decision makers. Specific efforts include:

- The JCMT&E WG has initiated discussions with European Command's Office of Defense Cooperation to conduct testing and data collection in its area of responsibility under operationally relevant environments important to the Combatant Command, Warfare Centers, and Programs of Record.
- The JCMT&E WG is cooperating with NATO partners and Partnership for Peace nations to provide opportunities to obtain and expand operationally relevant information in order to field new capabilities rapidly and reduce cost. The JCMT&E WG is building on the Center's proven record of conducting successful ASE data collection by coordinating live firings of radio frequency/electro-optical/IR SAMs, Hostile Fire Indication, and anti-tank guided missile firings by active duty air-defense units and test organizations in Finland, Sweden, the UK and Bulgaria. These efforts will provide measured operational performance of actual, modern, multifunction radars and integrated air defense systems that pose threats to U.S. and allied forces.
- The JCMT&E WG is the U.S. Steering Committee Chairman for bilateral and multinational Test and Evaluation Program Cooperative T&E Project Arrangements with Australia, Canada, and the UK. The JCMT&E WG is currently developing similar agreements with Germany, Finland, Denmark and Sweden. These efforts have already expanded the availability of air-electronic warfare system performance and suitability data to improve aircraft survivability. They have also identified opportunities to use other member nations' T&E capabilities to support U.S. program efforts.

The JCMT&E WG worked with the United States, Australia, Canada, and the UK to conduct modeling and simulation in Canada to support a combined MANPAD/radio frequency threat test of ASE installed in helicopters and fixed-wing aircraft at the Woomera Test Range, South Australia. That September 2016 threat test, trial DESERTRIDER 16, was designed to assess a preliminary open-air test methodology appropriate for testing integrated ASE. Combining the four nations' captive seekers, actual and simulated emitters for fixed- and rotary-wing aircraft equipped with flares and decoys provided each nation with valid, measured data not available singularly. Follow-on testing is being planned for laser warning/countermeasures systems in the UK, cold weather environment data collection in Canada, and ASE performance and tactics verification in the United States.

Index

Index

FY16 INDEX OF PROGRAMS

W

X

Y

Z

FY16 INDEX OF PROGRAMS

www.dote.osd.mil