
Director, Operational Test and Evaluation


LPD-17

**Follow-on Operational Test and Evaluation Report
on Chemical, Biological, and Radiological Defense**



November 2012

This report on the LPD-17 *San Antonio* class ship assesses the adequacy of the Chemical, Biological, and Radiological (CBR) Defense Follow-on Operational Test and Evaluation (FOT&E) event and the effectiveness of the LPD-17 in a CBR environment.


J. Michael Gilmore
Director



The USS *San Antonio* (LPD-17)

Executive Summary

This document reports results from the chemical, biological, and radiological (CBR) defense test conducted aboard USS *New York* (LPD-21) on February 15-16 and March 27-28, 2012, off the coast of Virginia. This test was part of the Follow-on Operational Test and Evaluation (FOT&E) program for the *San Antonio* class and was designed to assess the ship's ability to conduct amphibious operations in a contaminated (chemical) environment. Additionally, this report provides a status update to the deficiencies reported in DOT&E's June 2010 USS *San Antonio* (LPD-17) Class Amphibious Transport Dock Ship Combined Operational and Live Fire Test and Evaluation Report.

Test Adequacy

FOT&E CBR event was adequate to determine the ability of the LPD-17 class ships to conduct sustained operations in a contaminated (chemical) environment. DOT&E approved the Navy's Operational Test and Evaluation Force (OPTEVFOR) FOT&E Test Plan and Data Management Plans. OPTEVFOR conducted the test in accordance with the test plan.

The test concept was to simulate a chemical attack on the ship and observe the ship's response. A series of intelligence warnings with an increasing threat of chemical attack initiated the test. During that time, the ship increased Mission-Oriented Protective Posture (MOPP) levels per the CBR Bill followed by a simulated, threat-representative attack in which a helicopter (threat surrogate) flew over the length of the ship at an altitude of 300 feet while spraying a personnel-safe chemical weapon simulant.¹ This challenged the ship's chemical defense systems, such as the Collective Protection System (CPS), the Improved (Chemical Agent) Point Detection System – Lifecycle Replacement (IPDS-LR) and the Countermeasure Wash Down System (CMWDS). Additionally, the crew demonstrated their ability to decontaminate the ship and equipment. All four personnel decontamination stations were evaluated for functionality and personnel throughput was measured at one station. A final demonstration in which the welldeck crew donned chemical protective suits and masks, and launched two Landing Craft Air-Cushioned (LCAC) assault craft to demonstrate whether the ship's crew was capable of conducting amphibious operations in a contaminated environment.

CBR Effectiveness

The FOT&E CBR event demonstrated that the LPD-17 class of ships is effective in responding to a chemical warfare environment. The test further demonstrated the ability of the ship to conduct a subset of amphibious operations in a chemical environment. The CPS was able to prevent entry of simulant vapors into protected zones of the ship. The CMWDS functioned as expected. However, excess water due to poor deck surface drainage was noted on the weather

¹ The CBR-Bill is this ship's instructions and procedures for defense in a chemical, biological, or radiological attack.

decks after CMWDS activation. A leak, due to insufficient packing in a stuffing tube, occurred in the pilot house during an early MOPP level test of the CMWDS.²

The ship met the required throughput threshold for personnel decontamination, and the crew demonstrated the ability to carry out proper procedures to decontaminate the ship and equipment. While all four decontamination stations on the LPD-21 are functional, only two ships in the LPD-17 class (LPD-21 and LPD-22) have functioning litter-born casualty decontamination stations.

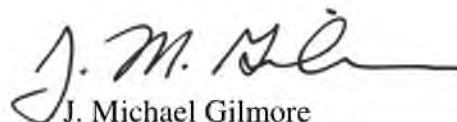
The LCAC demonstration, in which an LCAC was successfully launched but not recovered from the welldeck of the ship, illustrated that the welldeck crew can perform a limited set of amphibious operations while wearing chemical protective gear. This demonstration was not intended to test the ability of the LCAC crew to conduct operations in a contaminated environment, which will be demonstrated in future testing of the LCAC replacement program (the Ship to Shore Connector (SSC)).

The M256 survey kit is used by shipboard personnel to detect chemical vapors. Because this kit requires over 20 minutes to process a sample, it limits the crew's ability to expeditiously conduct surveys following a CBR attack. The Navy should investigate developing a portable detector similar to the IPDS-LR to expedite post-CBR attack surveys.

Recommendations

The Navy should implement the following recommendations and test during FOT&E:

- The Navy should address deck drainage problems, particularly areas in which large amounts of water can accumulate from the CMWDS.
- The Joint Program Executive Officer for Chemical and Biological Defense and the Navy should work to develop a more effective survey instrument than the M256 kit for chemical warfare agents onboard ships.
- The Navy should ensure that the remaining LPD-17 class ships with non-functional litter born casualty decontamination stations are retrofitted to render them functional.
- Because the LCAC crew was not in MOPP gear, the Navy should conduct a more robust test in the future.
- The Navy should also consider holding combined CBR training for both LCAC and ship crews to ensure both are capable of carrying out sustained operations in a CBR environment.


J. Michael Gilmore
Director

² A stuffing tube allows cables to pass through decks and walls of the ship.

Contents

System Overview	1
Test Adequacy	5
Assessment.....	9
Recommendations	19

This page intentionally left blank.

Section One System Overview

This document reports results from the chemical, biological, and radiological (CBR) defense test conducted aboard USS *New York* (LPD-21) on February 15-16 and March 27-28, 2012, off the coast of Virginia. This test was part of the Follow-on Operational Test and Evaluation (FOT&E) program for the LPD-17 class and was designed to assess the ship's ability to conduct amphibious operations in a contaminated (chemical) environment. The LPD-17 class ships are 24,900 ton, 684 feet long, diesel engine-powered amphibious transport ships that embark, transport, and deploy ground troops, equipment, and cargo (Figure 1-1). Each ship can embark 699 Marines. The LPD-17 class utilizes embarked Landing Craft Air Cushioned (LCAC), Landing Craft Utility (LCU), Amphibious Assault Vehicles (AAV), and various aircraft to accomplish ship-to-shore movement. The LPD-17 class has a floodable welldeck for LCAC, LCU, and AAV operations. Flight deck and hangar facilities are equipped to accommodate helicopters as well as MV-22 Osprey aircraft.



Figure 1-1. USS *San Antonio* (LPD-17)

The LPD-17 class has several systems that allow the ship to operate in a contaminated environment. These systems (discussed in detail below) include a collective protection system, a wash down system, decontamination stations, a chemical agent detection system, and other detection and protective equipment.

Collective Protection System (CPS). A subset of the ship's internal spaces are over-pressurized and provided with filtered High-Efficiency Particulate Air (HEPA) (Figure 1-2). The CPS protects the crew and prevents contaminated air from entering vital zones of the ship.



Figure 1-2. CPS Zone Boundaries in LPD-21

Countermeasure Wash Down System (CMWDS). The CMWDS is a series of external sprinklers that, when activated, spray the ship with sea water. The spray is intended to keep contaminants such as chemical or biological agents from adhering to the outer surfaces of the ship.

Decontamination Stations. The LPD-17 class is outfitted with four personnel decontamination stations. They are located (1) forward main deck below the bridge, (2) below the wardroom, (3) aft of the boat valley, and (4) forward of the hangar (Figure 1-3). Stations 1, 2, and 3 are for ambulatory personnel; Station 4 is for litter-born casualties.



Figure 1-3. Decontamination Stations on USS *San Antonio* (LPD-17)

The personnel decontamination stations are arranged as shown in Figure 1-4. Personnel enter from spaces external to a CPS zone and pass through clothing removal, shower, and air drying cells, and then enter the CPS-protected area of the ship. In the casualty decontamination station (Station 4), the casualty is moved through the same procedures while on a litter.

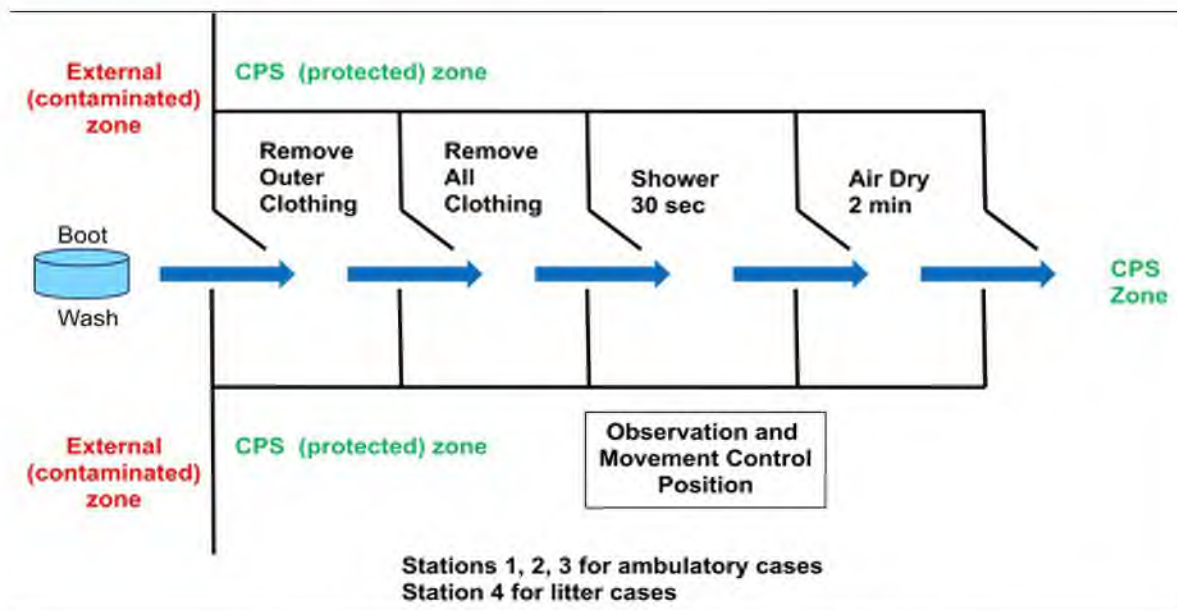


Figure 1-4. Decontamination Stations: Processing Plan View

Improved (Chemical Agent) Point Detection System – Lifecycle Replacement (IPDS-LR). The IPDS-LR is a chemical agent vapor detector that provides an alert that the ship has been exposed to a chemical agent. IPDS-LR uses ionization mass spectrometry to detect nerve and blister agents.³ The IPDS-LR has two air intake manifolds on either side of the bridge exterior. Alerts are displayed on a Control Display Unit (CDU) (Figure 1-5) in the Central Control Station (CCS) and on the Remote Display Unit (RDU) in the ship's bridge. The IPDS-LR and its predecessor the IPDS are not specific to the LPD-17 class; they are installed on all U.S. Navy surface ships.



Figure 1-5. IPDS-LR Control Display Unit

³ For more information, see DOT&E report, "Improved (Chemical Agent) Point Detection System – Lifecycle Replacement (IPDS-LR) Follow-on Test and Evaluation Report," April 2011.

Other CBR systems. The crew of the LPD-17 class ships have access to several other pieces of equipment that can be used to protect against, detect, or respond to a CBR attack. These include:

- **M8/M9 paper** – M8 and M9 paper are similar to litmus paper and are used to detect the presence of liquid chemical agents. The paper changes color based on the type of agent present (nerve or blister agent). M9 paper contains a sticky backing and can be attached to interior or exterior structures in order to detect the presence of chemical agent; M8 paper does not have a sticky backing but can be used during surveys by the crew to detect chemical agent liquids on the ship.
- **M256 kit** – The M256 kit detects chemical agent vapors in the air by using a series of glass vials containing solutions that react with chemical agent vapors. The M256 kit can detect nerve, blister, and blood agents but can take up to 20 minutes to determine whether an agent is present. The M256 kit is currently the only available means to detect chemical agent vapor during surveys onboard ship.
- **Mission-Oriented Protective Posture (MOPP) gear** – MOPP gear for crew of the LPD-17 class consists of the Joint Service Lightweight Integrated Suit Technology (JSLIST). Each crewmember is given his/her own set of gear, which includes protective over-garments, gloves, boots, and mask. Various gear is donned as the ship increases MOPP levels with increasing threat or intelligence information.
- **Fire hoses** – Crewmembers can use fire hoses (normally used for damage control), both internal and external, to decontaminate the ship and equipment.

Section Two

Test Adequacy

Follow-on Operational Test and Evaluation (FOT&E) was adequate to determine the effectiveness of the LPD-17 class when operating in a chemical, biological, and radiological (CBR) environment. The Director, Operational Test and Evaluation (DOT&E) approved the FOT&E Test Plan. The Navy's Operational Test and Evaluation Force (OPTEVFOR) conducted the test in accordance with this plan.

The Navy completed Initial Operational Test and Evaluation (IOT&E) on the LPD-17 class ship from 2007 through 2009. Demonstrating the capability to conduct sustained operations in a CBR environment remained for FOT&E. The CBR FOT&E was conducted onboard USS *New York* (LPD-21) on February 15-16 and March 27-28, 2012, off the coast of Virginia. The test was intended to demonstrate the capability of the Improved (Chemical Agent) Point Detection System – Lifecycle Replacement (IPDS-LR), the Countermeasure Wash Down System (CMWDS), and the Collective Protection System (CPS), as well as the crew's ability to decontaminate the ship, equipment and personnel, and the ship's ability to conduct sustained amphibious operations in a CBR environment.

Test Concept

The test concept was to simulate a chemical attack on the ship and observe the ship's response. A series of intelligence warnings of an increasing threat of chemical attack initiated the test. During that time, the ship increased Mission-Oriented Protective Posture (MOPP) levels per the CBR Bill followed by a simulated, threat-representative attack in which a helicopter (acting as a surrogate) flew over the length of the ship at an altitude of 300 feet while spraying a personnel-safe chemical agent simulant (Figure 2-1).⁴ The simulant used was a mixture of Methyl Salicylate and PEG-200 (hereafter designated as MeS) and is commonly used to simulate the blister agent Bis(2-chloroethyl) sulfide (hereafter designated as HD or mustard gas).⁵ IPDS-LR detected the blister agent following release from the helicopter and the chemical agent alarm activated in the pilothouse of the ship.

⁴ The CBR Bill is the ship's instructions and procedures for defense in a CBR attack.

⁵ PEG-200 is Polyethylene Glycol.



Figure 2-1. CH-46 Spraying Simulant onto USS New York (LPD-21)

Collective Protection

To determine whether the ship's CPS was able to prevent internal contamination with the agent simulant vapors, members from the Navy's OPTEVFOR placed atmospheric sampling canisters in internal and external locations on the ship. The canisters sampled the air for approximately 2 hours (before, during, and after the simulant release) and OPTEVFOR later analyzed the canisters for the presence of MeS using a mass spectrometer. Background samples were also collected prior to the simulant release to provide a baseline reading.

Countermeasure Wash Down System

While the CMWDS was active, OPTEVFOR made observations of the wash coverage area, with special attention to deck-mounted machinery. OPTEVFOR also took note of any areas that appeared dry after wash-down.

Equipment Decontamination

Because the CMWDS was effective in keeping the MeS (released from the helicopter) from adhering to the ship, a second application of simulant MeS was applied to the ship's boat valley, using a hand-held sprayer.⁶ This second application was required to facilitate the assessment of the crew's survey and decontamination procedures. Approximately 25 crewmembers participated in the decontamination of the affected area, using fire hoses and scrub brushes to decontaminate the boat valley.

Personnel Decontamination

The LPD-17 class Operational Requirements Document (ORD), which is classified, requires the ship be able to process a specified number of personnel per hour through the

⁶ The deck area between the fore and aft masts.

ambulatory decontamination stations. After completion of the boat valley decontamination described above, the crew proceeded to decontamination Station 3 (shown in Figure 1-3), where station throughput was measured and compared to the ORD requirement. This test measured only personnel throughput. Crewmembers were not purposefully contaminated. An assumption was made, supported by previous testing of similar decontamination stations on other ship classes, that the decontamination process itself is successful in removing agent from contaminated individuals and in keeping agent external to CPS-protected spaces.⁷ The other decontamination stations in the ship (1, 2, and 4) were activated and their functionality demonstrated by processing a single crewmember through each station.

Conducting Amphibious Operations

The ORD also requires the LPD-17 class be capable of conducting amphibious operations while in a CBR environment. On March 27-28, the Navy conducted a demonstration on USS *New York* (LPD-21) in which the welldeck crewmembers, specifically the ramp marshal, the safety observer, and their trainees, donned MOPP 4 gear and followed normal procedures for launching two Landing Craft Air Cushioned (LCACs). The LCAC crew were not in MOPP gear, and this demonstration only tested the LPD-21 crew's ability to function in a CBR environment. Because the LCAC crew were not in MOPP gear, the Navy plans to conduct a more robust test with the future LCAC replacement program, the Ship-to-Shore Connector (SSC).

Test Limitations

The Navy executed the test as planned, albeit on a revised and tighter schedule due to last-minute changes in the ship's schedule. A second external survey, to determine whether residual contamination was present (after the manual decontamination described above) was not conducted as required by the ship's CBR bill because of the shortened timeline.

One or two external survey and decontamination team members entering the decontamination station were not deliberately contaminated (with the hand-held sprayer) as called for in the test plan. All survey and decontamination (of ship and equipment) team members did, however, go through all of the procedures to be decontaminated.

⁷ "Developmental Testing (DT-III A) of the Collective Protection System (CPS) aboard the USS *Curtis Wilbur* (DDG-54)," Naval Surface Warfare Center Dahlgren Division (NSWCDD) December 1994.

This page intentionally left blank.

Section Three Assessment

Follow-on Operational Test and Evaluation (FOT&E) determined the effectiveness of the LPD-17 class of ships in responding to and operating in a chemical, biological, and radiological (CBR) environment. The LPD-17 class of ships is effective in responding to a chemical warfare event, and is able to conduct a limited set of amphibious operations in a CBR environment.

CBR Effectiveness

FOT&E demonstrated that the LPD-17 class of ships is effective in responding to a chemical warfare event. The test also demonstrated the ability of the ship to conduct a limited set of amphibious operations in a CBR environment. The Collective Protection System (CPS) was able to prevent entry of simulant vapors into protected spaces of the ship. The Countermeasure Wash Down System (CMWDS) functioned as designed. The throughput objectives for the personnel decontamination stations were met.

The Landing Craft Air Cushioned (LCAC) demonstration illustrated that the welldeck crews of the LPD-17 class ships can perform some normal operations while wearing Mission-Oriented Protective Posture (MOPP) 4 gear. However, the limited scope of the demonstration did not allow a full assessment of the ship's ability to conduct sustained, full-spectrum amphibious operations while in a CBR environment. Combined CBR training exercises with LCAC crews and amphibious ships should be conducted to ensure both crews are capable of carrying out these evolutions while wearing MOPP gear.

Collective Protection System Functionality

During fly-over, the helicopter encountered a moderate cross wind from the port side of the ship, causing the simulant to be deposited only on the starboard side (see Figure 3-1, as detected by M9 paper). This uneven simulant distribution pattern was not unexpected and is consistent with how a chemical agent may be deposited during an actual threat attack.⁸ The starboard side Improved (Chemical Agent) Point Detection System – Lifecycle Replacement (IPDS-LR) system responded to the simulant, and the ship went to MOPP 4 (full CBR protection) condition. According to the ship's CBR bill, MOPP 4 should have been initiated along with CMWDS when the intelligence report indicated the attack was imminent, but in the interest of ensuring the simulant reached the ship in order to observe the actual distribution pattern of the spray as well as test the CPS, the CMWDS was not activated in MOPP level 4 until after IPDS-LR detection of chemical vapor.

⁸ San Antonio Class (LPD-17) Chemical Warfare Threat Validation Report. August 2011. SECRET

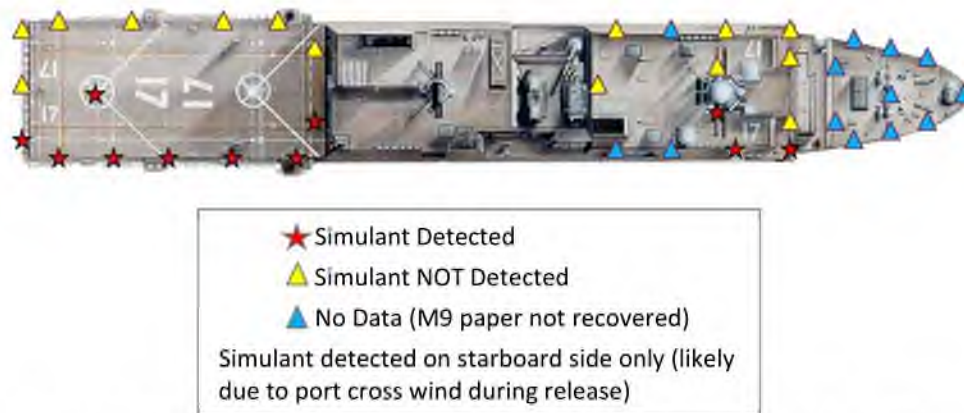


Figure 3-1. Pictorial Representation of Simulant Distribution Post-Deposition

To determine whether the ship's CPS was able to prevent chemical simulant vapors from entering protected spaces, air sampling canisters were placed inside and outside the ship's CPS zones to monitor the air before and after the simulant release. Figures 3-2, 3-3, and 3-4 show the locations of canisters inside and outside the ship. Unbracketed canisters were located in interior spaces, while those in black brackets were located in the ship's exterior.

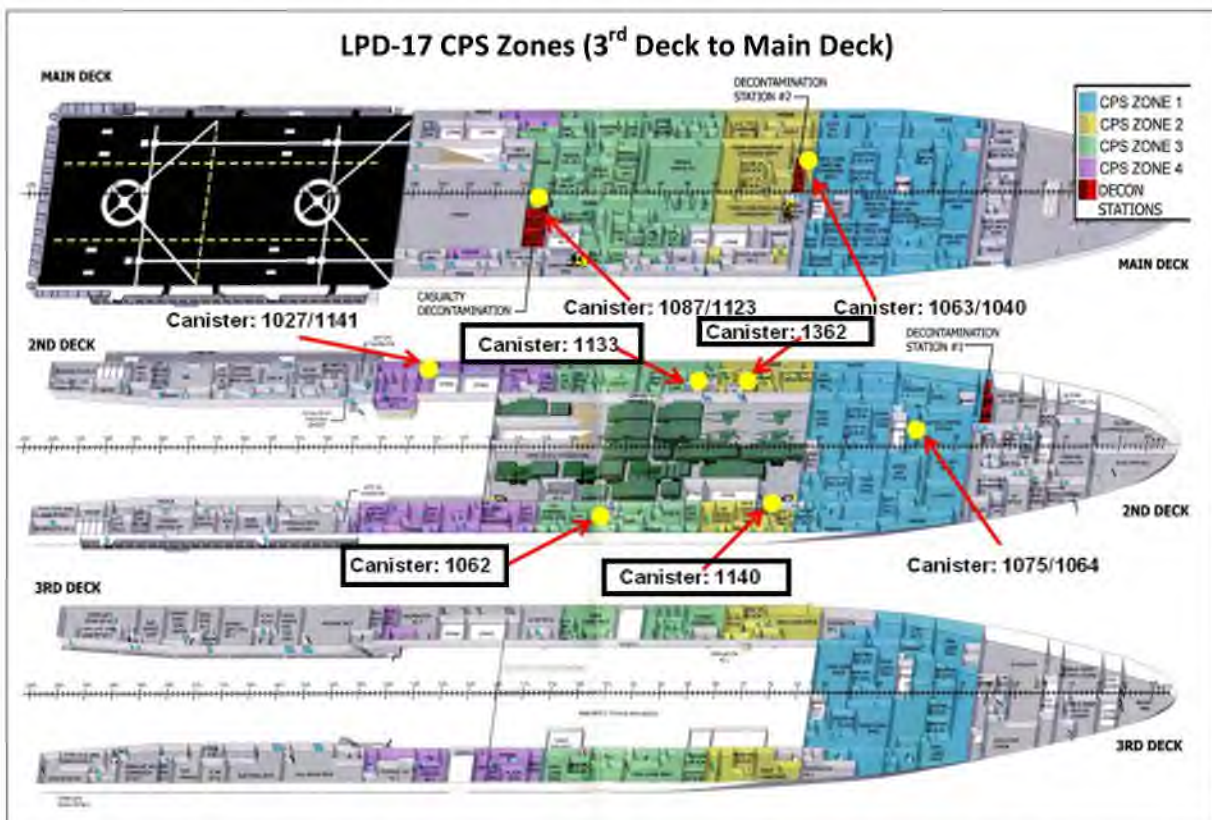


Figure 3-2. Location of Air Samplers Interior and Exterior from Third to Main Deck

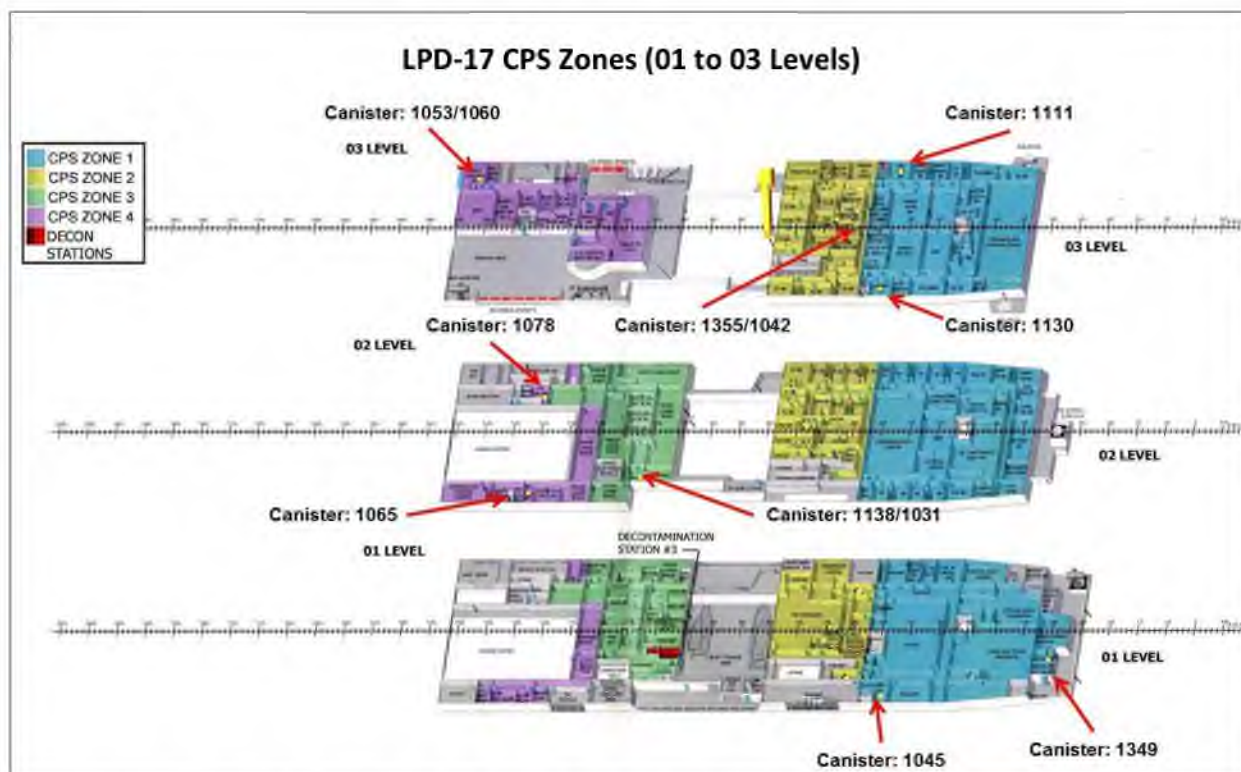


Figure 3-3. Location of Air Samplers Interior and Exterior from 01 to 03 Levels

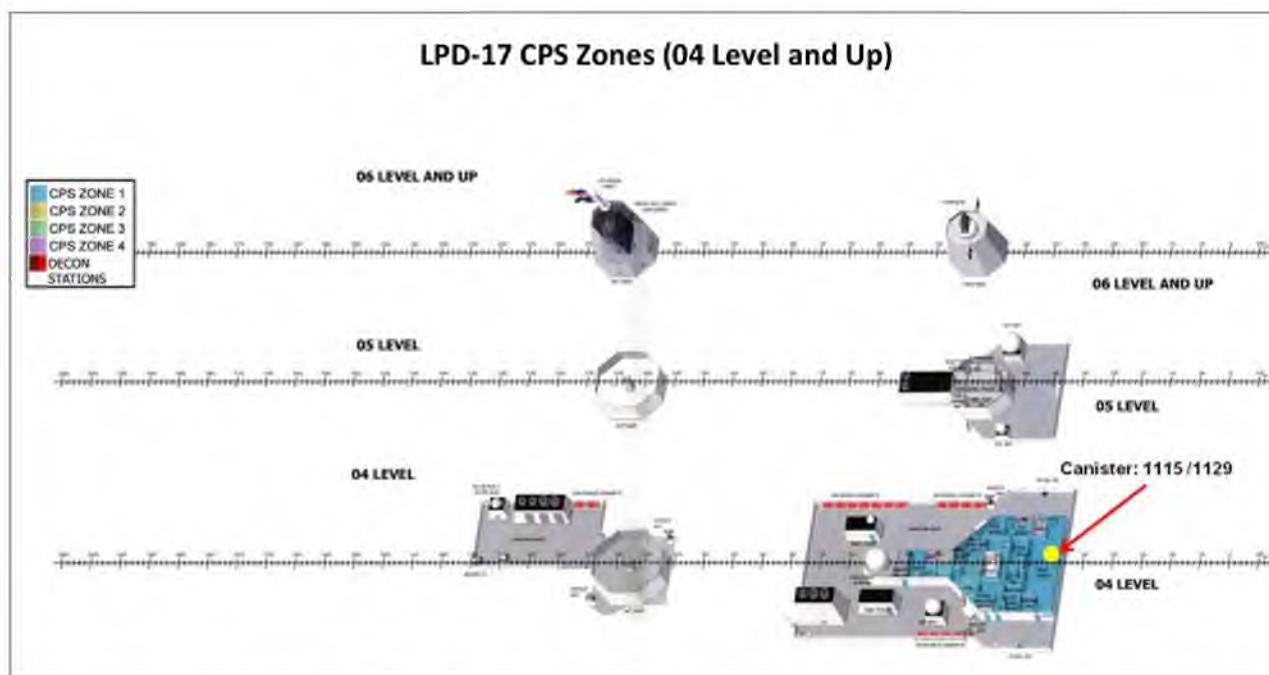


Figure 3-4. Location of Air Samplers Interior and Exterior from 04 Levels Up

Table 3-1 shows the Military Exposure Guidelines for exposure to HD (mustard) as defined by the U.S. Army Public Health Command.⁹ Since MeS is a simulant for HD, these concentrations can be compared to the amount of MeS detected outside and inside the ship to determine the potential threat to the crew.

Table 3-1. Military Exposure Guidelines for Various Concentrations of HD
MeS is a considered a simulant for HD

Army-defined HD (Mustard) Health Effects Levels	
Catastrophic	>10mg/m ³
Critical	10-2.5mg/m ³
Marginal	2.5-1.2mg/m ³
Negligible	1.2-0.4mg/m ³

Table 3-2 shows simulant deposit concentration as collected at several exterior locations around the ship and measured by mass spectrometry. As noted in the table, exterior locations of the ship were exposed to high levels of the simulant. At 12.7 mg/m³, one of the locations experienced concentrations well into the catastrophic level for human exposure to HD, and a second at 3.6 mg/m³ was in the critical range. These concentrations are consistent with the expected threat.¹⁰

Table 3-2. Mass Spectrometry Results for MeS of Exterior Air Samplers

Exterior Location	Simulant Concentration (mg/m ³)	Health Effects
04-62-1 CPS Zone 1	12.7	Catastrophic
04-62-2 CPS Zone 1	0.5	Negligible
01-30-3 CPS Zone 1	0.7	Negligible
1-65-2 CPS Zone 1	3.6	Critical
02-103-1 CPS Zone 4	0.4	Negligible
1-112-1 CPS Zone 4	0.3	N/A
03-114-2 CPS Zone 3	0.1	N/A
2-133-1 CPS Zone 3	0.1	N/A
04-36-1 CPS Zone 2	0.1	N/A
2-41-1 CPS Zone 2	0.1	N/A

⁹ "Health-based Chemical Vapor Concentration Levels for Future Systems Acquisition and Development." U.S. Army Center for Health Preparedness and Preventative Medicine (USACHPPM) Technical Report No. 64-FF-07Z2-07, February 2008. (USACHPPM is now known as the U.S. Army Public Health Command.)

¹⁰ *San Antonio Class (LPD-17) Chemical Warfare Threat Validation Report*. August 2011. SECRET

Table 3-3 shows the concentrations of simulant detected at various internal locations before and after the simulant was released. Simulant concentrations at all interior locations as measured by mass spectrometry began and remained below the threshold limit of detection (LOD) for the duration of the test. This indicates that the CPS was successful in preventing entry of high concentrations of simulant vapors outside of the CPS Zone 1 into the ship's protected spaces.

**Table 3-3. Mass Spectrometry Results for MeS of Interior Air Samplers
(Before and After the Simulant Spray)**

Interior CPS Zone Canister Location	Before and After Spray Mass Spec Results
CPS Zone 1 – Pilot House	Below LOD
CPS Zone 1 – Near ATM	Below LOD
CPS Zone 2 – Near DCA Stateroom	Below LOD
CPS Zone 2 – Decontamination Station	Below LOD
CPS Zone 3 – On top of Isolated Receptacle	Below LOD
CPS Zone 3 – Casualty Airlock Door	Below LOD
CPS Zone 4 – Near Emergency Light	Below LOD
CPS Zone 4 – Water Mist deck support	Below LOD

LOD: Limit of Detection (0.000651 mg/m³)

Countermeasure Wash Down System Functionality

Prior to the simulated chemical attack, a leak in the pilot house overhead (roof) occurred during an activation of the CMWDS. The leak, which was determined to be from a stuffing tube in which the packing failed, was repaired before the simulant was sprayed on the ship. Following the simulant release, the CMWDS functioned as designed.

Two anomalies were observed during and after the CMWDS activation:

- The gunwales on the bridge wings did not drain sufficiently and could allow accumulation of contaminated water. This was noted in previous testing.¹¹
- Depressions in the weather decks allow standing water to collect and therefore the potential for contaminated water to accumulate.

Equipment Decontamination Demonstration

In order to demonstrate the crew's ability to decontaminate the ship and equipment, an additional dissemination of MeS via hand-held sprayer was released in the boat valley, and the crew used fire hoses and scrub brushes to decontaminate the affected area (Figure 3-5) in accordance with the ship's CBR bill.

¹¹ See DOT&E's "USS *San Antonio* (LPD-17) Class Amphibious Transport Dock Ship Combined Operational and Live Fire Test and Evaluation Report." June 2010.



Figure 3-5. Decontaminating affected area in the Boat Valley

The efficacy of the decontamination in the boat valley was unclear. Although there was no referee equipment to verify the continued presence of simulant, the wintergreen smell of the simulant was apparent in the boat valley even after the decontamination was completed. The crew did not conduct an additional survey of the area to assess residual contamination as specified in the ship's CBR Bill. The crew's only means of conducting a survey of personnel or equipment after a chemical event is with the M256 kit. The long response time of the M256 kit (~20 minutes) makes it an ineffective tool for conducting thorough surveys to determine the extent of contamination. Lacking a portable rapid vapor detection device complicates the crew's ability to conduct post-decontamination inspections on or in the ship or if agent is present on crewmembers who have been decontaminated. Previous Navy acquisition systems have failed to deliver hand-held detectors that are suitable for shipboard use due to high numbers of false alarms. Similarly, the legacy IPDS chemical vapor detector is in the process of being removed from service due to a high number of false alarms. The newly-fielded IPDS-LR has a greatly reduced false alarm rate, indicating that recent technological advances may allow for development of a hand-held chemical agent vapor detector that is suitable for use in a shipboard environment. The Joint Program Executive Officer for Chemical and Biological Defense and the Navy should work to develop a more effective survey instrument for chemical warfare agents onboard ships.

Personnel Decontamination

The LPD class is required to achieve a specific decontamination throughput in the standard decontamination stations. To assess the throughput capability of these stations, personnel were cycled through Station 3 during the test. Figure 3-6 shows personnel in MOPP level 4 gear awaiting entry into Station 3 for decontamination. The demonstrated throughput rate met the ORD requirement.¹²

¹² Operational Requirements Document (ORD) for LPD-17 Amphibious Transport Dock Ship of 8 April 1996.

All four personnel decontamination stations were demonstrated to be functional at the time of the test; only two ships in the LPD-17 class (LPD-21 and LPD-22) had functioning litter-born casualty decontamination stations. The Navy should ensure that all LPD-17 class ships are retrofitted with functioning litter-born casualty decontamination stations.



Figure 3-6. Personnel Entering Decontamination Station 3 off Boat Valley

The FOT&E Test Plan called for one or two personnel to have simulant applied to their MOPP level 4 gear (so as to be contaminated with simulant prior to entering the decontamination station) to determine how well the station was able to remove simulant; this was not done during the test. Previous testing from other ship classes with the same decontamination stations did demonstrate their effectiveness using simulant-contaminated crewmembers.¹³

Each crewmember is assigned individually sized personal protective equipment, known as the Joint Service Lightweight Integrated Suit Technology (JSLIST), which includes a mask, gloves, boots, and suit. Masks are kept at the crewmember's work space, but suits are stored in individual duffle bags in lockers throughout the ship. The duffle bags are normally distributed to the crew prior to entering a chemical threat area. For this test, only those crewmembers directly involved with the test events were provided with training suits, although all crewmembers carried and donned their protective masks during the event. This event did not demonstrate the ability of the crew to disperse the stored JSLIST suits in a timely manner, a process that would take several hours to complete and requires the crew have advance warning of a chemical attack to take protective measures.

Sustained Amphibious Operations

Conducting normal amphibious operations includes launch and recovery of LCACs into and out of the LPD-17 class welldeck. During these operations, the welldeck crew must be able to communicate with the welldeck control room and transmit hand signals to the LCAC crew. If

¹³ "Developmental Testing (DT-IIIA) of the Collective Protection System (CPS) aboard the USS *Curtis Wilbur* (DDG-54)," NSWCDD December 1994.

the crew were wearing MOPP 4 gear, this would have to be done without interference from the MOPP 4 mask, gloves, and suit. On March 27-28, a demonstration was conducted in which the LPD-21 ramp marshal and safety observer donned MOPP 4 gear and launched an LCAC from the welldeck. The LCAC demonstration illustrated that the welldeck crews of the LPD-17 class ships can perform some normal operations while wearing MOPP 4 gear. As shown in Figures 3-7 and 3-8, the ramp marshal was able to guide the LCACs out of the welldeck without incident.



Figure 3-7. Ramp Crew Outfitting in MOPP 4 Gear



Figure 3-8. Ramp Crew Guiding LCACs Out of Welldeck while in MOPP 4 Gear

This demonstration was not intended to test the ability of the LCAC crew itself to conduct operations in a contaminated environment. The LCAC does not have a Collective Protection System, so the LCAC crew must wear protective equipment (JSLIST) in order to be protected in a contaminated environment. LCAC crews and ship crews typically carry out CBR

response training drills separately. The Navy should consider holding combined CBR training for LCAC crews and ship crews to ensure both are capable of carrying out sustained amphibious operations in a CBR environment. This concern will be examined during the Ship-to-Shore Connector (LCAC replacement) program's IOT&E.

This page intentionally left blank.

Section Four Recommendations

The Navy should implement and test during FOT&E the following recommendations to improve chemical, biological, radiological (CBR) defense capabilities on the LPD-17 class ships:

- The Navy should ensure that deck drainage, particularly areas in which large amounts of water can accumulate from the Countermeasure Wash Down System (CMWDS), are addressed.
- The Joint Program Executive Officer for Chemical and Biological Defense and the Navy should work to develop a more effective survey instrument than the M256 kit for chemical warfare agents for use onboard ships.
- The Navy should ensure ships with non-functional litter born casualty decontamination stations are retrofitted in order to render them functional.
- Because the LCAC crew was not in MOPP gear, the Navy should conduct a more robust test in the future (e.g., Ship-to-Shore Connector).
- The Navy should also consider holding joint CBR training for both LCAC and ship crews to ensure both are capable of carrying out sustained operations in a CBR environment.



OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

NOV 21 2012

OPERATIONAL TEST
AND EVALUATION

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

I have enclosed the LPD-17 Follow-On Operational Test and Evaluation (FOT&E) Report on Chemical, Biological, and Radiological (CBR) Defense as required by Sections 2399 and 2366, Title 10, United States Code. In the report, I conclude the following:

- The Navy demonstrated during the FOT&E CBR event in March 2012 that the LPD-17 class of ships can operate in a chemical warfare environment. The Improved Point Detection System – Lifecycle Replacement (IPDS-LR) detected a vapor cloud of chemical agent simulant prior to its contact with the ship. Additionally, the Chemical Protective System (CPS) prevented entry of simulant vapors into protected zones of the ship.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.

J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Adam Smith
Ranking Member





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

NOV 21 2012

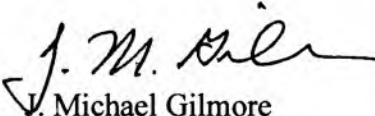
The Honorable C. W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

Dear Mr. Chairman:

I have enclosed the LPD-17 Follow-On Operational Test and Evaluation (FOT&E) Report on Chemical, Biological, and Radiological (CBR) Defense as required by Sections 2399 and 2366, Title 10, United States Code. In the report, I conclude the following:

- The Navy demonstrated during the FOT&E CBR event in March 2012 that the LPD-17 class of ships can operate in a chemical warfare environment. The Improved Point Detection System – Lifecycle Replacement (IPDS-LR) detected a vapor cloud of chemical agent simulant prior to its contact with the ship. Additionally, the Chemical Protective System (CPS) prevented entry of simulant vapors into protected zones of the ship.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

NOV 21 2012

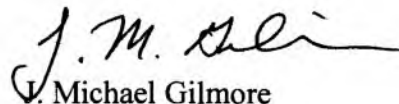
The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

Dear Mr. Chairman:

I have enclosed the LPD-17 Follow-On Operational Test and Evaluation (FOT&E) Report on Chemical, Biological, and Radiological (CBR) Defense as required by Sections 2399 and 2366, Title 10, United States Code. In the report, I conclude the following:

- The Navy demonstrated during the FOT&E CBR event in March 2012 that the LPD-17 class of ships can operate in a chemical warfare environment. The Improved Point Detection System – Lifecycle Replacement (IPDS-LR) detected a vapor cloud of chemical agent simulant prior to its contact with the ship. Additionally, the Chemical Protective System (CPS) prevented entry of simulant vapors into protected zones of the ship.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable John McCain
Ranking Member





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

NOV 21 2012

OPERATIONAL TEST
AND EVALUATION

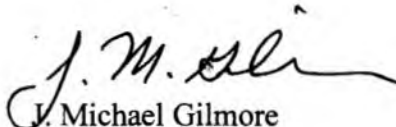
The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6025

Dear Mr. Chairman:

I have enclosed the LPD-17 Follow-On Operational Test and Evaluation (FOT&E) Report on Chemical, Biological, and Radiological (CBR) Defense as required by Sections 2399 and 2366, Title 10, United States Code. In the report, I conclude the following:

- The Navy demonstrated during the FOT&E CBR event in March 2012 that the LPD-17 class of ships can operate in a chemical warfare environment. The Improved Point Detection System – Lifecycle Replacement (IPDS-LR) detected a vapor cloud of chemical agent simulant prior to its contact with the ship. Additionally, the Chemical Protective System (CPS) prevented entry of simulant vapors into protected zones of the ship.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Thad Cochran
Ranking Member





Test and Evaluation of Materials Degradation

Corrosion Prevention, Mitigation, & Control

Briefing Prepared in Response to:
HASC Report 112-479, NDAA for FY2013
May 11, 2012



Overview



- *Corrosion Prevention, Mitigation, and Control (CPM&C) Background*
- *CPM&C Considerations*
- *Observed Problem Areas*
- *Operational Test and Evaluation CPM&C Observations*
- *Recent Lessons – F-22A*
- *F-22A Lessons Learned Applied to F-35*
- *DOT&E Actions and Considerations*
- *Additional Considerations*
- *Recommendations*



General Background



- Corrosion prevention, mitigation, and control (CPM&C)
 - Is a subset of overall system reliability, maintainability, and availability. CPM&C considerations influence both design and development activities as well as life cycle sustainment programmatic decisions.
- Success in meeting CPM&C qualification/specification criteria through system design and development is largely dependent on:
 - Robustness of the selected design
 - Understanding of the materials properties to be used in the system design
 - Rigor of the system design reviews conducted by the program management teams
 - Completeness of the systems engineering processes and developmental testing
- Similarly, successful CPM&C management across the life cycle of a given system is largely dependent on:
 - A funded CPM&C sustainment program that complements and supports the system as designed throughout the operational environments and expected service life of the system
 - The ability to address and resolve unanticipated CPM&C shortfalls that were not realized during system design, development, or pre-fielding test and evaluation



CPM&C Considerations



- Corrosion is not a new phenomena; CPM&C is one of many life cycle suitability considerations across all weapon systems
- CPM&C is a continuous process from system initial design, development and testing through life-cycle system sustainment:
 - Combination of system design considerations, as well as life cycle sustainment (prevention, inspection, maintenance, repair, replacement) of the system
 - Trade offs are made during system development phases with the intent of designing corrosion resistance and prevention properties that enable the system to function in the intended operational environment consistent with the program's planned CPM&C sustainment posture (inspection, maintenance, repair, replacement).
 - Sustainment is predicated on the "prevention and control" caveats – which drives inspection, repair, and (depending on the system) replacement of affected components and/or subsystems based on a given system's operational maintenance construct, sparing and replacement programs, and depot maintenance - all part of a weapon system's life cycle cost posture



Observed Problem Areas

- When systems fail to meet qualification/specifications prior to operational testing/fielding, root causes include:
 - Science and technology; inadequate design – *less than perfect understanding of the design/materials and physical integration processes; application of inappropriate/non-effective materials integration technologies*
 - Qualification testing – incomplete, non-robust systems engineering and/or developmental test and evaluation
 - *Inadequate direct government participation/oversight of corrosion testing*
 - *Non-robust environmental (climatic) qualification testing*
 - *Insufficient justification to verify closeout of corrosion control requirements*
 - *Limited ability to equate component-level accelerated corrosion test results to full-scale dynamic system performance over an expected 20-30 year service life*
- Post-Initial Operational Test and Evaluation problems occur with fielded systems when:
 - The robustness of the fielded system design doesn't support the program's planned CPM&C sustainment posture (inspection, prevention, repair, replacement) or vice versa. When this happens, consequences can include: reduced availability; increased manpower and resources costs, accelerated inspection/maintenance/repair/replacement, costly post-fielding retrofits or design changes, and increased life cycle costs



Operational Test and Evaluation CPM&C Observations



- DOT&E has not observed instances where CPM&C requirements have been “traded away” in the requirements development process.
- The overwhelming bulk of corrosion test and evaluation is accomplished early in system design and throughout the program’s systems engineering processes and developmental test and evaluation.
 - Given the relatively short duration of Initial Operational Test and Evaluation, it is unlikely that shortfalls in a system’s CPM&C capabilities may be fully discovered.
 - Notably, should significant CPM&C shortfalls be discovered in Initial Operational Test and Evaluation (IOT&E), there is little to no schedule margin to correct deficiencies. CPM&C problems realized in IOT&E may render the system not operationally effective or suitable.
- Incomplete knowledge of CPM&C shortfalls and/or reduced scope of environmental and corrosives testing during system development transfers the risk of discovery to IOT&E where there’s little if any opportunity to affect solutions



Recent Lessons – F-22A



- Prioritization of low observable requirements led to acceptance of other corrosion risks during system development
- Program implemented silver-filled conductive gap filler and paint in direct contact with aluminum structures – well known corrosive risk
 - No risk mitigation through increased testing during development; no trade studies to identify long-term costs of corrosion
- Performance-based acquisition approach:
 - Contractor corrosion testing without direct government participation; government accepted the risk and cost of failure
 - Insufficient justification to verify closeout of corrosion control requirements
- Environmental and occupational health concerns drove use of non-chromated outer mold line primer that didn't provide the needed corrosion protection; this led to additional corrosion issues in the field



Recent Lessons – F-22 (continued)



- Aircraft signature considerations drove design change in the number and size of drainage ports
 - Reduced from 201 initial design to 27 drainage ports
 - Remaining drainage ports proved insufficient in removing water and other corrosive liquids from aircraft cavities
 - Water intrusion issues at deployed locations led to post-fielding drain port redesign/retrofits
- Reduced scope climatic lab testing during developmental test and evaluation
 - Reduction from 6 to 3-month period
 - No severe wet weather testing
 - 2008 operational unit deployment to Guam experienced severe water intrusion and associate corrosion; forced redesign/addition of cockpit drain port
- No field test of final low observable coating system prior to Initial Operational Capability
 - 5-year Low Observables Over Time (LOSOT) testing from 2005-2010 necessary to determine stability, durability, and maintainability
- All operational testing in desert southwest environment
 - Operational units (Langley VA, Tyndall FL, Elmendorf AK) experienced additional corrosion issues not seen in desert southwest environmental
- Consequences: *Significant redesign/retrofit costs incurred post-IOT&E ~\$228M; increased manpower; reduced system operational availability*



F-22A Lessons Learned Applied to F-35



- Fewer outer mold line seams; gap filler less galvanically dissimilar from aluminum; less aluminum in outer mold line
- Early corrosion testing of conductive gap filler in representative operational environment
- Testing of full stack-up panel seams with simulated damage exposed to accelerated and outdoor (beach) exposures
- Sufficient internal drainage system
- Climatic lab testing planned to incorporate severe weather testing
- Flight testing in operational environments other than desert southwest ~3-4 years prior to IOT&E (Edwards CA, Eglin FL, Patuxent MD)



Overall Lessons Learned – F-22 to F-35



- Low observable aircraft CPM&C poses unique developmental and design challenges
 - Signature requirements must be balanced with evolving technologies
 - Trade-offs have consequences: signature vs. corrosion; signature versus drainage; optimum LO designs may be less than optimum for CPM&C considerations
 - Environmental considerations (e.g. non-chromated versus chromated primers) may result in unintended consequences that adversely affect CPM&C performance
- *Trades early in F-22 program (signature priority) resulted in adverse CPM&C consequences and significant retrofit costs post fielding*
 - *Potential problem areas were not highlighted in design reviews*
 - *Lack of government involvement and oversight of developmental qualification testing was a contributing factor – Total System Performance Responsibility (TSPR) contract type for both F-22 and F-35*
- Post-IOT&E CPM&C testing of low observables
 - 5-year F-22 Low Observables Stability Over Time (LOSOT) testing invaluable in assessing long-term system CPM&C durability, suitability, and maintainability
 - *Similar long-term testing approach for F-35 in work*



DOT&E Actions and Considerations



- Actions that DOT&E can, will, and does take to consider material degradation due to corrosion and associated impacts on operational effectiveness and suitability include the following:
 - Limitations (system quantities, test duration, basing, security, test range locations, and others) preclude testing in every possible operational environment. However, DOT&E conducts and will continue to conduct operational test and evaluation across the range of operational environments available during IOT&E periods. IOT&E – as a period of performance confirmation at the end of system development – cannot identify all unforeseen CPM&C shortfalls.
 - Where progress and results from developmental test and evaluation indicate potential shortfalls and challenges in CPM&C, DOT&E will include CPM&C in formal Operational Assessments prior to IOT&E.
 - Similarly, should progress in meeting CPM&C design specifications at programmatic milestone decision points prior to IOT&E indicate shortfalls in testing, or when novel materials and coatings are utilized (e.g. *low observables materials for aircraft*) DOT&E will require demonstration that system specification requirements are met as entrance criteria prior to IOT&E.
 - Where warranted based on system performance during developmental test and evaluation, DOT&E will direct additional CPM&C inspections and maintenance evaluations be incorporated into operational test and evaluation plans approved by the DOT&E.
 - For systems utilizing unique and novel materials and coatings (e.g. F-22 and F-35 low observable systems) experience has shown that conducting long-term testing over time has provided invaluable insight into the durability, maintainability, and sustainability of fielded systems. As was the case with the F-22 post-IOT&E 5-year Low Observables Stability Over Time operational test, DOT&E will continue to require such testing in the interest of informing such fielded systems' long-term operational effectiveness and suitability requirements are met.
 - In cases where CPM&C shortfalls are identified in IOT&E, DOT&E will require focused formal follow-on test and evaluation to determine the efficacy of CPM&C mitigation strategies implemented to address such shortfalls.



Additional Considerations

- Operational Test and Evaluation, occurring at the end of system development, affords only a limited duration in which to assess CPM&C characteristics of a given system. Accordingly, corrosion testing is primarily a function of early systems engineering design and developmental testing prior to IOT&E. As such, experience with recent systems (e.g. the F-22A & F-35) suggest actions that the Acquisition Community and Developmental Test and Evaluation agencies should implement to include:
 - Ensure government oversight and active participation in CPM&C qualification testing early during initial systems engineering design and component and subsystem developmental test and evaluation. Delegating CPM&C design and developmental decisions to contractors without government participation or oversight can have adverse consequences (e.g. F-22A outer mold line corrosion issues and post IOT&E retrofit costs).
 - Robust climatic laboratory environmental and corrosives testing during system development is crucial to identifying potential shortfalls and problems. Reducing the scope of climatic laboratory testing to accommodate near-term program budget and schedule challenges can result in unplanned and unbudgeted fielded system redesign or retrofit costs.
 - During developmental test and evaluation, conduct full system-level testing in diverse environments representative of those in which the fielded system will operate should be considered to provide insight into CPM&C capabilities and limitations.
 - Programs utilizing unique and novel materials and coatings (e.g. F-22A and F-35 low observable systems) should plan and program for post-operational fielding, long-term testing over time to ensure CPM&C stability, suitability, and maintainability features meet life-cycle performance requirements.



Recommendations



Early, informed, and complete design, systems engineering, and developmental test and evaluation with direct government involvement and oversight afford the best opportunity to mitigate CPM&C shortfalls and associated risks.

Development efforts must encompass such practices, and be informed by lessons learned across similar development efforts.



OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OCT 26 2012

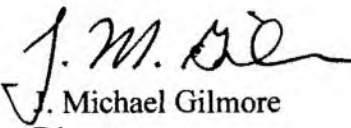
OPERATIONAL TEST
AND EVALUATION

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

I have enclosed a response to Committee Report 112-479, May 11, 2012 requesting a briefing addressing Test and Evaluation of Materials Degradation. In the briefing I have provided background information on corrosion mitigation, prevention, and control; addressed recent problem areas and lessons learned in the test and evaluation community; present actions taken by DOT&E; and recommendations and considerations for other agencies.

Should the Committee require additional information, my point of contact is Mr. Greg Barlow. He can be reached at greg.barlow@osd.mil, or 703.590.2999.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Adam Smith
Ranking Member



Director, Operational Test and Evaluation

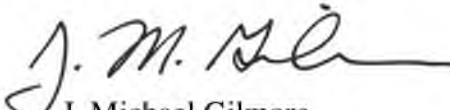
Joint Warning and Reporting Network (JWARN)

Major Automated Information System (MAIS)
Operational Evaluation



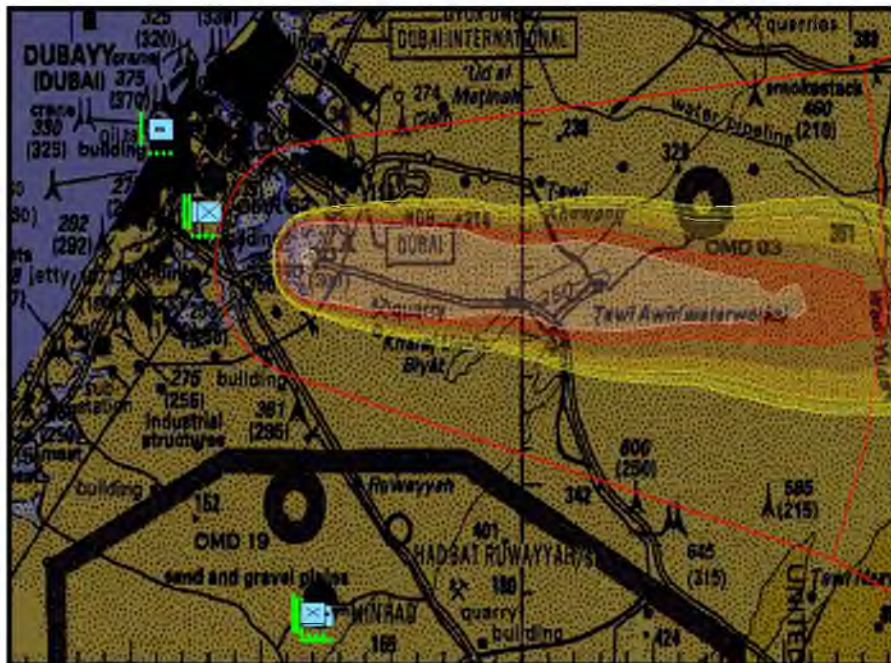
October 2012

This report on the Joint Warning and Reporting Network (JWARN) assesses the adequacy of testing and the operational effectiveness and suitability of the JWARN in support of a Full Deployment Decision on Global Command and Control System – Maritime (GCCS-M) for the Navy.


J. Michael Gilmore
Director



Navy Operations Specialist Employing JWARN during the Operational Test



JWARN software screen shot depicting Chemical, Biological, Radiological, and Nuclear Downwind Hazard Warning Area

Executive Summary

This report supports the Joint Warning and Reporting Network (JWARN) Increment 1 Full Deployment Decision on Global Command and Control System–Maritime (GCCS-M) for the Navy. The evaluation is based upon a follow-on operational test of JWARN Increment 1 hosted on GCCS-M and GCCS –Joint (GCCS-J) with Plain Language Address (PLA) capability conducted June 25-29, 2012, in San Diego, California.

JWARN software is currently deployed on the following Joint and Service command and control (C2) systems: GCCS–Army (GCCS-A), GCCS-J, and Command and Control Personal Computer (C2PC)/Joint Tactical Common Workstation (JTCW).

Operational Effectiveness

JWARN software hosted on GCCS-M is operationally effective to provide chemical, biological, radiological, and nuclear (CBRN) warning reports to units operating 10 or more kilometers from an initial CBRN release. Using JWARN, reports can be generated and received in time for such units to institute force protection actions before encountering CBRN hazards. JWARN enhances nuclear, biological, and chemical (NBC) situational awareness and supports operational decision making in response to basic NBC attacks by automating the NBC warning, reporting, and hazard prediction process. However, JWARN operators had difficulty in completing NBC warning and reporting for complex attack scenarios. JWARN demonstrated interoperability with GCCS-M on the test network.

Prior to operational testing, the Navy recognized that GCCS-J, the C2 system used by the service's Maritime Operations Centers (MOCs), was not interoperable with GCCS-M when ships operate in emissions control. The GCCS-J program office developed a modification to enable GCCS-J to transmit messages in PLA format. During testing, the MOC used the developmental version of GCCS-J with PLA. Cross-Service warnings using GCCS-J with PLA in test were likely 2 to 5 minutes faster than could be expected if GCCS-J with PLA is not deployed at Navy MOCs. Using GCCS-J with PLA led to 4 missions where units were warned in time to take protective action that would not have occurred if GCCS-J operators had to manually type the information into another C2 system in order to send the warning report. The Navy should work with the GCCS-J Program Manager to coordinate deployment of GCCS-J with PLA to its MOCs and other theater headquarters to enable timely cross-battle group and cross-Service warning and reporting when ships are implementing emissions control procedures.

System Overview

JWARN is software designed to automate the chemical, biological, radiological, and nuclear (CBRN) hazard warning and reporting processes. JWARN provides a single automated CBRN warning, reporting, and analysis tool for battle groups, battalions, squadron-level units, and above to support joint operations. The Services intend JWARN to improve the speed and accuracy of the North Atlantic Treaty Organization (NATO) CBRN basic warning and reporting process, as defined in Allied Technical Publication (ATP)-45(C), through automation. JWARN,

like the ATP-45 process it automates, provides limited immediate warning capability for personnel that are in the immediate vicinity of an attack.

Test Adequacy

Follow-on Operational Test and Evaluation (FOT&E) was adequate to determine JWARN operational effectiveness and suitability on GCCS-M in a simulated operational environment. FOT&E was conducted in accordance with the DOT&E-approved test plan. Additional follow-on operational testing of JWARN on GCCS-M in an operational environment is planned to fully assess JWARN's operational performance.


Operational Suitability

JWARN is operationally suitable for use by the Navy on GCCS-M. JWARN software hosted on GCCS-M experienced one operational mission failure (OMF) during 300 hours of operation during FOT&E (100 hours MTBOMF at the 80 percent lower confidence limit). The Navy user-defined reliability requirement is 100 hours MTBOMF. JWARN New Equipment operator training was adequate to successfully accomplish NBC warning and reporting for 83 percent of basic attack scenarios during FOT&E. JWARN operators had difficulty in completing NBC warning and reporting for complex attack scenarios.

Recommendations

DOT&E recommends the following actions:

- The Navy should work with the GCCS Program Office to request and coordinate deployment of GCCS-J with PLA capability to its Maritime Operations Centers.
- Once the Navy deploys JWARN on GCCS-M, the Commander Operational Test and Evaluation Force should conduct additional FOT&E of JWARN on a Navy ship with an operational network and naval communications systems to demonstrate interoperability on an operational network.
- The Navy should work with the JWARN Program Manager to develop and field computer-based scenario training that includes basic to advanced scenarios to reinforce TTPs, increase operator-level skills, and provide sustainment training for JWARN operators.


J. Michael Gilmore
Director

Contents

System Overview	1
Test Adequacy	9
Operational Effectiveness	15
Operational Suitability	21
Recommendations	25

This page intentionally left blank.

Section One

System Overview

This report supports the Joint Warning and Reporting Network (JWARN) Increment 1 Full Deployment Decision on Global Command and Control System-Maritime (GCCS-M) for the Navy. The evaluation is based upon a follow-on operational test of JWARN Increment 1 hosted on GCCS-M and GCCS-Joint (GCCS-J) with Plain Language Address (PLA) capability conducted June 25-29, 2012, in San Diego, California.

The JWARN Increment 1 is software designed to automate the chemical, biological, radiological, and nuclear (CBRN) hazard warning and reporting processes. JWARN is currently deployed on the following Joint and Service command and control (C2) systems: GCCS-Army (GCCS-A), GCCS-J, and Command and Control Personal Computer (C2PC)/Joint Tactical Common Workstation (JTCW).

System Overview

JWARN Increment 1 software resides on Joint and Service C2 systems. JWARN provides a single automated CBRN warning, reporting, and analysis tool for battle groups, battalions, squadron-level units, and above to support joint operations.

The Services intend for operators to use JWARN to:

- Create reports of CBRN events for transmission to higher headquarters and assigned units
- Create weather reports to support CBRN hazard prediction
- Perform analysis of CBRN information and warn units at risk from CBRN hazards
- Support CBRN battlefield management with nuclear exposure calculations, computation of cloud arrival times, route planning, and creation of CBRN annexes to operational plans and orders
- Create retrievable databases of CBRN events and reports
- Access Department of Defense (DoD) CBRN databases, references, and guidebooks
- Track information on unit operational status, CBRN equipment readiness, and consumption rates of CBRN supplies.

The Services intend JWARN to improve the speed and accuracy of the North Atlantic Treaty Organization (NATO) CBRN basic warning and reporting process, as defined in Allied Technical Publication (ATP)-45(C), through automation. JWARN, like the ATP-45 process it automates, provides limited immediate warning capability for personnel that are in the immediate vicinity of an attack. Observers using radio communications or hand signals and alarms triggered by local CBRN sensors provide immediate tactical warning of a CBRN hazard.

ATP-45(C) defines nuclear, biological, and chemical (NBC) report message formats to assure interoperability among coalition forces. Table 1-1 describes these report message formats.

Table 1-1. ATP-45(C) NBC Report Definitions.

NBC Report	Definition
NBC-1	Observer's Report: Basic and initial follow-up data about an NBC attack is used and provided by the observing unit.
NBC-2	Evaluated Data Report: One or more allocated NBC 1 reports provide the basis for the NBC 2 report, which relates reports received from different sources.
NBC-3	Immediate Warning of Predicted Contamination and Hazard Areas Report: Downward hazard areas are predicted by using NBC 2 reports and weather information as the basis for the NBC 3 report.
NBC-4	Reconnaissance, Monitoring, and Survey Results Report: The NBC 4 report is generated when a unit detects CBRN hazards through monitoring, survey, or reconnaissance.
NBC-5	Areas of Actual Contamination Report: Once JWARN processes the NBC 4 reports, a NBC 5 report will be generated that depicts the area(s) of actual contamination.
NBC-6	Detailed Information on Nuclear, Chemical, Biological, or Release Other Than Attack (ROTA) Events Report: This report summarizes information concerning attack(s) or incident(s).

JWARN uses the Common Operating Picture (COP) of the host C2 network to display ground maps, unit locations, the location of NBC events, and the predicted or actual location of NBC hazards to support Commanders' situational awareness and ability to respond. JWARN uses the C2 host system information on unit location to send NBC reports.

JWARN and the NBC Warning and Reporting Process

The ATP-45 process begins with an NBC-1 observer's report. An observer sends an NBC-1 report using voice or other means of communication to a unit that has JWARN capability. The JWARN operator manually enters this information into JWARN. JWARN requires the following information to generate an NBC-1 report:

- Date
- Time
- Location of the attack or observer and relative direction of the attack from the observer
- Release method and estimate of the quantity of the release
- Terrain type
- Weather

If the information entered is not complete, JWARN will alert the operator to the missing information necessary to generate an NBC-1 report.

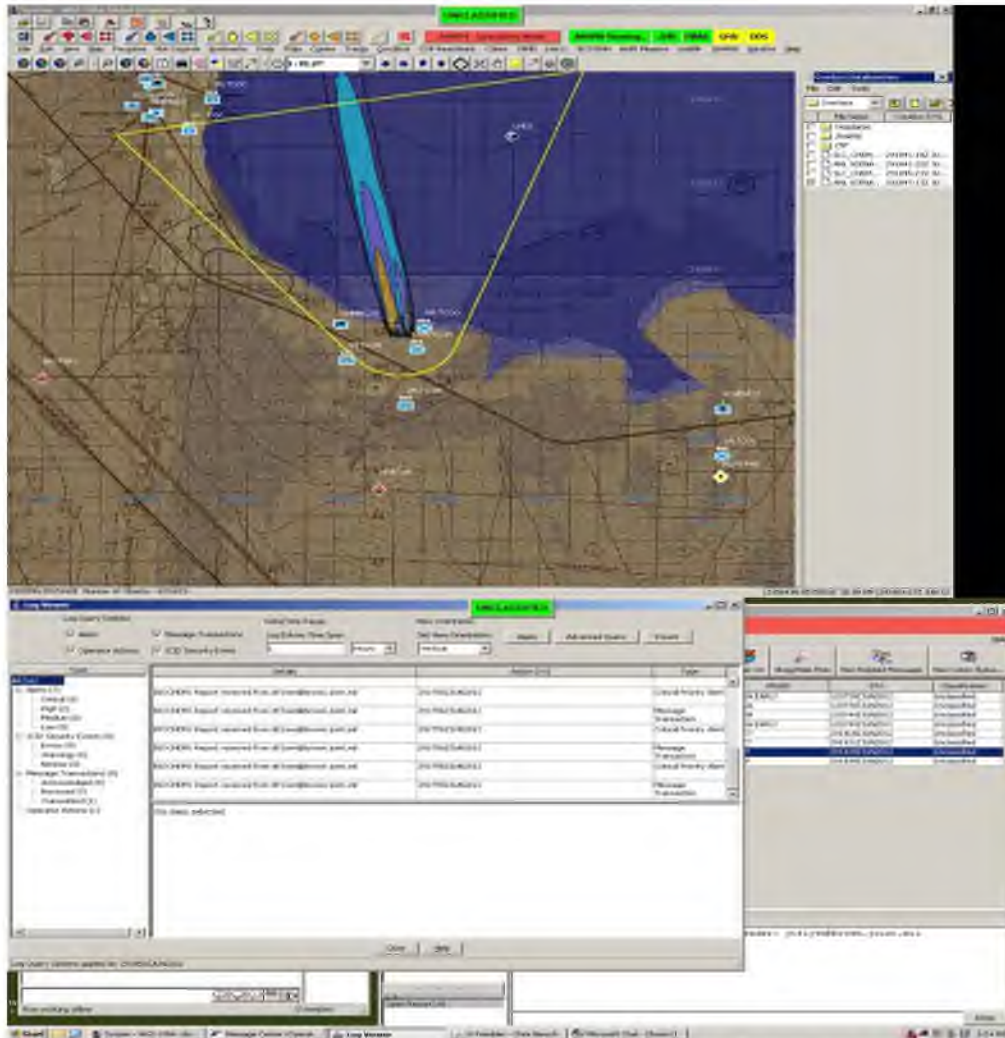
The JWARN operator uses the software to correlate multiple NBC-1 reports, using proximity and time as correlation factors, to determine if the NBC-1 reports relate to a single attack or multiple attacks. The operator requests that JWARN generate an NBC-2 report with the correlated results. The NBC-2 provides data for the JWARN operator to create an NBC-3 text file, which contains information to calculate and graphically display a downwind hazard prediction. The JWARN operator uses the host C2 system's unit-track database to determine unit position locations and identify units at risk. The operator can select units to receive the NBC-3 or JWARN can automatically send the NBC-3 to all units at risk. Upon receipt of an NBC-3, the unit at risk will institute force protection measures. The unit may use JWARN and received NBC-3 data to plot the hazard.

The ATP-45 hazard prediction overestimates the area in which units at potential risk receive hazard warnings. JWARN displays the hazard plot as a circle around the attack location and a downwind prediction in the form of a triangle. The type of CBRN attack, wind direction, and atmospheric stability also affect the shape of hazard plots. The JWARN ATP-45 downwind hazard predictions or hazard plots are the primary means to warn units at risk.

JWARN and JEM Downwind Hazard Predictions

The Services require JWARN to be interoperable with the Joint Effects Model (JEM), which produces refined CBRN hazard predictions using advanced modeling tools. Although the JEM hazard plot is more precise than the JWARN ATP-45 plot, its precision requires more detailed attack information, and is computationally intensive. As the JWARN operator receives additional information, he or she may elect to use JEM to plot downwind and topical hazards. Commanders may use JEM plots to select locations for reconnaissance teams to conduct surveys.

A C2 system operator may display ATP-45 hazard plots and JEM plots at the same time on the COP. Figure 1-1 depicts a JWARN ATP-45 hazard plot (yellow) and a JEM downwind hazard plot (blue) from a nerve agent rocket attack.



Navy Concept of Employment

Naval Task Force Commanders may order ships to maneuver to avoid NBC airborne contamination. Individual ship commanders order shipboard force protection measures, such as clearing decks of non-essential personnel, closing hatches and doors, upgrading individual Mission Oriented Protective Posture (MOPP), manning decontamination stations, and securing internal ventilation in response to CBRN hazard warnings.

Navy forces ashore, including Maritime Operations Centers (MOC), use JWARN hosted on GCCS-J. Navy MOCs are responsible for sharing JWARN warnings and reports between naval task forces, other joint forces operating in the theater, and higher headquarters.

Navy Command and Control Network

JWARN resides on GCCS-M client computers on Navy ships and on GCCS-J client computers in MOCs ashore. Messages leave the client and are sent to a Microsoft Exchange server and from there, leave the ship via Naval Modular Automated Communications System (NAVMACS) computers as e-mail. NAVMACS controls message traffic to and from the ship.

Ship-to-MOC

Messages leave a ship using the NAVMACS computers, and are sent to a satellite and then to a shore facility for relay to the MOC. The ship-to-MOC architecture is depicted in Figure 1-2.

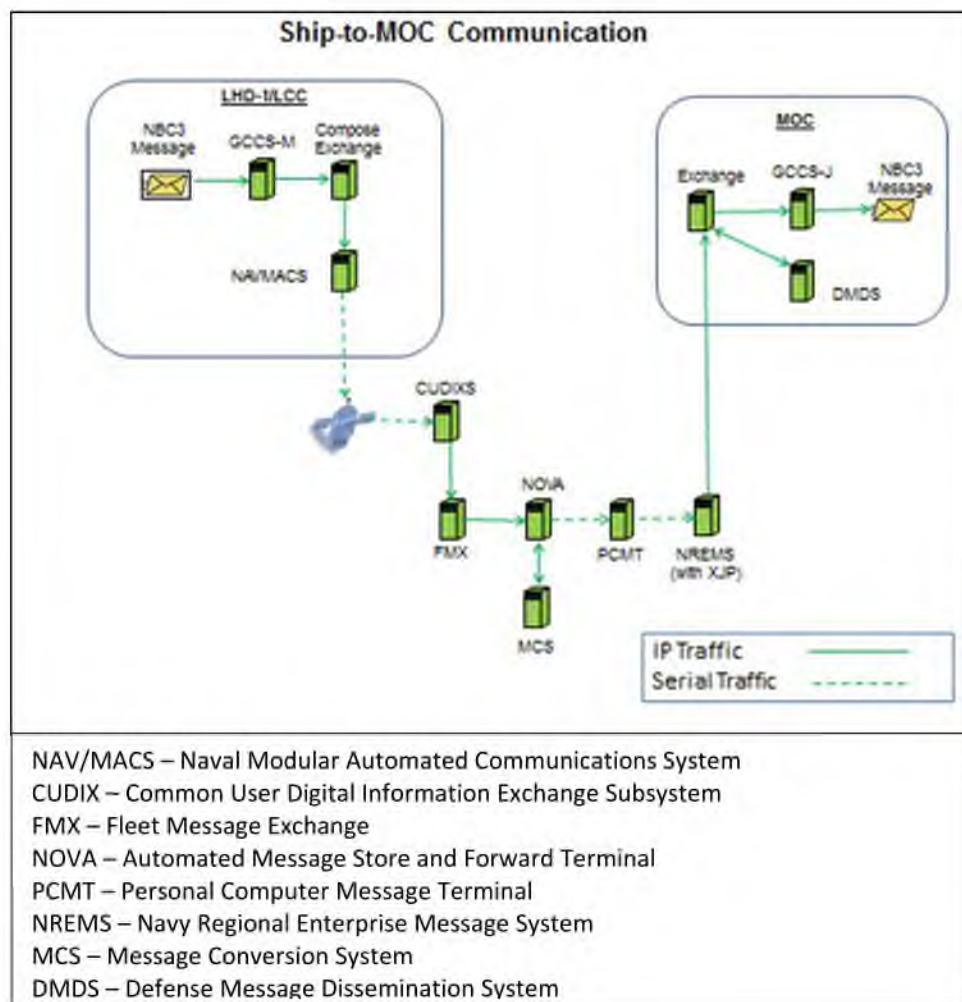


Figure 1-2. Ship-to-MOC Architecture

MOC-to-Ship

Messages from the MOCs to ships pass through a shore-based communications facility and are then routed to ships via one of three communications paths.

The Navy operational network switches between communications paths automatically depending on availability. The selection of primary, secondary, and tertiary paths is transparent to the user. If the primary and secondary paths fail, the last resort is to send a message to the ship using Fleet Broadcast. Fleet Broadcast is a radio transmission that is received by the ship from shore facilities. The detailed MOC-to-ship architecture is depicted in Figure 1-3.

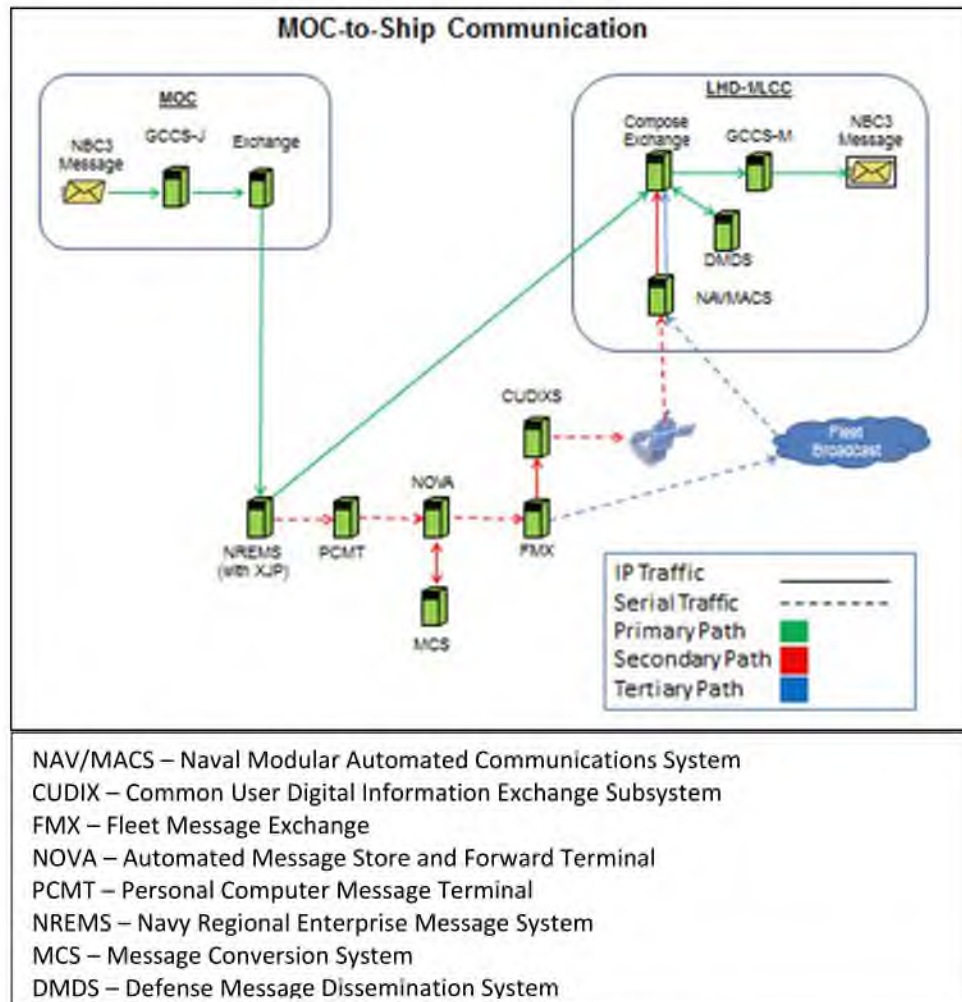


Figure 1-3. MOC-to-Ship Architecture

Ship-to-Ship

Messages leaving a ship pass through a satellite to a shore facility, back to a satellite, and to the destination ship. The ship-to-ship architecture is depicted in Figure 1-4.

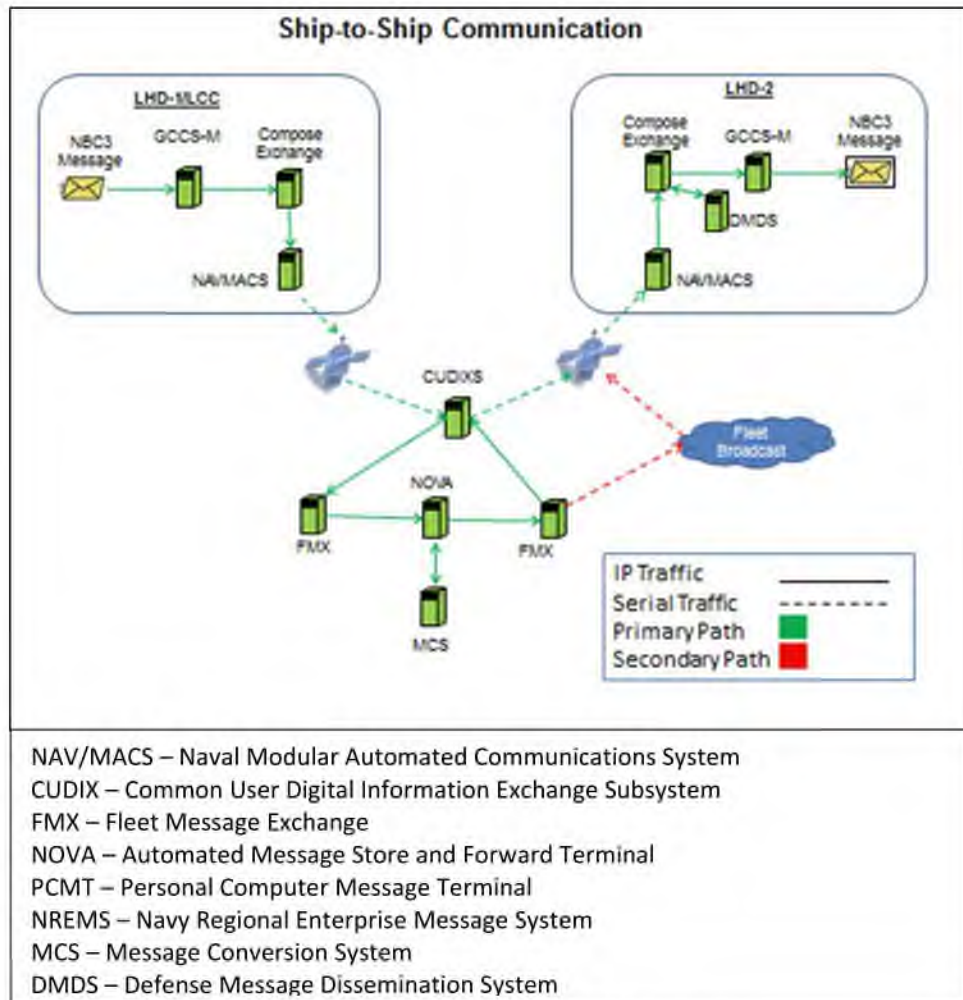


Figure 1-4. Ship-to-Ship Architecture

Special Considerations for Emissions Control

Naval forces employed in combat use Emissions Control (EMCON) procedures to manage or eliminate active emissions to prevent an adversary from locating ships. Navy Task Forces use EMCON to avoid detection en route to objective areas, or during naval and amphibious operations in littoral areas to avoid being targeted. Hazards originating ashore requiring ground forces to warn ships at sea would have to be fairly large to reach a ship at sea.

During the most restrictive level of EMCON, ships will shut down all incoming and outgoing e-mail services. JWARN messages are typically sent as e-mail messages. This action prevents ships from receiving JWARN messages as e-mail from MOCs or ground forces using GCCS-J. The only way to ensure NBC warnings are received by a ship in EMCON is for the message to be sent by Fleet Broadcast to a specific ship using a PLA message. PLA is the method used to denote the command short title and sometimes geographic location used in message addressing.

The currently deployed version of GCCS-J does not have PLA capability. A sailor in the MOC must manually enter the data from an incoming GCCS-J JWARN message into a legacy

version of C2PC for transmission to specific ships as a PLA message. This process takes approximately 2 to 5 minutes.

JWARN Key Performance Parameters (KPPs)

Table 1-2 contains a summary of the JWARN Increment 1 Key Performance Parameters (KPPs). In a memorandum dated April 26, 2011, the Joint Requirements Oversight Council deferred the sensor data input and warning dissemination requirements contained in KPPs 1 and 2(a) until JWARN Increment 2. These KPPs are not addressed in this evaluation. The KPPs in bold apply to the JWARN Increment 1.

Table 1-2. JWARN Key Performance Parameters.

KPP	Threshold Requirement
1. Sensor Data Input	<p>1a. JWARN shall collect and analyze inputs from connected sensors, such as sensor data and sensor alert status.</p> <p>1b. JWARN shall query for inputs from connected sensors, such as sensor data and sensor alert status.</p>
2. Warning Dissemination	<p>2a. JWARN shall automatically generate and send NBC 1 and NBC 4 reports with data from <i>connected sensors</i> within 2 minutes.</p> <p>2b. JWARN shall generate, edit, and disseminate NBC reports.</p> <p>2c. JWARN shall provide the operator the capability to select immediate, delayed, or on-command option for sending an NBC report to pre-designated or operator-selected recipients.</p> <p>2d. JWARN shall verify and record addressee receipt of NBC reports.</p> <p>2e. JWARN shall generate and disseminate ATP-45 plots and disseminate high fidelity plots and overlays to affected personnel.</p>
3. Net Ready:	<p>The system must fully support execution of joint critical operational activities identified in the applicable joint and system integrated architectures and the system must satisfy the technical requirements for transition to Net-Centric military operations to include:</p> <ul style="list-style-type: none"> • DoD Information Technology Standards Registry (DISR) mandated Global Information Grid Information Technology (GIG IT) standards and profiles identified in the Technical View-1 (TV-1) • DISR mandated GIG Key Interface Profile (KIP) identified in the KIP declaration table • Net Centric Operations Warfare – Reference Model (NCOW RM) Enterprise Services • Information Assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Approval to Operate by the Designated Approval Authority • Operationally effective information exchanges, and mission critical performance and Information Assurance attributes, data correctness, data availability, and consistent data processing specified in the applicable joint and system integrated architecture views.

JWARN has a reliability requirement of 1,367 hours Mean Time Between Operational Mission Failure (MTBOMF) when operating on a host C2 system and connected to sensors. The Navy has amended this requirement to be 100 hours MTBOMF for JWARN software operating on GCCS-M.

Section Two

Test Adequacy

Follow-on Operational Test and Evaluation (FOT&E) was adequate to determine JWARN operational effectiveness and suitability on GCCS-M in a simulated operational environment. Additional follow-on operational testing of JWARN on GCCS-M in an operational environment will be conducted to fully assess JWARN's operational performance.

The U.S. Army Test and Evaluation Command, supported by the Navy's Commander Operational Test and Evaluation Force and the Joint Interoperability Test Command, conducted FOT&E on JWARN Increment 1 June 25 – 29, 2012, at the Space and Naval Warfare (SPAWAR) facilities in San Diego, California. JWARN operational testing was conducted in accordance with the DOT&E-approved test plan.

Operational Test Description

The FOT&E was based upon a notional stability and support operation in a fictitious Persian Gulf country which was threatened by an enemy with a full range of CBRN capabilities. A Joint Task Force (JTF) with a subordinate Army Brigade Combat Team (BCT) was located ashore. An Amphibious Task Force, consisting of an amphibious command ship (LCC), two Landing Helicopter Docks (LHD1 and LHD2), and a destroyer (DDG), conducted amphibious operations in support of the JTF mission to defeat enemy forces and stabilize the friendly country. During the test, each unit was represented by at least one Army or Navy JWARN operator who performed NBC reporting functions using JWARN. The LCC was represented by one enlisted JWARN operator, one enlisted JEM operator, and one aviation field grade naval officer representative of a Combat Intelligence Center Watch Officer. The test included notional Army and Marine Corps companies located in hazard areas requiring NBC warning reports to be sent across Services.

A Navy MOC, notionally located ashore in another friendly country some distance from the JTF area of operations, routed NBC messages from ground units to the naval amphibious force. The notional unit locations and force lay down in the scenario were in accordance with Service doctrine. Ship locations changed with each phase of the joint operation. The LHDs used a notional Sea Port of Disembarkation to support the unloading of Marine landing forces. Figure 2-1 depicts the notional force deployment.

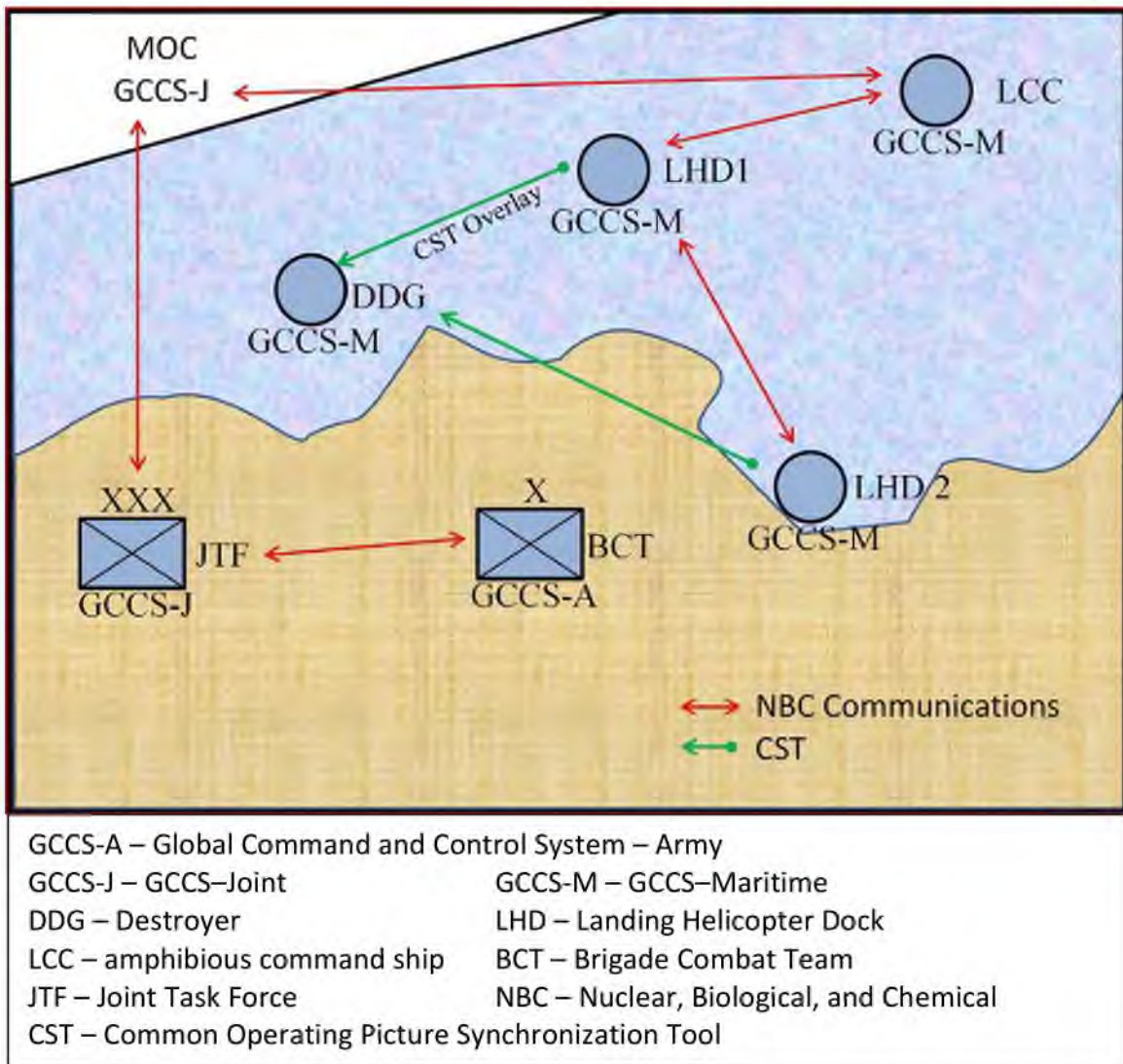


Figure 2-1. Force Deployment

The Navy LCC and LHDs used GCCS-M (v4.1) (Force Level) and the DDG used GCCS-M (v4.1) (Unit Level). Since the DDG does not have JWARN capability, the LCC or LHDs warned the DDG of CBRN hazards by sending it picture files of ATP-45 or JEM plots using the GCCS-M COP Synchronization Tool (CST).

The MOC used a developmental version of GCCS-J modified to support PLA. This enabled the MOC to automatically transmit incoming non-PLA e-mail messages as PLA messages to the LCC without re-entering the data in C2PC. The GCCS Program Manager plans to use data on GCCS-J with PLA from the FOT&E to support a decision on deploying GCCS-J with PLA in the future.

Table 2-1 identifies the C2 host system and JWARN software versions employed by each test unit.

Table 2-1. FOT&E Software Versions

Unit	C2 Host System	JWARN version
LCC	GCCS-M v4.1 Force Level (COMPOSE 4.0)	4.1.0.2
LHD-1	GCCS-M v4.1 Force Level (COMPOSE 4.0)	4.1.0.2
LHD-2	GCCS-M v4.1 Force Level (COMPOSE 3.5)	4.1.0.2
DDG	GCCS-M v4.1 Unit Level (COMPOSE 4.0)	4.1.0.2
MOC	GCCS-J v4.2.0.7	4.2.0.6
JTF	GCCS-J v4.2.0.7	4.2.0.6
BCT	GCCS-A BC 10.0.0 P07.1 (B4.1b Patch 7.1)	4.1.1.11 P4

FOT&E Operator Training

The JWARN Program Manager provided 40 hours of JWARN software New Equipment Training to JWARN operators prior to the start of test. No GCCS training was provided prior to the FOT&E. Test participants had varying levels of prior experience with GCCS-M. Navy CIC operators receive GCCS-M training at an advanced training school.

Test participants had a half-day to familiarize themselves with the test systems and participated in a half-day pilot test prior to the five-day operational test. The operational test consisted of 40 vignettes. The test team initiated each vignette by injecting one or more observation reports or NBC-1 messages to stimulate the warning and reporting sequence. The observations and NBC-1s were structured to provide the receiving unit with a sequence of reports. In general, more than one NBC-1 was required to provide sufficient information on the attack to prepare the NBC-3.

The attack scenarios were either basic or complex. Basic scenarios involved a single attack with observations received from a single source. Complex scenarios involved multiple attacks in combination with observation reports sent by multiple sources. Complex scenarios required the operator to synthesize information from a series of incomplete observer reports. No single observation report contained sufficient information to complete an NBC-3 report.

Table 2-2 depicts the factors and levels used to construct the operational test vignettes.

Table 2-2. Factors and Conditions Used in Test Design

Factor	Level
Attack type	Chemical, biological, radiological, nuclear, and toxic chemicals
Unit attacked	LCC, LHD1, LHD2, DDG, JTF, BCT
Communications path	Ground-to-ship, ship-to-ground, ship-to-ship, and ground-to-ground
Report type	NBC 1-5, SITREP, weather, and other
Distance of unit from attack area	0-5 km, 5-10 km, 10-15 km, >15 km
Units warned	LCC, LHD1, LHD2, DDG, JTF, BCT
Scenario type	Basic and complex

Test Network

Test communications hardware and software were representative of that used by the Navy. Each node had its own JWARN client, host C2 system, and communications, mapping, and unit location servers. The ground and naval units' client computers and servers were located in a laboratory at the Sea Systems Command Pacific facility in San Diego, California. A satellite simulator was used to replicate the delay associated with satellite communications for the Navy. The satellite simulator and associated systems were located in Charleston, South Carolina.

For the FOT&E, JWARN messages followed either the primary or secondary communications paths for MOC-to-ship and the MOC always used GCCS-J with PLA. All ship communications used PLA messages. Since the ships were not in EMCON for the exercise, they used Microsoft Chat for internal tactical communications. Ground units used conventional non-PLA GCCS-A or GCCS-J e-mail (Brigade-to-JTF and JTF-to-MOC) to communicate.

Test Limitations

Personnel Manning

With the exception of the LCC, operational cells did not have field grade watch officers or senior NBC enlisted personnel to assist the junior JWARN operators and make decisions. The command ship was represented by a field grade naval aviator, who was representative of a CIC watch officer. The lack of senior personnel overseeing activities at each notional ship contributed to operator difficulty when faced with multiple attacks at the same time.

GCCS-J with PLA

Prior to FOT&E, the Navy recognized that GCCS-J, the C2 system used by MOCs, was not interoperable with GCCS-M when ships operate in EMCON mode. The GCCS-J program officer developed a modification to enable GCCS-J to transmit messages in PLA format. During FOT&E, the MOC used the developmental version of GCCS-J with PLA. This test artificiality was created to test GCCS-J with PLA for joint use. Cross-Service warnings using GCCS-J with PLA in test were likely 3 to 5 minutes faster than could be expected if GCCS-J with PLA is not deployed at Navy MOCs. Using GCCS-J with PLA led to four missions where units were warned in time to take protective action that would not have occurred if GCCS-J operators had to manually type the information into another C2 system in order to send the warning report.

JEM Templates

JWARN and JEM use different input variables for Release Other Than Attack (ROTA), Toxic Industrial Chemical (TIC), and Incident Source Model (ISM) analysis. For example, JWARN uses the terms small, medium, and large to describe a TIC attack while JEM uses specific quantities expressed as gallons of agent. The JWARN Program Manager has developed templates for the JWARN operator to use when requesting a JEM plot. When the JWARN operator selects the normal ATP-45 variables, the template converts the JWARN input into meaningful terms for JEM. The ROTA templates were not loaded prior to test. This prevented the JWARN operators from creating JEM plots for ROTA events.

Test Network

The test network was operationally representative but lacked the redundant servers found aboard Navy ships. The test lacked near real-time maintenance to respond to computer and network issues. Aboard ship, Navy technicians are available to troubleshoot and repair NAVMACS and other communication computers. During test night operations, technicians were off duty and had to be recalled when problems arose. This increased repair times during critical outages. Additionally, software errors in some of the network systems caused frequent re-boots. The Navy has implemented a Fleet-wide correction for one of these errors.

Operationally, there are primary, secondary, and tertiary communications paths. If one path fails, the system automatically switches to another. During FOT&E, the Test Command Center forced the use of a particular communications path. Testers simulated communication failures by disconnecting one or more computer data input cables. This resulted in communication failures during test that would have caused an automated switch to another communications path on an operational network.

Due to software errors in some of the network systems, computer technicians had to reboot network components every twelve hours. In one instance during the test, this resulted in a 20-minute delay in the receipt of a JWARN message. The lack of availability during reboot and the lack of redundancy negatively impacted operational mission accomplishment during the test.

This page intentionally left blank.

Section Three

Operational Effectiveness

JWARN software hosted on GCCS-M is operationally effective to provide CBRN warning reports to units operating 10 or more kilometers from the initial CBRN release in time for units to institute force protection actions before encountering CBRN hazards. JWARN enhances NBC situational awareness and supports operational decision making in response to basic NBC threats by automating the NATO ATP-45 process of NBC warning, reporting, and hazard prediction. JWARN demonstrated interoperability with GCCS-M on the test network. The Navy should work with the GCCS-J Program Manager to coordinate deployment of GCCS-J with PLA to its MOCs and other theater headquarters to enable timely cross-battle group and cross-Service warning and reporting when ships are implementing emissions control procedures.

Unit-Level Mission Accomplishment

For a mission to be considered a success, a unit at risk must receive a JWARN CBRN hazard warning in time for assigned personnel to take protective measures before the hazard cloud arrives at the unit's location. Alternately, if there were no units at risk from the hazard, the mission was successful if a correct report was generated from received observations.

To determine the timeliness of a warning, DOT&E used test data on the time a warning was received by a unit and added 2 minutes (to account for doctrinal time to sound an alarm and for personnel to don protective masks or seek shelter). To determine cloud arrival time, DOT&E estimated the time of an attack to be 5 minutes prior to the time a test unit received a hand-delivered observation card from the test team. The additional 5 minutes accounts for the time it would take for a notional unit to prepare and transmit an observer report; as was observed in test. DOT&E used the test team's JEM predictions of hazard cloud behavior to determine the time between the attack and the arrival of the hazard cloud at a unit's location.

FOT&E included 82 opportunities for a unit to warn other units at risk. Of those, 41 opportunities involved units in close proximity to the hazard; an operator who was not properly engaged in the exercise; or network delays in receiving warning messages. In 36 of the total opportunities, a unit warned other units at risk in time to take protective measures. Figure 3-1 illustrates unit-level mission success in FOT&E, both in context of the 82 total opportunities (left column) and those 41 opportunities included in analysis (right column).

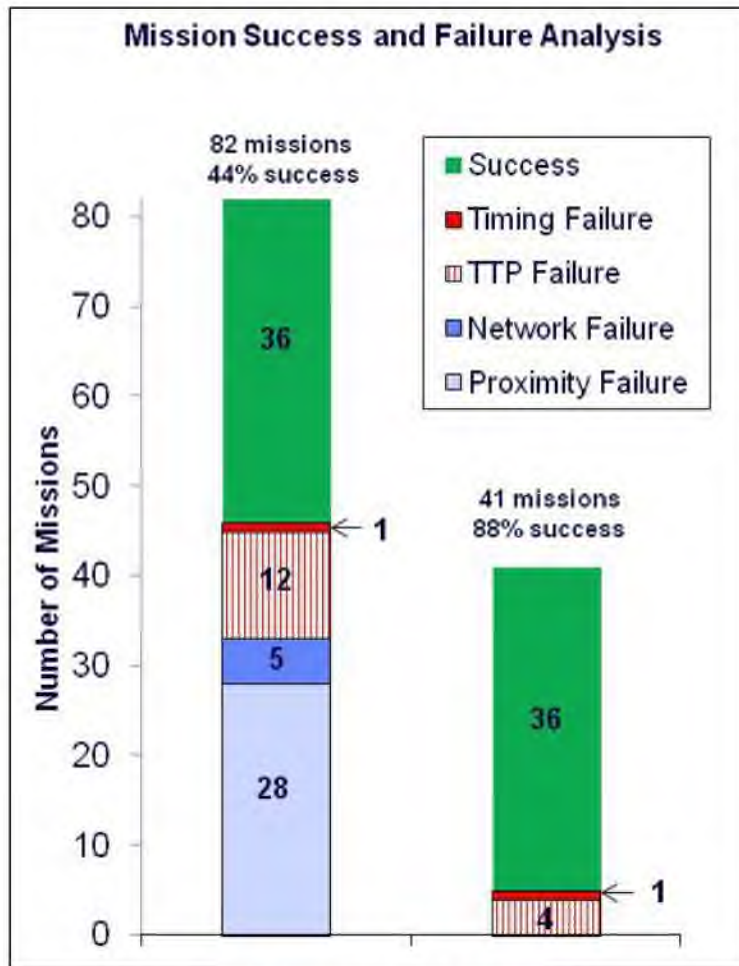


Figure 3-1. Overall Unit-Level Mission Success

Of the 82 total opportunities to warn units at risk, 28 involved units located ten kilometers or less downwind from the attack location (indicated in light blue on the first bar in Figure 3-1.) These opportunities to warn units at risk can be excluded from the mission analysis because they confirm a previously known JWARN system limitation associated with the man-in-the-loop warning and reporting process. Previous testing with JWARN deployed on GCCS-J, GCCS-A, and C2PC demonstrated that JWARN is not an effective warning tool when the unit at risk is less than 10 kilometers downwind of the initial hazard. The amount of time it takes for a JWARN operator to receive NBC observer reports and process the information is greater than the time it takes for the hazard cloud to travel to units located in close proximity to the attack. In these 28 instances, considered proximity failures, Navy units would rely on short-range tactical communications such as Microsoft chat and radio to communicate time-sensitive warnings within battle groups due to the proximity of the ships.

Five of the mission failures (indicated in a darker blue in Figure 3-1) were caused by network failures that delayed the receipt of warning messages. These network failures can be excluded because the test network did not provide operationally realistic redundancies and maintenance response.

There were 12 failures in which operators failed to implement the correct Tactics, Techniques, and Procedures (TTPs) to create an NBC-3 warning report. Eight of these procedural failures can be attributed to a single operator using GCCS-J at the JTF. This operator was not properly engaged in the exercise; thus, these eight failures are excluded.

The second bar in Figure 3-1 shows the mission success rate for JWARN when these opportunities are excluded from the unit-level mission success analysis. In the remaining 41 opportunities, operators used JWARN to successfully warn the units in 36 instances (88 percent of the time). Four of the mission failures (attributed to TTPs) involved complex scenarios with multiple attacks or multiple observer reports in which Navy operators did not warn units at risk. For the one remaining failure, the JWARN warning was received by the unit at risk too late to take protective actions. The unit was located 10.9 kilometers from the attack area.

Table 3-1 shows DOT&E's use of FOT&E data to model estimates of the probability of unit-level mission success based on four factors (distance from attack, communications path used, complexity of attack, and Service). The relationship between distance from attack and mission success is the most statistically significant factor ($p < 0.0001$). The complexity of an attack is also a significant factor in a unit's ability to utilize JWARN to warn units at risk in time to take protective action. The modeling indicates that communications path and Service do not significantly affect the mission success.

Table 3-1. Model Estimations of Probability of Unit Level Mission Success

Communications Path	Complexity of Attack	Distance from Attack					
		5 Kilometers		10 Kilometers		15 Kilometers	
		Navy	Army	Navy	Army	Navy	Army
Ground-to-Ground	Basic	N/A	0.14	N/A	0.79	N/A	0.99
	Complex	N/A	0.01	N/A	0.3	N/A	0.91
Ground-to-Ship	Basic	0.01	0.05	0.24	0.53	0.88	0.97
	Complex	0.01	0	0.04	0.1	0.45	0.75
Ship-to-Ground	Basic	0.27	0.58	0.9	0.97	0.99	0.99
	Complex	0.04	0.13	0.5	0.78	0.96	0.99
Ship-to-Ship	Basic	0.03	N/A	0.47	N/A	0.96	N/A
	Complex	0.01	N/A	0.1	N/A	0.69	N/A

0-49	
50-79	
80+	

Distance from Attack

Although JWARN automates the NATO ATP-45 CBRN Warning and Reporting Process, the process requires extensive analysis and report preparation time by the operator. During FOT&E, it took an average of 25 to 30 minutes, depending upon the communications path, for a

JWARN operator to prepare and send a warning report and a unit at risk to receive the report. In 59 of the 82 unit-level missions, units at risk received a warning report. However, at close ranges (0 to 5 kilometers), no unit was warned in time to take protective measures. Warning success improved to 13 percent for distances up to 10 kilometers. The impact of distance on warning units at risk is shown in Table 3-2.

Table 3-2. Mission Success Rate versus Distance from Attack

Distance from Attack	0-5 km	5-10 km	10-15 km	>15 km
Mission Success	0/12 (0%)	4/20 (20%)	9/10 (90%)	17/17 (100%)

Figure 3-2 depicts the relationship between warning time and cloud arrival time. Zero on the vertical axis represents the arrival of the hazard cloud. Positive numbers on the vertical axis represent the number of minutes a warning report arrived in advance of the hazard cloud. Negative numbers represent the number of minutes a warning report arrived after the hazard cloud arrived.

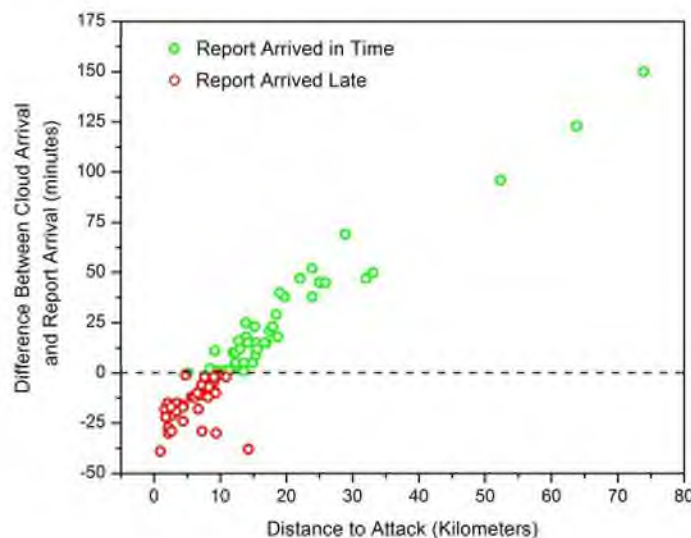


Figure 3-2. Comparison of Receipt of Warning and Arrival of Hazard Cloud

Figure 3-3 depicts the distribution of warning time when reports were received in time to take protective measures and when reports were not received in time or not received at all. For those missions that were successful, 59 percent of units were warned within 20 minutes of cloud arrival. Eighty-eight percent of units successfully warned were warned within one hour before cloud arrival. Thirty-one percent of units that were not warned in time received no report at all. The number of reports received within 20 minutes of cloud arrival indicated the importance of rapid report preparation. Operator actions, including the receipt of observations, critical thinking to process raw information, and report decision making, drive the timeliness of warning reports.



Figure 3-3. Time Distribution of JWARN Reports

JWARN Functional Capability

JWARN operators successfully exercised all of the system's functions required by the Navy on GCCS-M during the test. The Navy does not use the JWARN battlefield CBRN planning tools such as route planning, nor does the Navy use the tools to track unit CBRN equipment readiness, consumption rates, and MOPP status. During FOT&E, operators demonstrated JWARN capability to successfully perform the following required functions:

- Generate and transmit NBC reports
- Generate weather reports to support NBC hazard predictions

- Analyze NBC information to generate warnings for units at risk
- Create retrievable databases of NBC events and reports
- Populate CBRN information on the COP

JWARN Support to Decision Makers

All of test participants responded that JWARN increased their situational awareness, its results were interpretable, and it assisted in mission accomplishment.

The LCC had a field grade watch officer. The watch officer played the role of the ship's commander and made operational decisions in response to JWARN information. The watch officer directed the naval task force to maneuver to avoid predicted contamination and directed ships to upgrade the MOPP. In one vignette, he coordinated the rescue of personnel from an LHD that had been attacked by chemical rockets. The watch officer used Microsoft Chat on GCCS-M to communicate many of these decisions.

Interoperability

Data from the FOT&E indicate that JWARN is interoperable with GCCS-M and GCCS-J with PLA. The Joint Interoperability Test Command is conducting analysis and preparing a report to support formal interoperability certification.

JWARN demonstrated interoperability with the JEM. Operators using JWARN successfully completed 33 of 33 attempted JEM plots excluding 11 release other than attack (ROTA) plots. The operators were not able to complete the ROTA plots because the required templates had not been loaded on the JWARN client computers for test. The JWARN Program Manager should consider modifications to the JWARN to JEM interface to eliminate reliance on externally loaded templates.

Information Assurance

JWARN Multi-Service Operational Test and Evaluation on GCCS-J, GCCS-A, and C2PC in 2008 included JWARN Information Assurance vulnerability testing. Testing identified two administrative problems that the JWARN Program Manager successfully addressed. On August 3, 2011, the Joint Program Executive Officer for Chemical and Biological Defense approved an Authority to Operate for JWARN in support of the full deployment decisions on GCCS-J, GCCS-A, and C2PC.

In support of a full deployment decision for JWARN on GCCS-M, the JWARN Program Manager completed a technical scan of JWARN software hosted on GCCS-M to identify Information Assurance vulnerabilities. No significant vulnerabilities associated with JWARN were identified. The Navy will review these data with a view to approving an Authority to Connect to the GCCS-M system.

Section Four Operational Suitability

JWARN is operationally suitable for use by the Navy on GCCS-M. JWARN software hosted on GCCS-M experienced one operational mission failure (OMF) during 300 hours of operation during FOT&E (100 hours MTBOMF at the 80 percent lower confidence limit). The Navy user-defined reliability requirement is 100 hours MTBOMF. JWARN New Equipment operator training was sufficient to successfully accomplish NBC warning and reporting for 83 percent of basic attack scenarios during FOT&E. JWARN operators had difficulty in completing NBC warning and reporting for complex attack scenarios. The mission success rate for complex scenarios was 42 percent for Army and 44 percent for Navy JWARN operators.

Reliability

JWARN hosted on GCCS-M met the Navy user reliability requirement of 100 hours MTBOMF at the 80 percent lower confidence limit (LCL). JWARN reliability on GCCS-J and GCCS-A were assessed in DOT&E's August 10, 2010, memorandum for the Joint Program Executive Officer, entitled *Operational Evaluation of the Joint Warning and Reporting Network Joint Mission Application Software Increment I*.

Table 4-1 shows the test hours by C2 host system; an analysis of failures broken out by JWARN, C2 host, and network; and reliability estimates (for JWARN only and for total JWARN, host, and network) based on FOT&E.

Table 4-1. Reliability

C2 Host System	Test Hours	JWARN Failures	Host Failures	Network Failures	JWARN Software		JWARN + Host + Network	
					MTBF (Hours)	80% LCL (Hours)	MTBF (Hours)	80% LCL (Hours)
GCCS-M	300	1	1	5	300	100	43	29
GCCS-J (PLA)	100	0	0	3		62	33	18
GCCS-J	100	4	0	0	25	15	25	15
GCCS-A	102	0	0	0		63		63

JWARN Software

Five OMFs that occurred during FOT&E are attributed to JWARN software. One OMF occurred when messages sent from the LCC GCCS-M client running JWARN were not received by the intended recipient. The LCC JWARN operator could not open or delete the messages using the JWARN menu bar. The operator rebooted the JWARN GCCS-M client workstation and restarted both GCCS-M and JWARN in order for the messages to be successfully sent. The message arrived 20 minutes after it was initially sent by the JWARN operator at the LCC. Two

of the four JWARN OMFs on GCCS-J were caused by operator error when entering the wrong strike serial number into JWARN. JWARN was not able to correlate two NBC-1 reports due to the data entry error. The other two JWARN OMFs on GCCS-J occurred when the JWARN message center froze and the operator had to reboot the computer to resolve the failure.

Network/C2 Host

JWARN reliability is dependent upon the reliability of the network and host platform on which it resides. Host platform issues and network outages can affect the ability of JWARN to send timely warning messages to units at risk. When host and network failures are included in the JWARN on GCCS-M estimate, the overall Mean Time Between Failures (MTBF) estimate falls to 43 hours with an 80 percent LCL of 29 hours. The corresponding estimates for JWARN on GCCS-J with PLA are 33 and 18 hours, respectively. Since host and network failures are not related to JWARN software, they are not classified as JWARN OMFs.

The test network reflected the operational Navy network architecture but lacked the redundancy of the operational network and timely maintenance support. DOT&E estimates that five of eight network failures were caused by test limitations related to the lack of network redundancy and responsive maintenance.

Operational Availability

Operational availability (A_o) during FOT&E was 91 percent. Downtime includes the time the system was not available due to failures, network outages, routine maintenance, and rebooting of the systems. A tropical storm that hit the east coast during the test caused a network outage of over 4 hours and affected communications to and from the LHD ships. Availability increases to 93 percent if the network outage is not included in the calculation.

Routine reboots of the JWARN clients and the GCCS servers resulted in each node in the network being out of operation for 1.2 hours per day for a total of 43 hours during the test. Routine nightly reboot of clients caused 65 percent (43 of 66 hours) of downtime during FOT&E. The Navy conducts routine reboots at times that do not interfere with critical operations. To maintain critical capabilities, a Task Force Commander may pass CBRN defense responsibility to another ship while computers are being rebooted. Operational availability data are shown in Table 4-2.

Table 4-2. Operational Availability (A_o)

Node	Up Time (hours)	JWARN Downtime (hours)	Network Downtime (hours)	Routine Reboot Downtime (hours)	A_o – JWARN, Network, Routine Reboot	A_o – JWARN, Routine Reboot
BCT	95	0.2	0.8	6	0.93	0.94
DDG	96	0.0	0.0	5	0.95	0.95
JTF	93	0.7	0.3	6	0.93	0.93
LCC	91	0.6	1.4	7	0.91	0.92
LHD1	94	0.0	0.0	6	0.94	0.94
LHD2	83	0.0	12.0	5	0.83	0.94
MOC	86	0.1	6.9	7	0.86	0.92
All	637	1.6	21.4	43	0.91	0.93

Maintainability

JWARN operators perform basic operator-level tasks to fix computer problems. The primary operator response to a problem is to reboot the JWARN client computer. During FOT&E, operators rebooted the client computer seven times, with an average recovery time of 13 minutes. If operators could not fix a problem, they called the JWARN help desk. Navy operators called the help desk two times during the test. Each time, the problem was referred to network administrators, since the problem resided with the computer systems in Charleston, South Carolina. The Mean Corrective Maintenance Time for JWARN hosted on GCCS-M was 17.3 minutes, and for JWARN hosted on GCCS-J with PLA was 8.6 minutes. There was no user requirement for corrective maintenance activity.

As described in Section Two, the maintenance support for the test network was unrealistic, and DOT&E did not evaluate maintenance metrics associated with the network.

Data Management

JWARN is required to archive reporting data to support NBC battlefield reconstruction. Test files were successfully archived on a system computer disk for all vignettes. To support battlefield reconstruction and forensic investigations, JWARN annotates the address and time of all received reports. JWARN does not annotate sent reports. This makes it difficult to reconstruct what occurred.

Training

JWARN test operators stated that the New Equipment Training and training materials were adequate and prepared them to accomplish their missions. Test participants stated that they would like to receive more practical exercises to complement JWARN functionality training.

During test, DOT&E observed that Navy and Army operators experienced difficulty with complex scenarios. Complex scenarios involved multiple attacks in the battle area and/or observer reports from different sources. Basic scenarios involved single attacks combined with a single source for observation reports.

Navy operators using GCCS-M or GCCS-J with PLA successfully accomplished 83 percent of basic missions. Both Navy and Army operators had difficulty with complex scenarios. Army and Navy JWARN operators successfully accomplished 42 and 44 percent (respectively) of complex mission scenarios during FOT&E. Issues with complex scenarios included:

- Failure to recognize separate attacks
- Incorrect inputs to define attacks
- Inattention to detail
- Confusion between radiological attacks and nuclear attacks
- Loss of situational awareness (perhaps due to the speed of the exercise)
- Failure to recognize when a plot was obviously wrong

The Navy should review training for CIC watch officers and JWARN operators to determine the appropriate level of NBC knowledge and skills needed to address the expected threat. The Navy should explore opportunities for cross-training with the Marine Corps during amphibious exercises and pre-deployment training to increase NBC skills in the Navy.

The JWARN Program Manager should develop and field computer-based scenario training that includes basic to advanced scenarios to reinforce TTPs, increase operator skills, and provide sustainment training.

Section Five Recommendations

DOT&E recommends the following actions:

- The Navy should work with the GCCS Program Office to request and coordinate deployment of GCCS-J with PLA capability to its Maritime Operations Centers.
- Once the Navy deploys JWARN on GCCS-M, the Commander Operational Test and Evaluation Force should conduct additional FOT&E of JWARN on a Navy ship with an operational network and naval communications systems to demonstrate interoperability on an operational network.
- The Navy should consider cross-training with the Marine Corps during amphibious exercises and pre-deployment training to increase career-level NBC skills in the Navy.
- The Navy should work with the JWARN Program Manager to develop and field computer-based scenario training that includes basic to advanced scenarios to reinforce TTPs, increase operator-level skills, and provide sustainment training for JWARN operators.
- The JWARN Program Manager should modify the JWARN software to annotate sent messages in the archive files.
- The JWARN Program Manager should improve the JWARN to JEM interface to reduce the reliance on externally-loaded templates.



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OCT 22 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

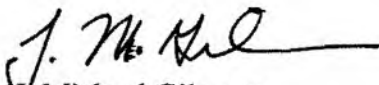
I have enclosed my operational evaluation report on the JWARN. This evaluation report supports the JWARN Increment 1 Full Deployment Decision on Global Command and Control System – Maritime (GCCS-M) for the Navy. In the report, I conclude the following:

- JWARN software hosted on GCCS-M is operationally effective to provide chemical, biological, radiological, and nuclear (CBRN) warning reports to units operating 10 or more kilometers from an initial CBRN release. Using JWARN, reports can be generated and received in time for such units to institute force protection actions before encountering CBRN hazards. JWARN enhances nuclear, biological, and chemical (NBC) situational awareness and supports operational decision making in response to basic NBC attacks by automating NBC warning, reporting, and hazard prediction process.
- JWARN is operationally suitable for use by the Navy on GCCS-M. JWARN New Equipment operator training was adequate to successfully accomplish NBC warning and reporting for 83 percent of basic attack scenarios during Follow-on Operational Test and Evaluation (FOT&E).
- Prior to operational testing, the Navy recognized that Global Command and Control System – Joint (GCCS-J), the command and control system used by the service's Maritime Operations Centers (MOCs), was not interoperable with GCCS-M when ships operate in emissions control. The GCCS-J program office developed a modification to enable GCCS-J to transmit messages in Plain Language Address (PLA) format, thereby circumventing the interoperability constraints imposed by emissions control. The Navy should work with the GCCS-J Program Manager to coordinate deployment of GCCS-J with PLA to its MOCs and other theater headquarters to enable timely cross-battle group and cross-Service warning and reporting when ships are implementing emissions control procedures.

I have sent copies to the Secretary of Defense; the Secretary of the Army; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; the Under Secretary of Defense for



Acquisition, Technology and Logistics; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Adam Smith
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OCT 22 2012

The Honorable C.W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

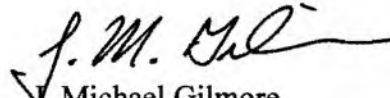
I have enclosed my operational evaluation report on the JWARN. This evaluation report supports the JWARN Increment 1 Full Deployment Decision on Global Command and Control System – Maritime (GCCS-M) for the Navy. In the report, I conclude the following:

- JWARN software hosted on GCCS-M is operationally effective to provide chemical, biological, radiological, and nuclear (CBRN) warning reports to units operating 10 or more kilometers from an initial CBRN release. Using JWARN, reports can be generated and received in time for such units to institute force protection actions before encountering CBRN hazards. JWARN enhances nuclear, biological, and chemical (NBC) situational awareness and supports operational decision making in response to basic NBC attacks by automating NBC warning, reporting, and hazard prediction process.
- JWARN is operationally suitable for use by the Navy on GCCS-M. JWARN New Equipment operator training was adequate to successfully accomplish NBC warning and reporting for 83 percent of basic attack scenarios during Follow-on Operational Test and Evaluation (FOT&E).
- Prior to operational testing, the Navy recognized that Global Command and Control System – Joint (GCCS-J), the command and control system used by the service's Maritime Operations Centers (MOCs), was not interoperable with GCCS-M when ships operate in emissions control. The GCCS-J program office developed a modification to enable GCCS-J to transmit messages in Plain Language Address (PLA) format, thereby circumventing the interoperability constraints imposed by emissions control. The Navy should work with the GCCS-J Program Manager to coordinate deployment of GCCS-J with PLA to its MOCs and other theater headquarters to enable timely cross-battle group and cross-Service warning and reporting when ships are implementing emissions control procedures.

I have sent copies to the Secretary of Defense; the Secretary of the Army; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; the Under Secretary of Defense for



Acquisition, Technology and Logistics; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OCT 22 2012

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

Dear Mr. Chairman:

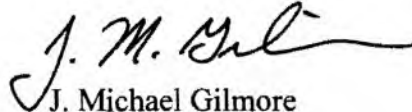
I have enclosed my operational evaluation report on the JWARN. This evaluation report supports the JWARN Increment 1 Full Deployment Decision on Global Command and Control System – Maritime (GCCS-M) for the Navy. In the report, I conclude the following:

- JWARN software hosted on GCCS-M is operationally effective to provide chemical, biological, radiological, and nuclear (CBRN) warning reports to units operating 10 or more kilometers from an initial CBRN release. Using JWARN, reports can be generated and received in time for such units to institute force protection actions before encountering CBRN hazards. JWARN enhances nuclear, biological, and chemical (NBC) situational awareness and supports operational decision making in response to basic NBC attacks by automating NBC warning, reporting, and hazard prediction process.
- JWARN is operationally suitable for use by the Navy on GCCS-M. JWARN New Equipment operator training was adequate to successfully accomplish NBC warning and reporting for 83 percent of basic attack scenarios during Follow-on Operational Test and Evaluation (FOT&E).
- Prior to operational testing, the Navy recognized that Global Command and Control System – Joint (GCCS-J), the command and control system used by the service's Maritime Operations Centers (MOCs), was not interoperable with GCCS-M when ships operate in emissions control. The GCCS-J program office developed a modification to enable GCCS-J to transmit messages in Plain Language Address (PLA) format, thereby circumventing the interoperability constraints imposed by emissions control. The Navy should work with the GCCS-J Program Manager to coordinate deployment of GCCS-J with PLA to its MOCs and other theater headquarters to enable timely cross-battle group and cross-Service warning and reporting when ships are implementing emissions control procedures.

I have sent copies to the Secretary of Defense; the Secretary of the Army; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; the Under Secretary of Defense for



Acquisition, Technology and Logistics; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable John McCain
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OCT 22 2012

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6025

Dear Mr. Chairman:

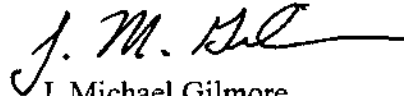
I have enclosed my operational evaluation report on the JWARN. This evaluation report supports the JWARN Increment 1 Full Deployment Decision on Global Command and Control System – Maritime (GCCS-M) for the Navy. In the report, I conclude the following:

- JWARN software hosted on GCCS-M is operationally effective to provide chemical, biological, radiological, and nuclear (CBRN) warning reports to units operating 10 or more kilometers from an initial CBRN release. Using JWARN, reports can be generated and received in time for such units to institute force protection actions before encountering CBRN hazards. JWARN enhances nuclear, biological, and chemical (NBC) situational awareness and supports operational decision making in response to basic NBC attacks by automating NBC warning, reporting, and hazard prediction process.
- JWARN is operationally suitable for use by the Navy on GCCS-M. JWARN New Equipment operator training was adequate to successfully accomplish NBC warning and reporting for 83 percent of basic attack scenarios during Follow-on Operational Test and Evaluation (FOT&E).
- Prior to operational testing, the Navy recognized that Global Command and Control System – Joint (GCCS-J), the command and control system used by the service's Maritime Operations Centers (MOCs), was not interoperable with GCCS-M when ships operate in emissions control. The GCCS-J program office developed a modification to enable GCCS-J to transmit messages in Plain Language Address (PLA) format, thereby circumventing the interoperability constraints imposed by emissions control. The Navy should work with the GCCS-J Program Manager to coordinate deployment of GCCS-J with PLA to its MOCs and other theater headquarters to enable timely cross-battle group and cross-Service warning and reporting when ships are implementing emissions control procedures.

I have sent copies to the Secretary of Defense; the Secretary of the Army; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; the Under Secretary of Defense for



Acquisition, Technology and Logistics; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Thad Cochran
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OCT 03 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

(U) I have attached the Initial Operational Test and Evaluation (IOT&E) report on the E-3 Airborne Warning and Control System (AWACS) Block 40/45 upgrade, required by Sections 2399 and 2366 of Title 10, United States Code. In the report, I conclude the following:

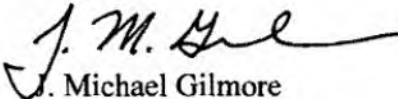
- (U) AWACS Block 40/45 upgrade enables E-3 crews to accomplish their Battle Management Command and Control mission and is therefore operationally effective. The upgrade provides automated tracking and combat identification, and improves the human machine interface; however, the Block 40/45 upgrade does not provide all required enhancements and it is not as interoperable as the legacy Block 30/35 E-3. Deficiencies include software written to outdated interoperability standards and choice of hardware with limited interoperability. Block 40/45 was not ready to enter IOT&E primarily because no government developmental test and evaluation was conducted prior to IOT&E. Aircrew and maintainers were not adequately trained and did not understand the capabilities and limitations of Block 40/45. This lack of training degraded the performance of the system during IOT&E.
- (U) AWACS Block 40/45 is not operationally suitable. Although Block 40/45 equipment and software are more reliable than the aging Block 30/35 equipment they replace, the upgrade nonetheless demonstrated poor reliability and maintainability during the IOT&E. Block 40/45 does not currently meet several key suitability requirements; however, the Air Force expects future AWACS system software and hardware upgrades will improve system reliability substantially.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Air Force; the Vice Chairman of the



[REDACTED]

Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Adam Smith
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OCT 03 2012

The Honorable C. W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

Dear Mr. Chairman:

(U) I have attached the Initial Operational Test and Evaluation (IOT&E) report on the E-3 Airborne Warning and Control System (AWACS) Block 40/45 upgrade, required by Sections 2399 and 2366 of Title 10, United States Code. In the report, I conclude the following:

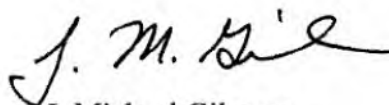
- (U) AWACS Block 40/45 upgrade enables E-3 crews to accomplish their Battle Management Command and Control mission and is therefore operationally effective. The upgrade provides automated tracking and combat identification, and improves the human machine interface; however, the Block 40/45 upgrade does not provide all required enhancements and it is not as interoperable as the legacy Block 30/35 E-3. Deficiencies include software written to outdated interoperability standards and choice of hardware with limited interoperability. Block 40/45 was not ready to enter IOT&E primarily because no government developmental test and evaluation was conducted prior to IOT&E. Aircrew and maintainers were not adequately trained and did not understand the capabilities and limitations of Block 40/45. This lack of training degraded the performance of the system during IOT&E.
- (U) AWACS Block 40/45 is not operationally suitable. Although Block 40/45 equipment and software are more reliable than the aging Block 30/35 equipment they replace, the upgrade nonetheless demonstrated poor reliability and maintainability during the IOT&E. Block 40/45 does not currently meet several key suitability requirements; however, the Air Force expects future AWACS system software and hardware upgrades will improve system reliability substantially.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Air Force; the Vice Chairman of the



[REDACTED]

Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.



J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OCT 03 2012

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20515-6050

Dear Mr. Chairman:

(U) I have attached the Initial Operational Test and Evaluation (IOT&E) report on the E-3 Airborne Warning and Control System (AWACS) Block 40/45 upgrade, required by Sections 2399 and 2366 of Title 10, United States Code. In the report, I conclude the following:

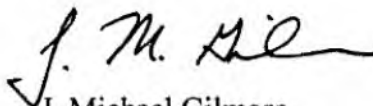
- (U) AWACS Block 40/45 upgrade enables E-3 crews to accomplish their Battle Management Command and Control mission and is therefore operationally effective. The upgrade provides automated tracking and combat identification, and improves the human machine interface; however, the Block 40/45 upgrade does not provide all required enhancements and it is not as interoperable as the legacy Block 30/35 E-3. Deficiencies include software written to outdated interoperability standards and choice of hardware with limited interoperability. Block 40/45 was not ready to enter IOT&E primarily because no government developmental test and evaluation was conducted prior to IOT&E. Aircrew and maintainers were not adequately trained and did not understand the capabilities and limitations of Block 40/45. This lack of training degraded the performance of the system during IOT&E.
- (U) AWACS Block 40/45 is not operationally suitable. Although Block 40/45 equipment and software are more reliable than the aging Block 30/35 equipment they replace, the upgrade nonetheless demonstrated poor reliability and maintainability during the IOT&E. Block 40/45 does not currently meet several key suitability requirements; however, the Air Force expects future AWACS system software and hardware upgrades will improve system reliability substantially.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Air Force; the Vice Chairman of the



[REDACTED]

Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable John McCain
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OCT 03 2012

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20515-6025

Dear Mr. Chairman:

(U) I have attached the Initial Operational Test and Evaluation (IOT&E) report on the E-3 Airborne Warning and Control System (AWACS) Block 40/45 upgrade, required by Sections 2399 and 2366 of Title 10, United States Code. In the report, I conclude the following:

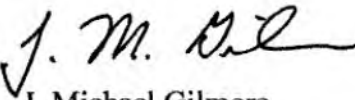
- (U) AWACS Block 40/45 upgrade enables E-3 crews to accomplish their Battle Management Command and Control mission and is therefore operationally effective. The upgrade provides automated tracking and combat identification, and improves the human machine interface; however, the Block 40/45 upgrade does not provide all required enhancements and it is not as interoperable as the legacy Block 30/35 E-3. Deficiencies include software written to outdated interoperability standards and choice of hardware with limited interoperability. Block 40/45 was not ready to enter IOT&E primarily because no government developmental test and evaluation was conducted prior to IOT&E. Aircrew and maintainers were not adequately trained and did not understand the capabilities and limitations of Block 40/45. This lack of training degraded the performance of the system during IOT&E.
- (U) AWACS Block 40/45 is not operationally suitable. Although Block 40/45 equipment and software are more reliable than the aging Block 30/35 equipment they replace, the upgrade nonetheless demonstrated poor reliability and maintainability during the IOT&E. Block 40/45 does not currently meet several key suitability requirements; however, the Air Force expects future AWACS system software and hardware upgrades will improve system reliability substantially.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Air Force; the Vice Chairman of the



[REDACTED]

Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Thad Cochran
Ranking Member


Common Remotely Operated Weapon Station (CROWS)

Initial Operational Test and Evaluation Report



September 2012

This report on the Common Remotely Operated Weapons Station (CROWS) fulfills the provisions of Title 10, United States Code, Section 2399. It assesses the adequacy of testing and the operational effectiveness and operational suitability of the CROWS.


J. Michael Gilmore
Director



CROWS with an M2 machine gun mounted on a Mine Resistant Ambush Protected vehicle



Gunner seated at the fire control unit

Initial Operational Test and Evaluation (IOT&E) Report

Summary

The Common Remotely Operated Weapon Station (CROWS) is operationally effective and operationally suitable. The CROWS target acquisition and engagement capabilities enable units to detect and engage targets at long range while on-the-move and stationary more effectively than a non-CROWS-equipped unit. The CROWS demonstrated 8,015 Mean Rounds Between System Abort (MRBSA), which exceeded its reliability requirement of 1,900 MRBSA, during Army Initial Operational Test and Evaluation (IOT&E) in 2009. The CROWS-equipped Up-Armored High Mobility Multi-purpose Wheeled Vehicle (HMMWV) (UAH) demonstrated the capability to support units as they shoot, move, and communicate.

System Overview

The CROWS system has been deployed worldwide with 11,690 systems procured to date. This report supports an Army Acquisition Executive decision to purchase 1,212 additional systems in September 2012.

The CROWS is a gunner-operated system that provides the capability to remotely aim and fire a suite of crew-served weapons. This capability can be accomplished from either a stationary platform or while on-the-move. The CROWS is configured for mounting on a variety of vehicles and uses the host vehicle's power. Figures 1 through 3 show the CROWS components and configurations. Figure 4 compares the CROWS to a gunner protection kit. The CROWS consists of:

- A mount, weapon cradle, and traverse and elevation drives
- A weapon interface, weapon remote charger, ammunition magazine feed system, viewing and sighting unit
- A laser range finder and electronics support unit/fire control processor
- A fire control unit and control grip located inside the vehicle.

The CROWS has the capability to mount any one of the following weapons: M2 .50-Caliber Heavy Barrel Machine Gun, MK19 40-mm Grenade Machine Gun, M240 7.62-mm Machine Gun, and M249 5.56-mm Squad Automatic Weapon.

The CROWS threshold interoperability requirement is to be capable of being mounted on the M1114 and M1116 UAH variants. The Army has mounted CROWS on the Mine Resistant Ambush Protected (MRAP) - All Terrain Vehicle (M-ATV) and other variants of MRAPs. The Army also intends to mount CROWS on the following vehicles:

- | | |
|--------------------------------|---------------------|
| • M113 Armor Personnel Carrier | • M1088 tractor |
| • Heavy Equipment Transporter | • M1083 cargo truck |
| • Palletized Load System truck | • M915 tractor |
| • M1A2 Tank | |



Figure 1. CROWS with M2 machine gun mounted on a Mine Resistant Ambush Protected vehicle



Figure 2. Gunner seated at the fire control unit



Figure 3. CROWS components



Figure 4. CROWS (left) and gunner protection kit (right)

The CROWS allows the gunner to remain protected inside the vehicle and is designed to provide enhanced target acquisition, identification, and engagement capabilities for wheeled and tracked vehicles. In comparison, the Objective Gunner Protection Kit (OGPK) (as shown in Figure 4 (right)) is a motorized rotating turret designed to be mounted on top of the HMMWV and MRAP vehicles. The OGPK includes a sling for the gunner, transparent armor, and rear view mirrors.

Missions

Units equipped with the CROWS engage in direct combat action against enemy forces, and provide convoy and base security and troop transport.

Test Adequacy

The Army conducted the IOT&E in 2009 and completed developmental testing in 2010. At the time the IOT&E was conducted, CROWS was an Acquisition Category (ACAT) II program. The Army Test and Evaluation Command (ATEC) was responsible for approving the test plan, conducting the IOT&E, and reporting their evaluation to the Army. Representatives from DOT&E visited the site during the conduct of the IOT&E in October 2009 to monitor test execution adequacy; however, the program was not under DOT&E oversight at the time of the IOT&E and DOT&E did not approve the operational test plan.

Early in FY12, the Army Acquisition Executive notified the Under Secretary of Defense (USD) for Acquisition, Technology and Logistics (AT&L) that the CROWS program was expected to reach an ACAT I funding level for the procurement year. In March 2012, the USD(AT&L) designated the CROWS program an ACAT IC Major Defense Acquisition Program with the Army as the lead Service. This designation caused the program to come under DOT&E oversight even though the Army had completed all operational testing.

In June 2012, PEO Soldier requested that DOT&E prepare an operational test and evaluation report to Congress to support a September 2012 production decision for the procurement of the final 1,212 CROWS systems. To do so, DOT&E used the results from the following events:

- 2009 CROWS IOT&E;
- CROWS Production Verification Test (PVT);
- 2009 M-ATV IOT&E;
- 2010 Special Operational Forces (SOF) M-ATV IOT&E;
- Corrective actions taken by the program between 2010 and 2012;
- An assessment of current CROWS capability observed during fielding to elements of the 101st Airborne Division at Fort Campbell, Kentucky, in August 2012.

Operational Test and Evaluation

A TEC conducted the IOT&E at Fort Carson, Colorado, in October – November 2009. The IOT&E consisted of two phases: live-fire gunnery and force-on-force vignettes. The Army IOT&E test plan called for 10 force-on-force vignettes. Six vignettes provided information. Three vignettes were cancelled due to weather and one had data instrumentation problems. The Battalion Commander removed his Soldiers from the field due to a severe winter storm.

The IOT&E test unit consisted of a Military Police (MP) platoon composed of a Platoon Leader, Platoon Sergeant, and eight three-man teams. The MP platoon conducted seven force-on-force vignettes, and eight days (executed one additional day) of weapons live-fire gunnery. During the live-fire gunnery, the Soldiers used four types of weapons – an M2 heavy machinegun, an MK19 grenade machinegun, an M240 light machinegun, and an M249 squad automatic weapon – firing at stationary targets while in a fixed position, and firing at stationary targets while the vehicle was moving. The eight teams of MPs operated three CROWS-equipped UAHs. There were six additional UAHs with mounted OGPKs to enable a force-on-force comparison of a CROWS-equipped squad with a non-CROWS-equipped squad. Each team consisted of a vehicle driver, a vehicle commander, and a CROWS operator.

The IOT&E used force-on-force vignettes consistent with a Southwest Asia scenario. During the six valid vignettes, Soldiers used the CROWS in executing the following IOT&E missions:

- Static security operations involving limited movement, security of critical assets and facilities, and defensive operations;
- Route and area reconnaissance, mobile patrolling, and security of designated convoys with security vehicles committed to ensure constant movement and security of convoy vehicles;
- An initial reaction force responding to enemy attacks.

An enemy force armed with assault rifles and rocket-propelled grenades (RPGs) attacked the MP unit during missions. In addition to blank ammunition, the enemy used RPG simulators that included a noise and smoke replicator to add realism.

Soldier maintainers performed unit-level small-arms maintenance on the weapons mounted on the CROWS. Field service representatives performed maintenance on the CROWS system, consistent with the planned sustainment concept at that time.

Developmental Testing

The CROWS IOT&E data were supplemented by developmental testing. These tests included:

- PVT conducted at the Aberdeen Test Center (ATC), Aberdeen Proving Ground, Maryland;
- Cold Regions Test Center (CRTC), Fort Greely, Alaska;
- Tropic Regions Test Center (TRTC), Schofield Barracks, Hawaii;
- Yuma Test Center (YTC), Yuma, Arizona.

Operational Test and Evaluation

In addition to the CROWS IOT&E, Infantry and SOF units used MRAP-mounted CROWS during the 2009 M-ATV IOT&E and the 2010 SOF M-ATV IOT&E. Both operational tests were conducted at Yuma Proving Ground, Arizona.

New Equipment Training (NET) for Fielding

In August 2012, 32 Soldiers from different units at Fort Campbell participated in New Equipment Training (NET) that included classroom and hands-on weapons installation of all four weapons types, bore sighting, and simulator engagements. The training concluded with on-the-move operations and a gunnery live-fire event. For the gunnery event, each Soldier fired an M240B machine gun mounted on a CROWS, engaging targets out to 800 meters. At the conclusion of the training, all Soldiers were certified capable of using CROWS as a weapons platform.

Operational Effectiveness

The CROWS is operationally effective. The CROWS target acquisition and engagement capabilities enable units to detect and engage targets at long ranges while on-the-move and stationary more effectively than non-CROWS-equipped units. The CROWS is more accurate while firing at long ranges than a crew-served weapon fired by a gunner using the OGPK. A unit with CROWS-equipped vehicles can synchronize target acquisition, maneuver, and provide responsive fires during missions such as Route Reconnaissance, Area Security, and Overwatch. During the IOT&E live-fire gunnery phase, the MP platoon operating the CROWS-equipped UAHs detected and engaged more targets than when using the OGPK-equipped UAHs at ranges that would have been representative of Area Security, Route Reconnaissance, and Security Escort missions.

During the 2009 M-ATV IOT&E, vehicle crews were able to suppress targets using the CROWS on the M-ATV. Using the Multiple Integrated Laser Engagement System (MILES) test instrumentation, vehicle crews employed the CROWS-mounted M2 caliber machine guns and the M240B 7.62 mm machine guns to suppress the threat force during missions. The Infantry units were able to effectively employ weapons mounted in the gunner stations during 11 of 11 missions. These missions included Route Security, Combat Convoy, Cordon and Search, and Route Reconnaissance.

During the 2010 SOF M-ATV IOT&E, the SOF M-ATV crews effectively engaged stationary and moving targets with the CROWS-mounted M2 .50-caliber machine guns during the live-fire convoy gunnery event. The SOF crews hit 82 percent of the targets during the day and 77 percent of targets (day and night). The SOF M-ATV crews effectively engaged stationary and moving targets with CROWS-mounted MK19 machine guns. The SOF crews hit 54 percent of targets during day firing. Night firing was not conducted.

Weapons Accuracy

As shown in Table 1 (below), the CROWS-equipped unit demonstrated the capability to acquire and engage standard vehicle targets out to the maximum effective range of the four weapons systems during testing in basic climate conditions. The MK19 did not fire accurately against area and point targets in the hot and high altitude environment of the desert. Subsequent to the PVT, the firing tables and system software were modified to improve the MK19 performance. Additional MK19 firing tests are planned for October 2012 at ATC to verify correction to the MK19 firing tables and MK19 accuracy. ATEC will validate CROWS MK19 accuracy at high altitude in a desert environment at YTC in the summer of 2013.

The MK19 did not provide accurate fire solutions for area targets during cold environment testing due to the limitation of the CROWS Laser Range Finder (LRF) performance in ice and fog conditions. The Army intends to revise the manual to include the limitation of the performance of the LRF in the cold environment.

The ability of the crew with a CROWS-equipped vehicle to provide responsive fires is degraded when the weapon malfunctions and ammunition feeder jams. During the CROWS IOT&E, the CROWS operators experienced 14 incidents of ammunition feeder jams and 17 incidents of weapons malfunctioning. The CROWS operator had to stop firing and a member of the crew had to vacate his protected position to climb out of the vehicle to fix the problem, exposing the crew to enemy fire.

Table 1. PVT Weapons Accuracy Performance Results

Weapon	Threshold	Basic (ATC)*	Desert (YTC)	Tropic Region (TRTC)	Cold Region (CRTC)
MK19	Area target – at least 50% at 1,500 meters. Area Target defined as 50 meters deep by 10 meters wide shall hit one round of two separate three round bursts at a vertical silhouette of Soldier. Point target – at least 50% at 1,200 meters. Stationary target defined as 2.3 x 2.3 x 4.6 meter cube or 2.3 x 2.3 meter shall hit one round of two separate three to five round bursts at 1,200 meters.	Achieved 95% against both Area and Point targets.	No hits were scored against Area or Point targets.	No MK19 accuracy testing was conducted.	No hits scored against Area targets. Achieved 100% against Point targets.
M2	Area target – at least 50%. Target defined as 50 meters deep by 10 meters wide shall hit one round of two separate three round bursts at a vertical silhouette of Soldier. Point target – at least 50%. Stationary target defined as 2.3 x 2.3 x 4.6 meter cube or 2.3 x 2.3-meter vertical shall hit one round of two separate three to five round burst at 1,200 meters.	Achieved 85% against Area targets. Achieved 97% against Point targets.	Achieved 100%.	Achieved 50% against a Point target. Not tested against an Area target.	Achieved 100% against Area and Point targets.
M240B	At least 50% at up to 800 meters. One hit from each 10-round burst on a 2 meter high by 3 meter wide target.	Achieved 95%.	Achieved 90%.	Achieved 50%.	Achieved 100%.
M249	At least 50% at up to 800 meters. One hit from each 10-round burst on a 2 meter high by 3 meter wide target.	Achieved 96%.	Achieved 100%.	Achieved 50%.	Achieved 95%.

* The percentage achieved is the 80 percent lower confidence bound on 100 percent success in each trial.

Situational Awareness

During the 2009 M-ATV IOT&E and the 2010 SOF M-ATV IOT&E, the CROWS demonstrated good long-range situational awareness during the day and at night. During the CROWS IOT&E and SOF M-ATV IOT&E, the units had poor situational awareness at close range, in complex terrain, and in an urban environment with the CROWS-equipped vehicles. In these tests, this shortcoming was mitigated when the units employed a combination of OGPK-equipped vehicles and CROWS-equipped vehicles. The OGPK-vehicles provided better short range situational awareness. Long-range situational awareness was not demonstrated during the CROWS IOT&E because of the cancellation of the four vignettes due to severe weather.

The CROWS operator has limited capability to scan and observe activities and threats surrounding the vehicle and at close range. The CROWS has a restrictive field of view for target

acquisition compared to gunners operating from the OGPK. The CROWS daylight sight provides a 47-degree field of view and its minimum focus distance is 2 meters. The CROWS thermal sighting provides a narrow 10-degree field of view. These capabilities limit the CROWS operator from acquiring dispersed targets, whereas a gunner operating the OGPK can rapidly scan for and detect close-in and widely dispersed targets.

Operational Suitability

The CROWS is operationally suitable. During IOT&E, the CROWS demonstrated 8,015 MRBSA exceeded its reliability requirement of 1900 MRBSA. The CROWS-equipped UAH demonstrated the capability to perform its mission essential functions of move, shoot, and communicate. The CROWS can be maintained by Soldier maintainers. The crew was able to quickly dismount the vehicle during missions without interference from the CROWS. Training and manual deficiencies detracted from the ability of the MP unit to accomplish missions in the 2009 IOT&E. These deficiencies and the status of their correction are discussed below.

New Equipment Training. During the 2009 IOT&E, 50 percent of the Soldiers reported the training did not prepare them to operate the equipment. The crews and gunners struggled to properly employ the CROWS throughout the test:

- Soldiers initially had difficulty using the CROWS functions to detect and identify the OPFOR.
- During the gunnery live-fire event, the Soldiers incorrectly loaded ammo into CROWS ammo containers.
- Soldiers failed to establish no-fire and no-traverse zone limits for gun movement.
- The training package lacked information on CROWS employment considerations or recommended tactics, techniques, and procedures to the unit.

The revised 2012 NET has improved over the IOT&E NET. A new program of instruction (POI) incorporates expanded hands-on, situational awareness, safety instructions, and gunnery live-fire exercises. The POI lessons include the correct method to establish no-fire and no-traverse zones.

Operator Manual. The CROWS operator manuals used during IOT&E lacked procedures to employ CROWS in extreme cold weather. A new cold weather start-up procedure was incorporated in the updated manual. The updated operator manual also includes detailed warnings on potential safety hazards of not establishing a weapon movement no-fire and no-traverse zone.

CROWS Manual Gunnery. When the CROWS automated fire control system fails, Soldiers must manually fire the weapon. During the IOT&E, Soldiers had difficulty manually aiming weapons on the CROWS because of the height of the weapon. Soldiers of average height had to raise their arms above their heads to reach the weapon trigger due to the height of the weapon integrated on the CROWS. Shorter Soldiers require a gunner stand to employ weapons properly.

Cartridge Case and Link Deflection. Soldiers are exposed to enemy fire when clearing cartridge cases and links based on gunnery live fire. Subsequent to the IOT&E, the link guide has been redesigned to better deflect expended cartridge cases and links. This fix is planned to be implemented and fielded in early 2013.

Disorientation. During the IOT&E, several gunners experienced dizziness while operating the CROWS inside the vehicle while on-the-move. This physical condition may be due to motion sickness caused by focusing on the CROWS screen during vehicle movement.

Reliability

The threshold reliability requirement is a 90 percent probability of acquiring and engaging a standard NATO-sized vehicle target out to the maximum effective range of the weapon for 200 rounds without experiencing a system abort. This translates to 1,900 rounds without a system abort. Based on the results of both operational and developmental testing, this requirement was met. The CROWS provides the gunner a 94 percent probability of firing 200 rounds without a system abort. Table 2 shows the CROWS reliability data and demonstrated MRBSA. In the 2009 IOT&E and 2012 New Equipment Training at Fort Campbell, there were no system aborts.

Table 2. CROWS Reliability Data and Demonstrated Estimate

Event	Rounds fired	System Aborts	Effective Function Failures (EFFs)	Demonstrated MRBSA (80% lower confidence level)	System Abort (SA) and Effective Function Failure (EFF) Description
IOT&E at Fort Carson (2009)	12,900	0	1	>8,015	1 EFF: Error Message causes CROWS to be unable to fire for maximum time period of 2 minutes
Basic (ATC)	4,600	2	3	>1,075	SA 1 and 2: Could not fire weapon; Firing and Servo disabled and sight elevation blocked 3 EFFs: A laser range finder returned error message; the round counter function incorrectly; and a thermal imagery module would not focus
Cold Region (CRTC)	4,859	2	1	>1,136	SA 1: Could not fire weapon; Firing and Servo disabled and sight elevation blocked SA 2: Could not fire weapon, firing disabled 1 EFF: Laser range finder displayed "error"
Tropic Region (TRTC)	3,746	1	3	>1,251	SA 1: Could not fire, malfunction of the display panel 3 EFFs: two round counters functioned incorrectly and one display went blank
Desert Region (YTC)	4,120	1	8	>1,376	SA 1: Could not fire weapon, Firing and Servo displayed sight elevation motion error 8 EFFs: two Ammo Count incorrect, three weapons jammed using .50-cal ammo, a tensor pin backed out, a fault code of preventing weapon elevation, a fault code- blocked charging actuator
All testing*	30,225	6	16	>3,330	

The CROWS experienced six effective function failures of the round counter during PVT when it did not display the correct amount of fired ammo. Although this failure mode was not experienced in the IOT&E, erroneous count of ammo expenditure has an operational impact to the crew employing a CROWS-equipped vehicle because full expenditure of ammunition requires a time consuming reload sequence for both the CROWS and the weapon. Subsequent to the PVT, the program has fixed the round counter software to display the correct rounds expended. A pressure plate has been added to the ammunition box that reports when there is a low-ammunition state, which allows the gunner to quickly reload the ready box and link the new ammunition to the remainder in the box.

Based on reliability root cause analysis and assessment performed after the IOT&E, five of the six system aborts during PVT were software failures. The CROWS software is being improved to eliminate the weapon firing failures. The one non-software system abort was a broken housing around the display unit allowing water seepage because the mounting holes were drilled too deep. To mitigate this failure, the vendor has modified the process of drilling the mounting holes.

Maintenance

The CROWS can be maintained when mounted on the HMMWV. During the November 2011 Logistics Demonstration, Soldier maintainers successfully demonstrated Preventative Maintenance Checks and Services (PMCS) and performed all maintenance tasks using the special tool kit and the General Mechanics Tool Kit (GMTK).

Recommendations

The CROWS program manager should implement the following recommendations:

- Conduct follow-on operational testing to evaluate the effectiveness and suitability of CROWS as it is integrated for use on combat vehicles in addition to the HMMWV and MRAP.
- Investigate increasing the field of view of the CROWS daytime and thermal sights to improve CROW operator determination of enemy location. The CROWS imaging sights have limited field of view, which affects the crew's ability to acquire and engage the enemy.
- Test to confirm the updated fire tables corrective action improve the MK19 accuracy with CROWS in a desert environment.
- Validate that link guide corrective action deflects expended cartridge cases and links.



OFFICE OF THE SECRETARY OF DEFENSE

WASHINGTON, DC 20301

SEP 27 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

Early in Fiscal Year 2012, the Army Acquisition Executive notified the Under Secretary of the Defense for Acquisition, Technology and Logistics (USD(AT&L)) that the CROWS program was expected to reach an Acquisition Category (ACAT) I funding level for the procurement year. In March 2012, the USD(AT&L) designated the CROWS program an ACAT 1C Major Defense Acquisition Program with the Army as lead Service. This designation caused the program to come under my oversight even though the Army had completed all operational testing. Consequently, I have attached at TAB A the CROWS IOT&E report now required by Section 2399, Title 10, United States Code. In the report I conclude the following:

The CROWS is operationally effective and suitable. CROWS enables a unit to detect and engage targets at long ranges more effectively than a non-CROWS-equipped unit. The CROWS is more accurate while firing at long ranges than a crew-served weapon fired by a gunner and exceeded its reliability requirement during IOT&E.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Adam Smith
Ranking Member





OFFICE OF THE SECRETARY OF DEFENSE

WASHINGTON, DC 20301

SEP 27 2012

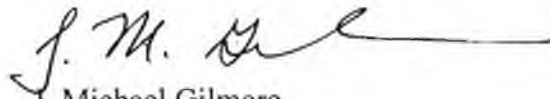
The Honorable C. W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

Dear Mr. Chairman:

Early in Fiscal Year 2012, the Army Acquisition Executive notified the Under Secretary of the Defense for Acquisition, Technology and Logistics (USD(AT&L)) that the CROWS program was expected to reach an Acquisition Category (ACAT) I funding level for the procurement year. In March 2012, the USD(AT&L) designated the CROWS program an ACAT 1C Major Defense Acquisition Program with the Army as lead Service. This designation caused the program to come under my oversight even though the Army had completed all operational testing. Consequently, I have attached at TAB A the CROWS IOT&E report now required by Section 2399, Title 10, United States Code. In the report I conclude the following:

The CROWS is operationally effective and suitable. CROWS enables a unit to detect and engage targets at long ranges more effectively than a non-CROWS-equipped unit. The CROWS is more accurate while firing at long ranges than a crew-served weapon fired by a gunner and exceeded its reliability requirement during IOT&E.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member





OFFICE OF THE SECRETARY OF DEFENSE

WASHINGTON, DC 20301

SEP 27 2012

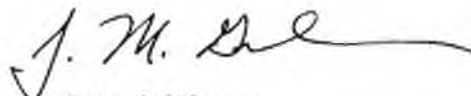
The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

Dear Mr. Chairman:

Early in Fiscal Year 2012, the Army Acquisition Executive notified the Under Secretary of the Defense for Acquisition, Technology and Logistics (USD(AT&L)) that the CROWS program was expected to reach an Acquisition Category (ACAT) I funding level for the procurement year. In March 2012, the USD(AT&L) designated the CROWS program an ACAT 1C Major Defense Acquisition Program with the Army as lead Service. This designation caused the program to come under my oversight even though the Army had completed all operational testing. Consequently, I have attached at TAB A the CROWS IOT&E report now required by Section 2399, Title 10, United States Code. In the report I conclude the following:

The CROWS is operationally effective and suitable. CROWS enables a unit to detect and engage targets at long ranges more effectively than a non-CROWS-equipped unit. The CROWS is more accurate while firing at long ranges than a crew-served weapon fired by a gunner and exceeded its reliability requirement during IOT&E.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable John McCain
Ranking Member





OFFICE OF THE SECRETARY OF DEFENSE

WASHINGTON, DC 20301

SEP 27 2012

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6025

Dear Mr. Chairman:

Early in Fiscal Year 2012, the Army Acquisition Executive notified the Under Secretary of the Defense for Acquisition, Technology and Logistics (USD(AT&L)) that the CROWS program was expected to reach an Acquisition Category (ACAT) I funding level for the procurement year. In March 2012, the USD(AT&L) designated the CROWS program an ACAT 1C Major Defense Acquisition Program with the Army as lead Service. This designation caused the program to come under my oversight even though the Army had completed all operational testing. Consequently, I have attached at TAB A the CROWS IOT&E report now required by Section 2399, Title 10, United States Code. In the report I conclude the following:

The CROWS is operationally effective and suitable. CROWS enables a unit to detect and engage targets at long ranges more effectively than a non-CROWS-equipped unit. The CROWS is more accurate while firing at long ranges than a crew-served weapon fired by a gunner and exceeded its reliability requirement during IOT&E.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.

J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Thad Cochran
Ranking Member



Director, Operational Test and Evaluation

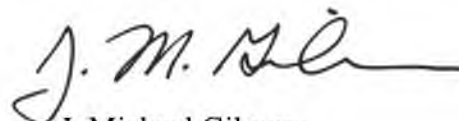
**Warfighter Information Network – Tactical
(WIN-T) Increment 2**

Initial Operational Test and Evaluation



September 2012

This report on the Warfighter Information Network – Tactical (WIN-T) fulfills the provisions of Title 10, United States Code, Section 2399. It assesses the adequacy of testing and the operational effectiveness, operational suitability, and survivability of the WIN-T.


J. Michael Gilmore
Director

The marginal cost of producing this report is estimated to be \$44K. The estimated acquisition cost of the program which this report address is approximately \$10,052.8M.



Components of the Warfighter Information Network – Tactical (WIN-T)

Executive Summary

This is my assessment of test adequacy, operational effectiveness, operational suitability, and survivability of the Warfighter Information Network-Tactical (WIN-T) Increment 2, to support a full-rate production decision review scheduled for September 18, 2012. This assessment is based on the WIN-T Increment 2 Initial Operational Test and Evaluation (IOT&E) conducted May 8-25, 2012 by the Army Test and Evaluation Command at Fort Bliss, Texas; White Sands Missile Range (WSMR), New Mexico; Fort Riley, Kansas; Fort Campbell, Kentucky; and Fort Gordon, Georgia. It was conducted in conjunction with the Army's Network Integration Exercise 12.2. This report is augmented by the Product Qualification Testing – Government (PQT-G) developmental test Phase 1 and Phase 2 that were conducted by the Aberdeen Test Center at Aberdeen Proving Grounds, Maryland. The test locations allowed evaluation of a geographically dispersed network in desert, forest, and urban environments. Testing of the WIN-T Increment 2 was adequate and was conducted in accordance with a Director, Operational Test and Evaluation (DOT&E)-approved test plan.

The test unit, 2nd Brigade, 1st Armored Division, at Fort Bliss/WSMR is a heavy brigade combat team that provided a brigade headquarters and six battalions equipped with WIN-T Increment 2. The 101st Airborne Division at Fort Campbell provided the division-level command posts equipped with WIN-T Increment 2 configuration items. A sustainment brigade at Fort Riley provided a support brigade headquarters and two subordinate battalion command posts. The IOT&E test unit operations included offensive, defensive, and stability missions employed at-the-halt and on-the-move.

The Army intends WIN-T to transport information to the right place at the right time, including when the communications nodes and the unit command centers are on-the-move. The WIN-T communications backbone enables exchange of voice, video, and data throughout theater, corps, division, brigade combat team, battalion, and company-level elements. WIN-T Increment 2 builds upon the WIN-T Increment 1 at-the-halt network to support on-the-move operations. The fundamental new capabilities for Increment 2 are enhanced on-the-move Voice over Internet Protocol (VoIP) telephone and battle command applications. The new technologies that provide these capabilities are the Net-Centric Waveform (NCW) for ground-to-satellite communications, Highband Networking Waveform (HNW) for ground-to-ground, line-of-sight communications, and Colorless Core Security Architecture, which supports multiple security levels and improves network efficiency.

Operational Effectiveness

The WIN-T Increment 2 system contains multiple configuration items and technologies, each of which performed at different levels of effectiveness during the IOT&E. The following WIN-T Increment 2 configuration items and technologies are operationally effective:

- **Tactical Communications Node (TCN)**, a large “mobile cell phone tower” to provide communication and networking for all echelons.

- **Point of Presence (PoP)**, a smaller vehicle to provide a connection to the network for commanders at all echelons.
- **The Net-Centric Waveform (NCW)** for ground-to-satellite communications. The Tactical Communications Node (TCN), Point of Presence (PoP), and Soldier Network Extension (SNE) vehicles use the NCW.
- **Colorless Core Security Architecture**, to support multiple security levels and improve network efficiency.
- **Satellite Tactical Terminal+ (STT+)**, a trailer-mounted satellite terminal which provides greater satellite bandwidth to the TCN at-the-halt.
- **Network Operations and Security Center (NOSC)**, to support network management.
- **Vehicle Wireless Package (VWP)**, to provide a short-range wireless connection to TCNs on-the-move and at-the-halt.
- **Modular Communications Node – Basic (MCN-B)**, a tactical fiber linked communications package that provides Non-secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) access up to 1 kilometer away from the TCN.
- **Joint Gateway Node (JGN)**, to connect to Joint, strategic, allied, coalition, and commercial networks at large command centers.

The following configuration items and technologies are not operationally effective:

- **Soldier Network Extension (SNE)**, to provide a network connection to company commanders.
- **Highband Networking Waveform (HNW)**, to provide terrestrial network connectivity to TCN and PoP vehicles to reduce demand on NCW satellite resources.
- **Tactical Relay – Tower (TR-T)**, a 30-meter mast to extend the range of the HNW line-of-sight communications network.

WIN-T Increment 2 network management demonstrated improvement over the 2009 Limited User Test (LUT) by the addition of improved training and improved software tools. System self-monitoring, both locally and remotely from the NOSC, worked well. Users had several different ways of monitoring network status and could query network details as needed. The NOSC-reported status was consistent with the actual network. While the NOSC software toolkit was effective to execute network operations at the division and brigade, the battalion network managers and the TCN operators do not have the sufficient network management tools to perform their mission.

WIN-T Increment 2 relies upon the TCN, PoP, and SNE to provide the Army's "initial on-the-move" network. The TCN and PoP met the unit's mission requirements for throughput and performance, as indicated by instrumented data collected during the IOT&E and Soldiers' positive evaluations. The TCN and PoP provided division, brigade, and battalion staff on-the-

move voice and data communications and decreased Tactical Operations Center (TOC) displacement times. The SNE did not meet the unit's mission requirements. SNE users experienced low VoIP success rates, delays when communicating, low file transfer rates, and poor quality of service. The SNE mission command applications were not useful to Soldiers due to insufficient SNE bandwidth.

Given sufficient satellite bandwidth, the NCW supported unit operations both at-the-halt and on-the-move. The NCW consistently provided a large number of network connections. At WSMR, the NCW provided the means to maintain network connections to most Increment 2 network nodes. At Fort Campbell, the NCW provided reliable means to connect the stationary division Joint Operations Center (JOC) and the division Tactical Command Post (TAC) located 30 kilometers away. During on-the-move operations (twice daily convoy movements), the TCN and PoP demonstrated that NCW provides a reliable network connection when not obstructed by overhead vegetation or urban terrain.

Unexpected drops of NCW routes between Increment 2 configuration items occurred during the IOT&E. There is the potential for interrupted service for VoIP, chat, and mission command applications when NCW routes are dropped. Although the operational impact of dropped NCW nodes was not evident during the IOT&E, dropped NCW routes could become a problem as the Army increases the size of the WIN-T network and moves to more real-time applications that require higher bandwidth among numerous users.

The terrestrial HNW line-of-sight network demonstrated poor transmission range in vegetation, rolling hills, and urban terrain. The TR-T was not able to keep the HNW line-of-sight networks connected to static and mobile users. Because terrain and vegetation interfered with the HNW's line-of-sight, the number of HNW connections maintained by TCN and PoP vehicles dropped when the vehicles were on-the-move. While attempting to restore the dropped HNW connections, the WIN-T Increment 2 network cycled between NCW satellite communications and line-of-sight HNW. Cycling between HNW and NCW increases the amount of network bandwidth needed for "overhead," which is bandwidth used for network routing information, not user content. This increased overhead disrupted network connections across the HNW network, including connections between vehicles which were not moving.

During the IOT&E, the unit's network managers limited the number of allowable HNW connections to minimize the disruptions caused by HNW and NCW cycling. Network management reduced the occurrence of network disruptions but also reduced network performance. If not corrected, the impact of HNW and NCW cycling will increase as the Army increases the size of the WIN-T Increment 2 network.

Operational Suitability

Overall, WIN-T Increment 2 is not operationally suitable. The VWP and MCN-B are reliable. The other six WIN-T Increment 2 configuration items did not meet their reliability requirements. VWP and JGN are maintainable. The other six items did not meet their maintainability requirements. None of the on-the-move platforms (i.e., TCN, PoP, or SNE) met their reliability requirements or their maintainability requirements. There were twice the number

of Field Service Representatives (FSRs) performing maintenance during the IOT&E relative to the Army's support plan, and repair times for half of the configuration items were observed to take 2-4 times longer than the Army's Mean Time to Repair (MTTR) requirements. Four of six of the items that did not meet reliability requirements have a reliability growth potential that is lower than the Army's new lower threshold reliability requirement. This means that it is not likely that these configuration items will reach their reliability requirements via executing a test-fix-test growth program exclusively. This should not discourage current or future test-fix-test cycles, but rather temper expectations for the reliability levels that can realistically be achieved by such means. The primary operational impacts of low reliability and long repair times on the WIN-T Increment 2 configuration items include:

- more frequent loss of essential functions;
- increased life-cycle costs in terms of repair parts and maintenance man-hours;
- increased logistical footprint, and;
- lower operational availability to commanders and Soldiers.

Soldiers at brigade were able to maintain the system, but Soldiers at the TAC, battalions, and companies were dependent on 12 contractor FSRs within the brigade to maintain the system. The FSRs employed during the IOT&E were twice the number specified in the Army's Maintenance Support Plan.

Since the PoP, SNE, and VWP lack independent power, Soldiers operated the vehicles' engines continuously to provide power for these systems. This continuous operation of vehicles' engines produced excessive noise, engine wear, and fuel consumption. The WIN-T Increment 2 TCN, PoP, and SNE are armored, wheeled vehicles, which prevented these vehicles from keeping up with tracked vehicle formations moving through open terrain. WIN-T Increment 2 vehicles cannot be transported by rotary-wing aircraft, which limits their ability to accompany units that use aircraft for mobility.

Survivability

The WIN-T Increment 2 is not survivable. WIN-T Increment 2 had significant Information Assurance vulnerabilities during the IOT&E that would degrade a unit's ability to succeed in combat. The Army Research Laboratory, Survivability/Lethality Analysis Directorate (ARL/SLAD) and the Army's Threat Systems Management Office (TSMO) team conducted threat computer network operations and Information Assurance scans of the WIN-T Increment 2 network. The TSMO team conducted open-air electronic warfare and testing against the WIN-T Increment 2. The results of these tests are discussed in a classified annex to this report.


Recommendations

The Army should consider the following actions to improve the WIN-T Increment 2:

- **Improve Reliability.** The Army should dedicate resources to fix WIN-T Increment 2's demonstrated reliability and improve the network's ability support the

- probability of completing a 72-hour mission. Reliability improvements should be demonstrated during a future operational test event.
- Consider appointing an independent reliability, availability, and maintainability (RAM) review panel to complete a reliability growth strategy that includes test-fix-test activities and, where not capable of meeting reliability goals, recommend configurations for materiel redesign.
 - Perform a lifecycle cost analysis of the demonstrated IOT&E Mean Time Between Essential Function Failure values and determine the additional costs for maintenance support of the WIN-T Increment 2 due to poor reliability.
 - **Soldier Network Extension.** The Army should identify the root causes of and correct the poor performance of the SNE and demonstrate its effectiveness in a future operational test event.
 - **Improve WIN-T Increment 2 Waveforms.** The Army should conduct further testing, assessment and improvement of HNW and NCW to address deficiencies noted during the IOT&E. Waveform improvements should be demonstrated during a future operational test event.
 - Improve HNW transmission range. The HNW waveform has limited range in vegetation, urban, or complex terrain. The Army should consider solutions for increasing the HNW transmission range, such as using multiple frequency bands and/or increasing radio transmission power.
 - Improve HNW stability. As supported mobile platforms moved, the HNW network demonstrated instability that included bandwidth reductions, cycling issues with NCW, and disruption of adjacent HNW node services. The Army should assess the cause of poor HNW network stability and correct these deficiencies.
 - Improve NCW stability (route drop). The Army should identify the root causes of and correct the NCW dropped routes demonstrated during IOT&E.
 - **Tactical Relay – Tower.** The single TR-T supporting the HNW network was not able to support the brigade's dispersion during offensive operations. In addition to fixing the TR-T materiel deficiencies, the Army should assess the fielding quantities of TR-Ts to support brigade operations.
 - **Survivability.** The Army should address the deficiencies and recommendations listed in the classified annex and the ARL/SLAD report.
 - **Electronic Warfare.** The Army should assess NCW and HNW under an operationally realistic electronic warfare threat during a future operational test event.
 - **Network Management.** The Army should improve network management tools:
 - Improve the ability to manage the HNW network.

- At the brigade TAC, battalion, and TCN, provide the option to display the entire brigade network and train soldiers to assume network management in the absence of the brigade TOC.
- Provide the ability to display status information for mission command applications and communications systems operating within the unit's area of responsibility.
- **Mission Command Applications.** The Army should create and operationally implement a mission command applications architecture that is based upon mission requirements (both on-the-move and at-the-halt) by echelon that is supportable by the WIN-T Increment 2 network.
- **Training.** The Army should improve WIN-T Increment 2 training to include operation of the Combat Net Radio Gateway, increased maintenance for operators, and basic network fundamentals for battalion and company network managers.
- **Mobility.** The Army should assess WIN-T Increment 2 mobility against its full range of potential missions and demonstrate combat vehicle integration in future operational test events.
- **Power.** The Army should provide independent power sources for WIN-T Increment 2 configuration items to prevent continuous operation of vehicle power.
- **Configuration Item Basis of Issue Plan.** The Army should reassess the distribution of VWP and SNE configuration items to support unit at-the-halt and on-the-move operations.


J. Michael Gilmore
Director

Contents

System Overview	1
Test Adequacy	11
Operational Effectiveness	15
Operational Suitability	31
Survivability	39
Recommendations	41

This page intentionally left blank.

Section One

System Overview

System Description

The Army intends the Warfighter Information Network – Tactical (WIN-T) to transport information to the right place at the right time, including when the communications nodes and the unit command centers are moving. The WIN-T communications backbone enables exchange of information (voice, video, and data) throughout theater, corps, division, brigade combat team, battalion, and company-level elements. WIN-T Increment 2 builds upon the WIN-T Increment 1 at-the-halt network to support on-the-move operations. The fundamental new capabilities for Increment 2 are enhanced on-the-move Voice over Internet Protocol (VoIP) telephone and battle command applications. The new technologies that provide these capabilities are:

- Net-Centric Waveform (NCW) for ground-to-satellite communications. Tactical Communications Node (TCN), Point of Presence (PoP), and Soldier Network Extension (SNE) vehicles all use the NCW. Each maneuver brigade has a distinct NCW network to provide connectivity when the command centers are at-the-halt and to connect the Increment 2 mobile configuration items when the brigade is on-the-move.
- Highband Networking Waveform (HNW) for ground-to-ground, line-of-sight communications. The HNW provides additional connectivity to TCN and PoP vehicles within the formation to off-load traffic from the satellites when line-of-sight exists. SNE vehicles are not HNW-capable. There is an HNW network at the division level and each maneuver brigade has a separate brigade HNW network.
- Colorless Core Security Architecture. The Colorless Core supports multiple security levels by leveraging a common internet protocol (IP) backbone to simplify network management and optimize bandwidth allocation. The Colorless Core transmits everything over IP and encrypts all traffic, whether classified or not, with a Type I High Assurance IP Encryptor (HAiPE)-compliant device. The traffic from each classification enclave then flows through a Colorless Core private network router through the transmission system.

WIN-T Increment 2 Configuration Items

The WIN-T Increment 2 Initial Operational Test and Evaluation (IOT&E) examined the effectiveness the three technologies listed above (NCW, HNW, and Colorless Core), as well as the following 9 configuration items:

- Tactical Communications Node (TCN)
- Point of Presence (PoP)
- Soldier Network Extension (SNE)
- Satellite Tactical Terminal+ (STT+)

- Tactical Relay – Tower (TR-T)
- Network Operations and Security Center (NOSC)
- Vehicle Wireless Package (VWP)
- Modular Communications Node – Basic (MCN-B)
- Joint Gateway Node (JGN)

The effectiveness evaluation did not include assessment of a tenth WIN-T configuration item, the Regional Hub Node (RHN), because the Network Service Center – Training (NSC-T) at Fort Gordon provided connectivity between the increments that replicated the support provided by an RHN.

Tactical Communications Node (TCN)

The TCN (Figure 1-1) provides communication and networking services at-the-halt and on-the-move. A TCN is employed at the division, brigade, and maneuver battalion levels. The TCN is best described as a “mobile cell phone tower” connected to the network using both HNW line-of-sight and NCW satellite communications. The TCN provides an array of communications services, including secure and non-secure local area networks (LAN) and VoIP phones, computer, and video networking. TCNs also provide a Combat Net Radio Gateway to interconnect multiple, shorter-range legacy combat net radios, such as the Single Channel Ground and Airborne Radio System (SINCGARS.)

The TCN is integrated into the armored Family of Medium Tactical Vehicles (FMTV), and the TCNs tested during IOT&E were production-representative. The circular antenna for the HNW line-of-sight network is mounted on a 10-meter telescoping mast located just aft of the TCN’s cab. The flat plate Range Throughput Extension Kit (RTEK) antenna extends the range of a single HNW link, and is also on the mast. The mast must be stowed in the down position for travel, and can be extended at-the-halt. The generator for on-the-move operations is in the center of the vehicle over the forward dual or second axle. A larger towed generator is used at-the-halt. In the rear of the vehicle atop the electronics bay is the dome that houses the NCW satellite communications antenna.



Figure 1-1. WIN-T Increment 2 TCN

Point of Presence (PoP)

As with the TCN, the PoP (Figure 1-2) provides at-the-halt and on-the-move connection to the network using HNW line-of-sight and NCW satellite communications. The PoP is employed at the division headquarters (three vehicles), the brigade headquarters (two vehicles), and maneuver battalion headquarters (one vehicle per headquarters). PoP capabilities include VoIP and a suite of mission command applications. The mission command applications installed in the Mine Resistant Ambush Protected (MRAP) vehicles during the Increment 2 IOT&E were:

- Force XXI Battle Command Brigade and Below Joint Capability Release (FBCB2 JCR) with Chat
- Tactical Ground Reporting (TIGR)
- Command Post of the Future (CPOF)
- Advanced Field Artillery Tactical Data System (AFATDS)
- Jabber Chat

All of these applications can be displayed on the WIN-T-provided display that is used to manage the PoP.

The HNW line-of-sight antenna is mounted on the roof just forward of the rear axle. The 20-inch NCW satellite communications antenna is mounted on the roof at the rear of the vehicle. The PoP was integrated into 11 unit-provided MRAP vehicles for the IOT&E. The PoPs provided for IOT&E were production-representative.



Figure 1-2. WIN-T Increment 2 PoP, Installed in an MRAP All-Terrain Vehicle (M-ATV)

Soldier Network Extension (SNE)

The SNE (Figure 1-3) provides at-the-halt and on-the-move connection to the network via NCW satellite communications only. SNE nodes are employed by company commanders throughout a brigade combat team. Capabilities include VoIP and mission command applications. The mission applications installed in the SNE during IOT&E were the same as those installed in the PoP. Like TCNs, SNE vehicles provide a Combat Net Radio Gateway to interconnect shorter-range legacy combat net radios. PoP vehicles do not have this capability.

The dome at the rear of the SNE vehicle houses the 18-inch NCW satellite communications antenna. This antenna is smaller than the 20-inch PoP satellite antenna. The Army installed 33 SNEs in unit-provided MRAPs for the Increment 2 IOT&E. The majority of SNEs were used by Company Commanders. The battalion commanders for 1-35 Armor and 1-6 Infantry had SNEs installed in their MRAPs, in accordance with the Army fielding plan. The PoPs within these two battalions, typically used by the battalion commanders, were installed in the battalion S-3 vehicles. The SNEs used during IOT&E were production-representative.



Figure 1-3. WIN-T Increment 2 SNE, Installed in an M-ATV

Satellite Tactical Terminal+ (STT+)

The STT+ (Figure 1-4) is a towed, trailer-mounted satellite terminal with an on-board generator which provides greater satellite bandwidth to the TCN when it is stationary. The STT was developed during the Increment 1 program. The STT+ supports the Increment 1 frequency division multiple access (FDMA) and time division multiple access (TDMA) waveforms, and the Increment 2 NCW. During the IOT&E, only the FDMA and the NCW waveforms were used. The STT+ items used in IOT&E were production-representative.



Figure 1-4. WIN-T STT+

Tactical Relay – Tower (TR-T)

The TR-T (Figure 1-5) is a 30-meter mast providing a relay capability to extend the range of the HNW line-of-sight communications network. Two TR-Ts are fielded to each division. During the IOT&E, one TR-T was at Fort Campbell and one was at Fort Bliss/WSMR. The TR-Ts used were production-representative.



Figure 1-5. WIN-T TR-T

Network Operations and Security Center (NOSC)

The Increment 2 NOSC (Figure 1-6) provides the hardware and software infrastructure to support Soldier network management of the WIN-T Increment 2 network. The Increment 2 NOSC has two designs, one to support the brigade (NOSC-B) and another to support the division (NOSC-D). The NOSC supports communications planning, monitoring, network configuration and management, and Information Assurance.

Like the TCN, the NOSC is integrated into an FMTV truck. Network management components are permanently housed and operated in the vehicle shelter on the FMTV. The set of network management laptops in the command posts are connected to the equipment in the NOSC via tactical fiber optic cable. The NOSC acquires transmission services from a co-located TCN. The NOSC includes a trailer with an environmental control unit and generator. The NOSC used for IOT&E was production-representative.



Figure 1-6. WIN-T NOSC

Vehicle Wireless Package (VWP)

The VWP is a communications package designed to connect subscribers over the air to TCNs. The parent TCN provides a wireless “hot spot” for VWP-equipped vehicles. It provides wireless connectivity to Secret IP Router Network (SIPRNET) and Non-secure IP Router Network (NIPRNET) through the Local Access Waveform at a required range of 4 kilometers.

Modular Communications Node – Basic (MCN-B)

The MCN-B (Figure 1-7) is a tactical fiber link which provides NIPRNET and SIPRNET access to buildings and tents up to 1 kilometer away from the parent TCN. The MCN-B transit cases are transported as loose cargo on the back of the TCN.



Figure 1-7. WIN-T MCN-B

Joint Gateway Node (JGN)

The JGN (Figure 1-8) provides capabilities for WIN-T to connect to current Joint, strategic, allied, coalition, and commercial networks at large command centers. The JGN is a transit case assemblage that travels with a TCN.



Figure 1-8. WIN-T JGN

Regional Hub Node

A Regional Hub Node (Figure 1-9) is a satellite ground station to provide long haul tactical communications and network management services to users, such as those using WIN-T. Regional Hub Nodes are fixed sites at five locations worldwide. They will be upgraded to support WIN-T Increment 2 waveforms. The Army intends each Regional Hub Node to have

sufficient numbers of modems and transmission bandwidth to support three divisions and a corps headquarters.



Figure 1-9. Regional Hub Node

Concept of Employment

Figure 1-10 portrays the notional concept of employment of WIN-T Increment 2 waveforms at the division and below. Each maneuver brigade has a separate NCW satellite network. A division has four maneuver brigade NCW networks plus a division-level network. The HNW line-of-sight network supports all division nodes.

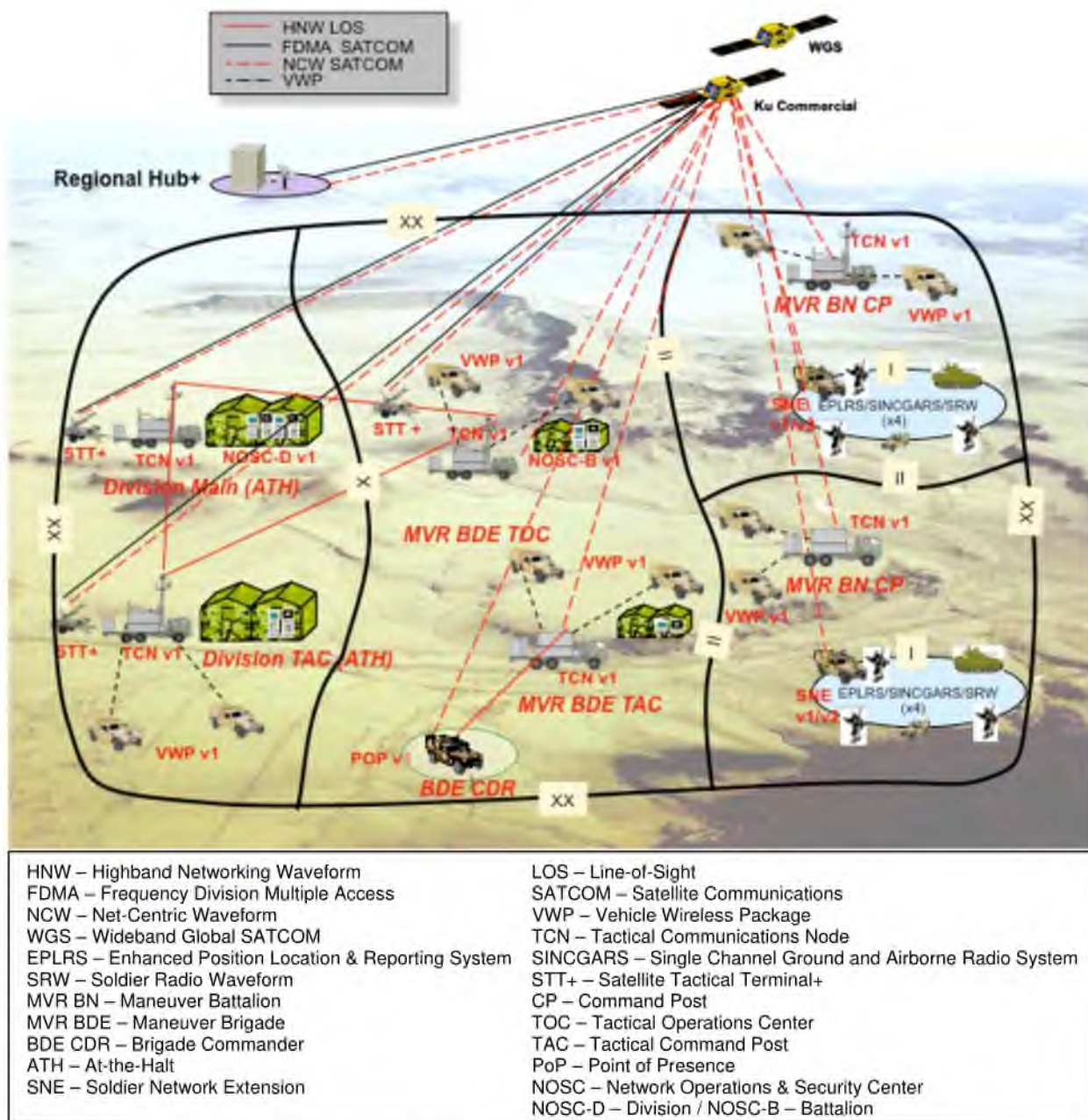


Figure 1-10. WIN-T Increment 2 Division-Level Communications Network (Notional)

This page intentionally left blank.

Section Two Test Adequacy

Operational Testing

The operational testing of the Warfighter Information Network – Tactical (WIN-T) Increment 2 was adequate to support an assessment of the communications system’s operational effectiveness, suitability, and survivability. The test was conducted in accordance with the Director, Operational Test and Evaluation (DOT&E)-approved test plan and is intended to support a full-rate production decision review scheduled for September 2012.

The evaluation is based upon the WIN-T Increment 2 Initial Operational Test and Evaluation (IOT&E) and developmental testing. During May 8-25, 2012, the Army Test and Evaluation Command (ATEC) conducted the WIN-T Increment 2 IOT&E record test as part of the Network Integration Evaluation (NIE) 12.2 at Fort Bliss, Texas; White Sands Missile Range (WSMR), New Mexico; Fort Riley, Kansas; Fort Campbell, Kentucky; and Fort Gordon, Georgia.

These locations allowed the WIN-T Increment 2 IOT&E to test in desert, forest, and urban environments. ATEC Aberdeen Test Center conducted Phase 1 and Phase 2 of the Product Qualification Testing – Government (PQT-G) developmental testing at Aberdeen Proving Grounds, Maryland. The operational test dates and the events that led up to the IOT&E appear in Table 2-1.

Table 2-1. Test Schedule

Activity	Date
Garrison Communications Exercise	April 9-13, 2012
Field Communications Exercise	April 16-25, 2012
New Equipment Training (NET)	January 4 – March 16, 2012
NET Crew Drills (Fort Bliss)	March 7-16, 2012
NET Crew Drills (Fort Campbell)	March 12-23, 2012
Instrumentation Verification and Validation	April 9-27, 2012
Pilot Test	April 30 – May 4, 2012
Pilot Test Data Authentication	May 5-6, 2012
Operational Test Readiness Review 3	May 7, 2012
Record Test	May 8-25, 2012

The test unit, 2nd Brigade, 1st Armored Division, at Fort Bliss/WSMR, is a heavy brigade combat team that provided a brigade headquarters and six battalions equipped with WIN-T Increment 2. The 101st Airborne Division at Fort Campbell provided the division-level command posts equipped with WIN-T Increment 1a and WIN-T Increment 2 configuration items. A sustainment brigade at Fort Riley provided a support brigade headquarters and two subordinate battalion command posts equipped with WIN-T Increment 1b. The Network Service

Center – Training (NSC-T) at Fort Gordon provided connectivity between the increments that replicated the support provided by a Regional Hub Node.

Test Scenario

The test units executed decisive action operations that included offensive, defensive, and stability missions employed at-the-halt and on-the-move. The 101st Airborne Division headquarters issued warning orders (WARNOs), fragmentary orders (FRAGOs), and operations orders (OPORDs) to transition the test through scenario phases. Each phase was designed in accordance with the requirements of the 72-hour Operational Mode Summary/Mission Profile (OMS/MP). The 18-day operational test included the following phases:

- **Phase I.** The brigade occupied Tactical Assembly Area (TAA) Anzio and prepared for combat.
- **Phase II.**
 - **Phase IIa.** The cavalry squadron reconnoitered Route Gold and Objective Bear, developing situational awareness of friendly and threat composition.
 - **Phase IIb.** The cavalry squadron moved forward past the armor and infantry units.
 - **Phase IIc.** The cavalry squadron screened along Route Bronze, prevented reinforcement against the Division objective's western flank. The armor unit provided area security near Objective Wolf and the infantry unit provided area security near Objective Bear.
- **Phase III.** The cavalry squadron continued to screen along Route Bronze to prevent reinforcement against the Division objective's western flank. The armor unit seized Objective Hawk and reestablished the international border. The infantry unit interdicted the enemy to prevent consolidation of enemy forces to the rear of Division objective.
- **Phase IV.** The cavalry squadron continued screening Route Bronze, preventing reinforcement against the Division objective's western flank. The armor unit provided area security of Objective Hawk to prevent consolidation of defeated enemy forces. The infantry unit disrupted enemy lines of communication, preventing consolidation of enemy forces to the rear of Division objective.
- **Phase V.** The brigade transitioned area of operation security to Ellisian Forces and prepared for future operations.

The division and brigade's movement of tactical operations centers and units allowed the IOT&E to test the on-the-move capability of WIN-T Increment 2. Table 2-2 provides a summary of unit movements during the WIN-T Increment 2 IOT&E.

Table 2-2. WIN-T Increment 2 Unit Movements

UNIT	Location 1	Move 1	Location 2	Move 2	Location 3	Move 3	Location 4	Move 4	Location 5
101st Joint Operations Center	Old Theater	None							
101st Tactical Operations Center	WIN-T Training Area	May 15	OP 12 Range	May 17	WIN-T Training Area				
Brigade Main	TAA Anzio	May 12	Oro Grande	May 19	Space Harbor	May 24	TAA Anzio		
Brigade Tactical Operations Center	TAA Anzio	May 9	Al Jarbah	May 15	Space Harbor	May 19	Tula then Oscura	May 24	Oro Grande
Brigade Special Troops Battalion	TAA Anzio	May 12	Oro Grande	May 19	Space Harbor	May 24	TAA Anzio		
1-1 Cavalry Squadron	TAA Anzio	May 12	Al Jarbah	May 15	RCRC	May 24	Oro Grande		
1-6 Infantry Battalion	TAA Anzio	May 11	Oro Grande	May 14	East of Dona Anna	May 24	TAA Anzio		
1-35 Armor Battalion	TAA Anzio	May 12	CACTF	May 19	Tula then Oscura	May 24	Oro Grande		
B/1-35 Armor Battalion	TAA Anzio	May 12	CACTF	May 15	RCRC	May 19	Tula		
4/27 Field Artillery Battalion	TAA Anzio	May 12	Oro Grande	May 19	Space Harbor	May 24	TAA Anzio		
47 Brigade Support Battalion	TAA Anzio	May 10	LSA Black	May 20	901 Complex	May 24	TAA Anzio		

TAA – Tactical Assembly Area

RCRC – Red Canyon Range Camp

CACTF – Combined Arms Collective Training Facility

Information Assurance

During IOT&E, the Army Research Laboratory Survivability/Lethality Analysis Directorate (ARL/SLAD) conducted Information Assurance assessments on WIN-T Increment 2 that included:

- Step 4 – Operational Information Assurance Vulnerability Evaluation
- Step 5 – Protect, Detect, React, and Restore Evaluation
- Step 6 – Continuity of Operations Evaluation

These tests were performed in accordance with the DOT&E memorandum “Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs,” dated January 21, 2009.

Electronic Warfare

During the IOT&E, Electronic Warfare (EW) testing consisted of open-air jamming and direction finding operations. The Threat Systems Management Office (TSMO) provided and operated the jamming, direction finding, and GPS-imitating equipment to support the multiple 72-hour scenarios in an EW environment. All threats portrayed were in accordance with the accredited threat training support package for WIN-T Increment 2.

System Support

Field Service Representatives (FSRs) participated in the IOT&E as sustainment-level maintenance. FSR support of the operation, maintenance, and support of WIN-T Increment 2 IOT&E exceeded the maintenance support concept for a heavy brigade combat team that provides six FSRs. During the WIN-T Increment 2 IOT&E, the program provided six FSRs on the day shift and six additional FSRs on the night shift.

Test Limitations

The Army conducted the WIN-T Increment 2 IOT&E in accordance with a DOT&E-approved test plan. Test limitations were:

- **Lack of Network Planning.** The test unit did not plan the WIN-T IOT&E network. The Army used the Brigade Modernization Command and contractors to conduct network planning and to configure WIN-T Increment 2 systems. During unit movements, the division and brigade network management teams planned network reconfigurations.
- **Satellite Bandwidth.** The WIN-T Increment 2 IOT&E was a brigade-level operational test with two Net-Centric Waveform networks. The Army reserved satellite bandwidth that exceeded the operational demand by almost three times the IOT&E usage.
- **Signal Site Security.** The Tactical Relay – Tower (30-meter mast) and the Soldier Network Extension retransmission vehicles were deployed throughout the operating area without force protection.

Section Three

Operational Effectiveness

The Warfighter Information Network – Tactical (WIN-T) Increment 2 is composed of several configuration items and technologies, each of which performed at different levels of effectiveness during the Initial Operational Test and Evaluation (IOT&E). The following configuration items and technologies were operationally effective:

- Net-centric Waveform (NCW)
- Tactical Control Node (TCN)
- Point of Presence (PoP)
- Colorless Core Security Architecture
- Satellite Tactical Terminal+ (STT+)
- Network Operations and Security Center (NOSC)
- Vehicle Wireless Package (VWP)
- Modular Communications Node – Basic (MCN-B)
- Joint Gateway Node (JGN)

The following configuration items and technology were not operationally effective:

- Highband Networking Waveform (HNW)
- Soldier Network Extension (SNE)
- Tactical Relay – Tower (TR-T)

Given sufficient satellite bandwidth, the NCW supported unit operations both at-the-halt and on-the-move. The terrestrial HNW line-of-sight network demonstrated poor transmission range in vegetation, rolling hills, and urban terrain. During movement, the WIN-T Increment 2 network cycled between NCW satellite communications and line-of-sight HNW, resulting in loss of network connectivity.

WIN-T Increment 2 relies upon the TCN, PoP, and SNE to provide the Army's "initial on-the-move" network. The TCN and PoP met the unit's mission requirements for throughput and performance, as indicated by instrumented data collected during the IOT&E and Soldiers' positive evaluations. The TCN and PoP provided division, brigade, and battalion staff on-the-move voice and data communications and decreased Tactical Operations Center (TOC) displacement times. The SNE did not meet the unit's mission requirements. SNE users experienced low Voice over Internet Protocol (VoIP) success rates, delays when communicating, low file transfer rates, and poor quality of service. The SNE mission command applications were not useful to Soldiers due to insufficient SNE bandwidth.

WIN-T Increment 2 network management was operationally effective and demonstrated improvement over the 2009 Limited User Test (LUT) by the addition of improved training and

improved software tools. The TR-T was not able to keep the HNW line-of-sight networks connected to static and mobile users.

Network Performance

In addition to using WIN-T Increment 1 waveforms, the WIN-T Increment 2 program developed two new waveforms, the satellite-based NCW and the line-of-sight HNW. The TCN and PoP connect to the network using both waveforms. The PoP and TCN switch between waveforms depending on the ability to connect to HNW or NCW. The network selects HNW when available in order to conserve satellite bandwidth, which may be limited in some theaters. The SNE connects to the Increment 2 network using only the NCW satellite waveform.

The NCW connected most of the 51 available WIN-T Increment 2 configuration items to the network during the IOT&E. The HNW connected a varying subset of the 15 TCNs and PoPs participating in the test. During daylight hours when all of the available configuration items were operational, the Brigade Commander was typically connected to over 45 of the other 51 configuration items provided to commanders and command posts within his brigade using either HNW or NCW. Figure 3-1 illustrates that WIN-T Increment 2 provided good connectivity to support the brigade's operations on-the-move, with NCW serving as the primary waveform connecting the configuration items. The general rise and fall rhythm of the plot is due to Soldiers turning on WIN-T Increment 2 systems in the morning and off at night.

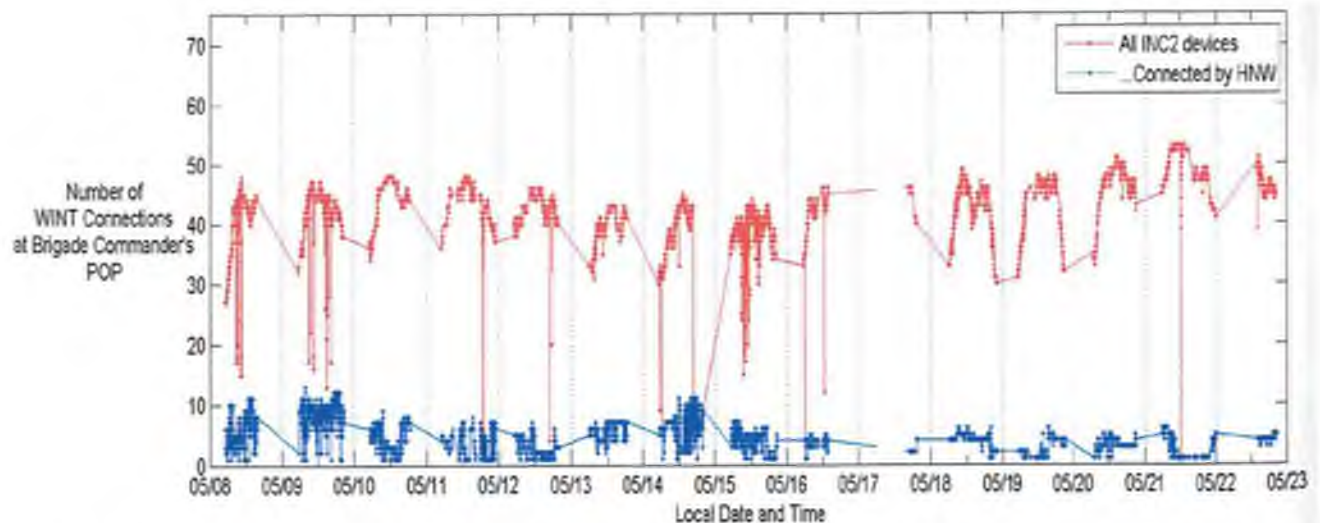


Figure 3-1. Number of WIN-T Nodes Connected to the Brigade Commander's PoP during the IOT&E.

The NCW consistently provided a large number of network connections. The HNW's ability to maintain a commander's connections to the network varied depending on the commander's vehicle location and whether the vehicle was on-the-move. Because terrain and vegetation interferes with HNW's line-of-sight, the number of network connections maintained by HNW dropped while on-the-move. Figure 3-2 shows the connectivity between the Brigade Commander's PoP and the other Increment 2 configuration items present at WSMR on May 10. The upper graph shows the Brigade Commander's distance from the brigade Main Command

Post (MAIN) and the brigade Tactical Command Post (TAC). From 5:00 a.m. until 9:00 a.m., the Brigade Commander's PoP is at the brigade MAIN (41 kilometers from the brigade TAC). Using his PoP, the Brigade Commander moves from the brigade MAIN to the brigade TAC from about 9:00 a.m. to 10:30 a.m., and remains there until 1:00 p.m. He then returns to the brigade MAIN.

The blue line in the bottom graph of Figure 3-2 illustrates that the Brigade Commander was able to connect with about seven HNW-capable line-of-sight nodes using the HNW network while stationary at the brigade MAIN; he was able to connect with about one-third of the HNW line-of-sight nodes while at the brigade TAC. HNW connectivity is higher at the MAIN because there were several battalion TOCs nearby which had HNW nodes. While on-the-move, the commander's HNW connections dropped to as low as one or two. The red line shows that throughout the day, NCW helped maintain the Brigade Commander's connections with most available network nodes.

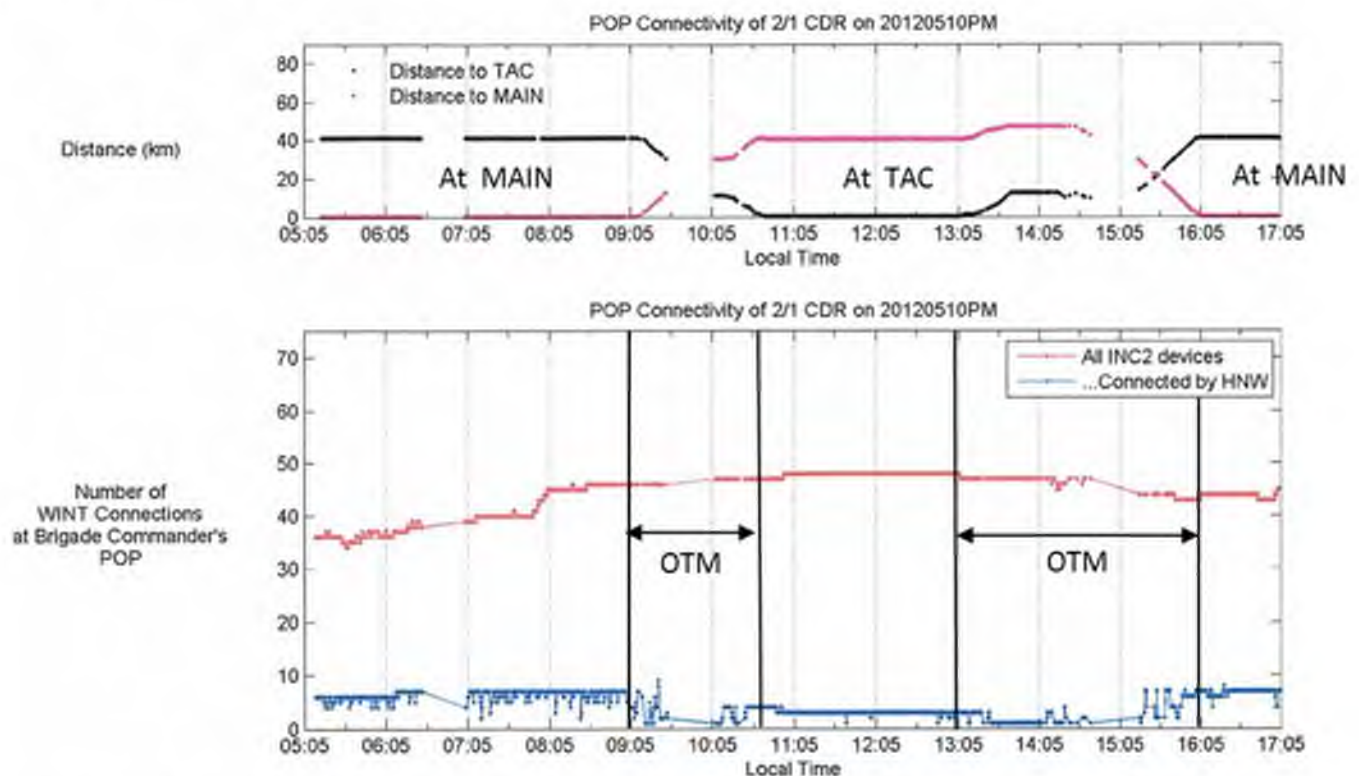


Figure 3-2. Number of WIN-T Increment 2 Configuration Items Connected to the Brigade Commander's PoP from 5:00a.m.-5:00 p.m. on May 10, 2012.

Waveform Performance

Network Centric Waveform

The NCW is operationally effective. At WSMR, the NCW provided the means to maintain network connections to most Increment 2 network nodes (Figure 3-1). At Fort Campbell, the NCW provided reliable means to connect the stationary division Joint Operations

Center (JOC) and the division TAC located 30 kilometers away. During on-the-move operations (twice daily convoy movements) the TCN and PoP demonstrated that NCW provides a reliable network connection when not obstructed by overhead vegetation or urban terrain.

NCW Throughput

Table 3.1 shows the IOT&E throughput rates demonstrated for the key Increment 2 mobile configuration items on-the-move (OTM) and at-the-halt (ATH). These rates are driven by user demand, so a low throughput value in the table does not necessarily mean the Increment 2 configuration item was unable to achieve a higher throughput. It may reflect lack of user demand for a higher bandwidth. For example, the fact that the PoP ATH value in Table 3.1 is lower than the SNE ATH value may be because the commanders transferred from the PoP to the TCN at TAC or MAIN while at-the-halt, and hence had little need to use the PoP for data exchange.

Table 3.1. NCW Throughput Rates for TCN, PoP, and SNE at Fort Bliss/WSMR during the IOT&E.

	TCN OTM	PoP OTM	SNE OTM	TCN ATH	PoP ATH	SNE ATH
NCW Med^a	47 Kbps	26 Kbps	18 Kbps	42 Kbps	8 Kbps	19 Kbps
NCW Peak^b	700 Kbps	126 Kbps	121 Kbps	922 Kbps	110 Kbps	177 Kbps

^a NCW Med is the median throughput measurement.

^b NCW Peak is the throughput threshold which includes 99 percent of total throughput measurements to preclude extreme cases. In other words, 1 percent of throughput measurements (taken every 10 seconds) are higher than the listed value.

The table shows that both the PoP and SNE had low median total throughput compared to the TCN when at-the-halt and on-the-move, indicating less frequent use. The Production Qualification Test – Government (PQT-G) for the PoP and the SNE demonstrated that the PoP can support 400 Kbps and that the SNE can support 200 Kbps while on-the-move. These values met the Army's throughput requirements for the PoP (256 Kbps) and SNE (128 Kbps), and are greater than the user demand during the IOT&E. Commanders and key staff who used both the PoP and the SNE reported that PoP performance was better than the SNE, especially on-the-move. The SNE did not support the unit's mission need during mobile operations.

At-the-halt, the PoP and SNE are capable of using the NCW network in a similar manner, with 90 percent of their throughput rates at 40 Kbps or less during IOT&E. Figure 3-3 shows a cumulative probability distribution chart for the demonstrated NCW throughput values for the TCN, PoP, and SNE over the course of the IOT&E, taken when these vehicles were at-the-halt. It includes data for all of the vehicles in the test. The y-axis of the chart shows the percentage of the time that NCW throughput was equal to or lower than the x-axis value. The vertical line on the chart is at 40 Kbps throughput. The lower horizontal line shows that approximately 0.5 (50 percent) of the TCN throughput values were 40 Kbps or less. The higher horizontal line

shows that for both the PoP and the SNE, 0.85 (85 percent) of the throughput values were 40 Kbps or less. A shallower curve indicates a higher demonstrated throughput.

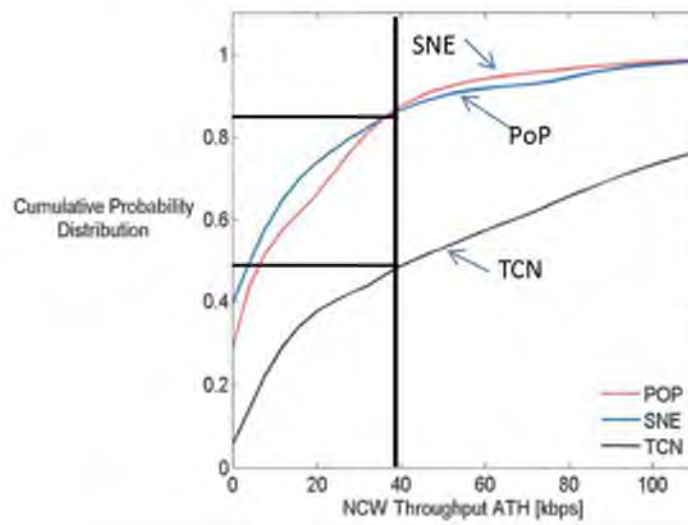


Figure 3-3. NCW Throughput At-the-Halt

On-the-move, the PoP and SNE did not demonstrate similar use of the NCW network. The SNE demonstrated half of its at-the-halt cumulative throughput, with 80 percent of throughput rates at 20 Kbps or less. The PoP demonstrated a cumulative throughput comparable to its at-the-halt value. Figure 3-4 shows the NCW throughput cumulative probability distribution for those periods when the TCNs, PoPs, or SNEs were on-the-move. This figure shows a marked difference between the PoP and SNE demonstrated throughput. 80 percent of the SNE throughput values were 20 Kbps or less, while 80 percent of the PoP throughput values were 40 Kbps or less. The SNE value of 20 Kbps is less than the Army's on-the-move requirement of 64-128 Kbps. Since basic VoIP telephone calls require between 16 and 32 Kbps, this indicates that the PoP's throughput was able to support VoIP most of the time, while the SNE's throughput was not.

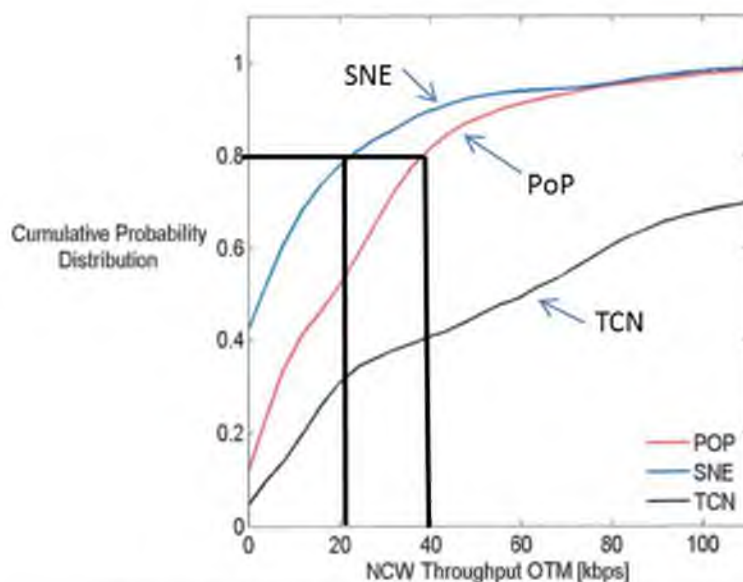


Figure 3-4. NCW Throughput On-the-Move

Used out of context, certain types of IOT&E data show similarities in performance between the PoP and the SNE. For example, the PoP and the SNE showed similar packet completion rates, LAN router availabilities, and Quality Edge Device modes. These data do not provide sufficient information to determine how well user applications, such as VoIP, worked on the PoP and SNE. During the IOT&E, users consistently assessed the TCN and PoP as performing well on-the-move and the SNE as not. The throughput data shown above reflects actual data usage for the PoP and the SNE, and is consistent with the user assessments.

NCW Satellite Bandwidth Usage

The NCW waveform recorded a peak network throughput across the brigade of 3.8 Mbps of user traffic, which was supported by two 36 MHz satellite transponders. User traffic averaged about 1 Mbps. Using two 36 MHz satellite transponders to support a peak of 3.8 Mbps of user traffic is not an efficient use of satellite bandwidth. The Army's analysis shows that there was excess satellite bandwidth reserved for the IOT&E, and that much of this bandwidth was not used.

Highband Networking Waveform

The HNW is not operationally effective. The HNW did not provide sufficient transmission range for mobile operations in vegetation and in urban environments. The waveform demonstrated deficiencies that affected network performance. The HNW is designed to provide line-of-sight connectivity for the TCNs and the PoPs, both at-the-halt and on-the-move. During the IOT&E, the brigade was not able to maintain connectivity across the network using HNW.

Soldiers employed the division's TR-T to connect the stationary division TAC to the stationary division TOC at Fort Campbell. When HNW nodes were on-the-move at Fort Campbell, terrain and vegetation prevented those nodes from reliably connecting to the HNW

network. At WSMR, a single HNW network was maintained in the initial assembly area. As the brigade's vehicles moved north into attack positions, the HNW network began to fragment, and the network split into four segments connected by NCW. TR-Ts deployed at Fort Campbell and WSMR – one at each location – were not able to maintain a contiguous HNW network and were seldom employed.

Table 3.2 shows the total HNW network throughput on-the-move and at-the halt for the TCN and PoP (the SNE does not have HNW capabilities).

Table 3.2. HNW Throughput Rates for TCN and PoP at Fort Bliss/WSMR during the IOT&E.

	TCN OTM	PoP OTM	TCN ATH	PoP ATH
HNW Med^a	35 Kbps	8 Kbps	122 Kbps	35 Kbps
HNW Peak^b	441 Kbps	152 Kbps	927 Kbps	221 Kbps

^a HNW Med is the median throughput measurement.

^b HNW Peak is defined as the throughput threshold which includes 99 percent of total throughput measurements. In other words, 1 percent of throughput measurements (taken every 10 seconds) are higher than the listed value.

Although the peak throughput values are high, the median values are low, especially for the on-the-move TCN and for the PoPs in general. This indicates a low usage of HNW due to the network connection problems discussed above.

HNW demonstrated poor transmission range and poor support of mobile operations in the vegetation and terrain of Fort Campbell. Figure 3-5 shows the time during IOT&E that the Increment 2 network configuration items used the HNW, NCW, or other waveforms (such as legacy waveforms). "HNW-Single Hop" designates routes wherein one Increment 2 node is connected directly to another via HNW. "HNW-Multi-Hop " designates routes where HNW nodes are connected via at least one intermediate HNW node. The data illustrate that during the IOT&E at Fort Campbell, single-hop and multi-hop HNW routes are available less than 10 percent of the time when nodes are greater than 2 kilometers apart.

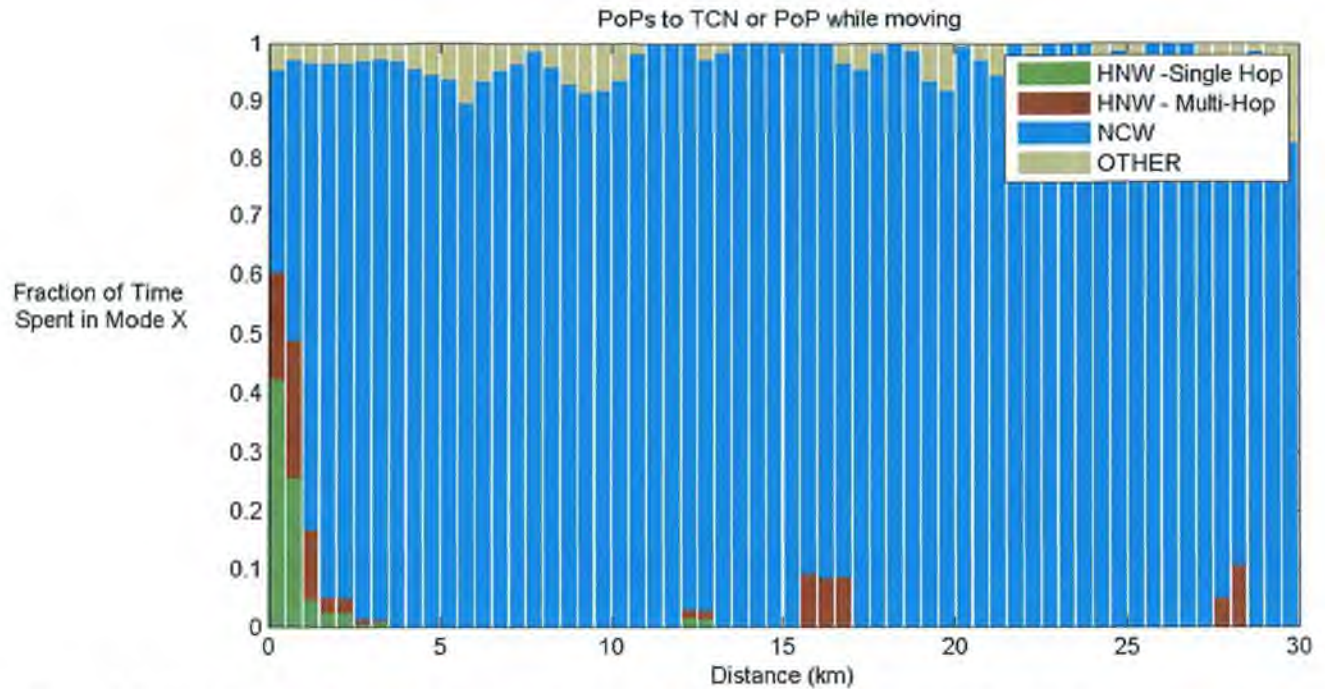


Figure 3-5. Distribution of network connectivity for HNW Single-Hop (green), HNW Multi-Hop (red), and NCW (blue) at Fort Campbell (vegetation). The figure shows percentage of time connected with respective waveform.

HNW supported mobile operations in the desert and terrain of WSMR. Figure 3-6 demonstrates that during the IOT&E at WSMR in a desert valley environment, the maximum single hop range for HNW was 15 kilometers. At 5 kilometers, about one-third of the nodes use single-hop HNW routes, about one-third of the nodes use multi-hop HNW routes, and the remaining one-third of the nodes use NCW satellite routes. As the transmission range increases, the percentage of HNW routes decrease.

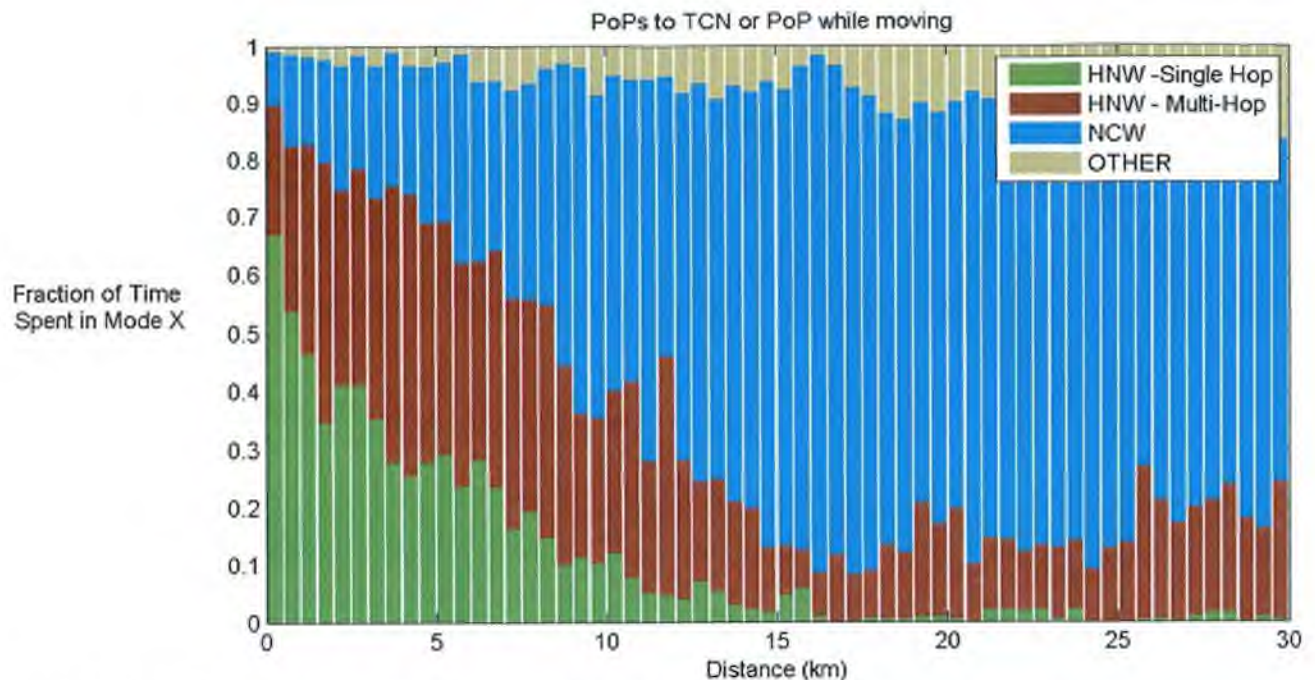


Figure 3-6. Distribution of network connectivity for HNW Single-Hop (green), HNW Multi-Hop (red), and NCW (blue) at Fort Bliss/WSMR (treeless desert valley). The figure shows percentage of time connected with respective waveform, NOT percentage of traffic.

HNW and NCW Cycling

The TCN and the PoP connect to the Increment 2 network either by the NCW or HNW waveforms. They are designed to switch between the two waveforms depending on line-of-sight connectivity. Increment 2 is designed to prefer the HNW line-of-sight network, when available, to reduce traffic on the NCW satellite network.

Changing waveforms increases the amount of network bandwidth needed for “overhead.” Overhead is bandwidth that is used for network routing information, not user content. When HNW-capable vehicles (TCNs and PoPs) move, HNW line-of-sight can be lost, causing the network to attempt to switch to the NCW satellite connection. If the network cycles rapidly between the HNW and the NCW waveforms instead of switching cleanly, the increased overhead can result in decreases in network performance. One way to measure network performance is the packet completion rate (PCR), which indicates what percentage of data packets were successfully transmitted through the network. Developmental testing at Fort Greely, Alaska found that the PCRs decreased from a high of 99.4 percent to as low as 84.5 percent when a mobile PoP was permitted to cycle between waveforms.

During the IOT&E, the WIN-T Increment 2 network cycled between waveforms. The cycling occurred more than half of the time when at least one TCN or PoP moved. During cycling, the unit’s network managers observed disruptions in adjacent HNW-capable vehicles’ ability to support user traffic, even if those vehicles were stationary. For example, a network management Soldier at the NOSC noted that PoP terminals coming into and out of the HNW network reduced the voice and data traffic destined for the division main command post TCN.

To improve network stability, the unit's network managers limited the number of allowable connections for each HNW node. The brigade began the IOT&E with each HNW node having five allowable connections, but eventually restricted connections to as few as two nodes to maintain a stable HNW network. Restricting connections between nodes that have radio line-of-sight reduces the occurrences of network instabilities but also reduces network throughput.

Figure 3-7 illustrates the effect of waveform cycling. The top graph of the figure shows the movement of the Brigade Commander's PoP on May 10, 2012. From 6:00 a.m. to just before 9:00 a.m., the PoP was stationary at the brigade MAIN, where there was a TCN. From this time to 10:00 a.m. the Brigade Commander's PoP traveled to the brigade TAC, where there was another TCN. Both the PoP and the TCN have HNW and NCW capability.

The middle two graphs of Figure 3-7 show cycling between the HNW (blue line) and the NCW (green line) as the Brigade Commander's PoP is traveling to the brigade TAC. Cycling begins to occur when the Brigade Commander's PoP goes out of range of the brigade MAIN TCN's HNW antenna.

The final graph of Figure 3-7 highlights the operational cost of the cycling. The number of HNW nodes that are available to the PoP (and the TCNs at MAIN and TAC) drops at the same time that the cycling begins. The movement of one Increment 2 configuration item (the Brigade Commander's PoP) disrupts the network connections of other, stationary HNW-capable configuration items (the TCNs at MAIN and TAC).

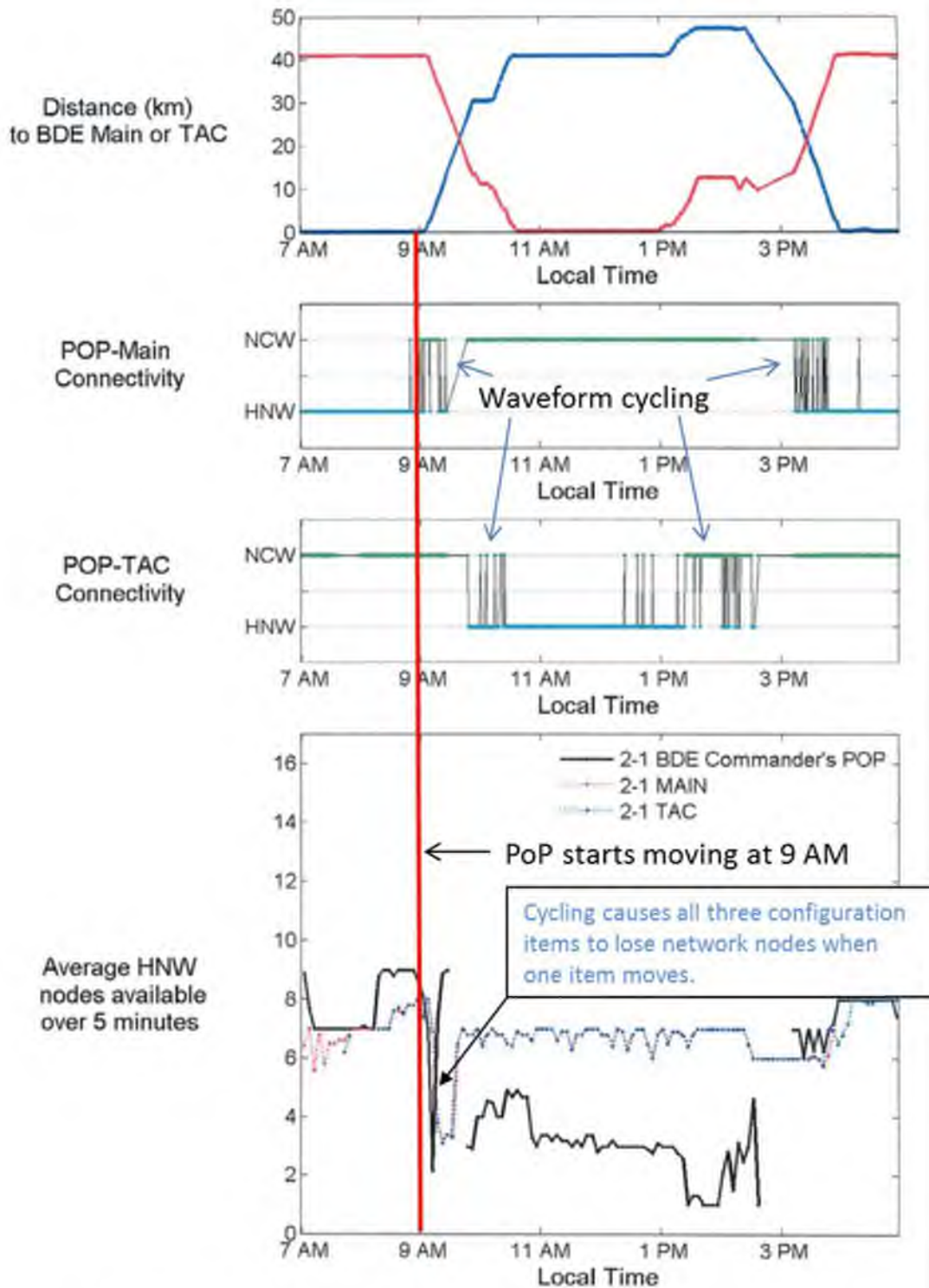


Figure 3-7. Brigade Commander's PoP Cycling between 6:00 a.m. and 6:00 p.m. on May 10, 2012.

The data from the IOT&E showed that moving HNW-capable WIN-T Increment 2 configuration items can cause cycling in the Increment 2 network. This cycling can contribute to dropped network nodes, increased network overhead, and decreased network performance. More

investigation is required to characterize the impacts of waveform cycling and minimize its impact to WIN-T Increment 2 users.

During the IOT&E, NCW users experienced occasional dropped NCW routes to the larger network of NCW-capable vehicles (e.g., TCNs, PoPs, and SNEs). There is the potential for interrupted service for VoIP, chat, and mission command applications when NCW routes are dropped. Figure 3-8 shows several instances of dropped NCW routes on May 9, 2012.

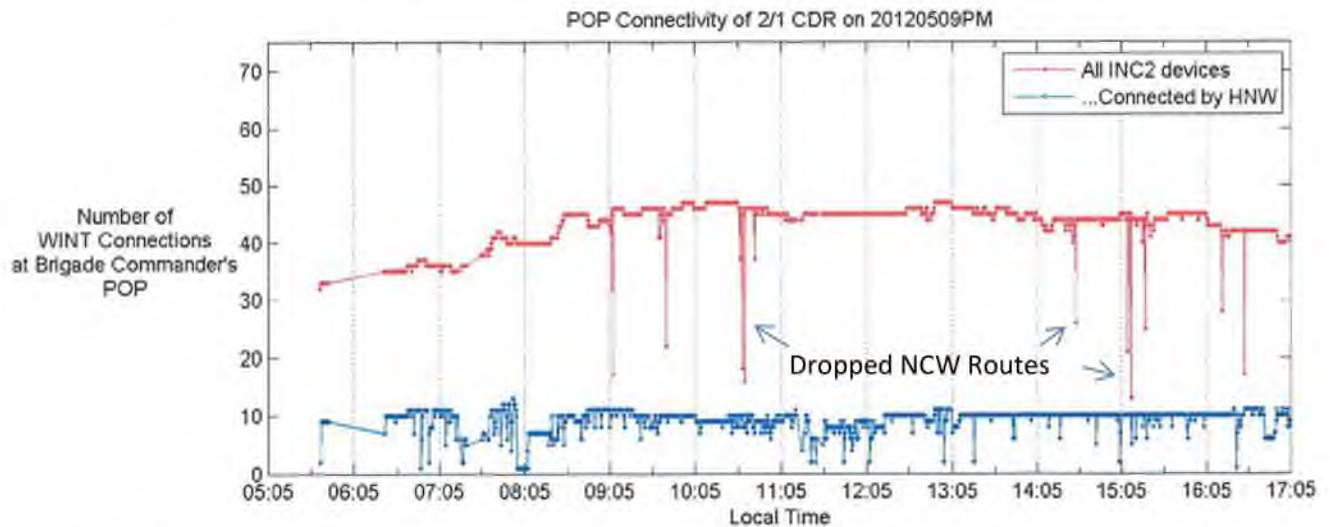


Figure 3-8. Number of WIN-T Increment 2 Configuration Items Connected to the Brigade Commander's PoP on May 9, 2012

During the IOT&E, there were 70 incidents in which at least 10 NCW-capable vehicles lost connectivity with at least 10 NCW routes nearly simultaneously. Some of these incidents appear to involve all NCW-capable vehicles. Figure 3-9 shows, over the course of the IOT&E, the number of reports from NCW-capable vehicles that indicate a loss of 10 or more NCW routes nearly simultaneously (within a two-minute time interval). For example, on May 13, there were close to 40 reports that NCW-capable vehicles lost 10 or more NCW routes nearly simultaneously.

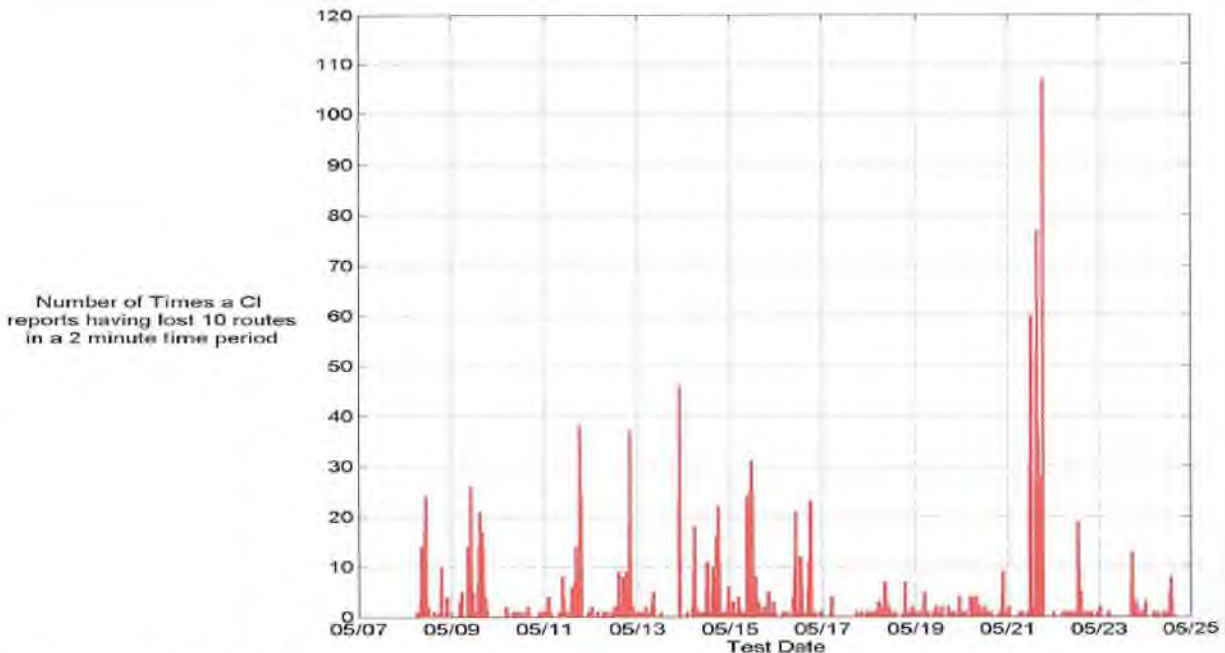


Figure 3-9. Number of Reports of WIN-T Increment 2 Configuration Items Dropping 10 or More NCW Routes Nearly Simultaneously

Because the duration of the dropped NCW routes was less than 30 seconds, the operational impact of the dropped routes was not evident during the IOT&E. Dropped NCW routes could become a problem as the Army scales up the size of the WIN-T network and moves to more real-time applications that require higher bandwidth among numerous users. The program manager should conduct additional testing and analysis of this phenomenon to determine its cause, as well as its potential to affect operations as the size of the WIN-T network increases. The Army should conduct further testing, assessment, and improvement of HNW and NCW to address the deficiencies noted above. To help characterize network cycling and NCW route drop behaviors, the Army should design future tests to collect sufficient data to answer the following questions:

- How does network size and usage affect the cycling or NCW route drop behaviors?
- How do the behaviors change as the number of HNW- and NCW-capable vehicles in motion increases?
- How does different terrain affect the behaviors?
- How long does it take the network to stabilize (i.e., reconverge) after the onset of the behaviors?
- What impact do the behaviors have on battle command applications, VoIP calls, and chat sessions?

Network Management and Operations

WIN-T Network Management is operationally effective and supports unit operations. The tools provided for the IOT&E were improved over those used at the 2009 LUT. During the IOT&E, Soldiers at the division and brigade level were able to monitor and restore the Increment 2 network. This was not demonstrated during the LUT. Division and brigade Soldiers were able to plan and execute network movements to support unit operations and modify the network to optimize performance. One battalion network manager performed a sophisticated reconfiguration of the unit's routers to connect fire support data to the command post. Several shortcomings remain:

- The Army's Network Integration Evaluation (NIE) staff and contractors performed the majority of initial IOT&E network planning. A brigade NOSC should be able to plan their entire network.
- Soldiers at the brigade TAC, at the battalion TOCs, and at the companies required FSR support to maintain the Increment 2 network. They needed additional network management tools to display the entire brigade network. This would allow trained Soldiers to assume network management if the brigade TOC became incapable of doing so.
- Network Operations soldiers at each echelon need additional network management tools to provide status information for all mission command applications and communication systems operating at each echelon.

WIN-T Increment 2 Configuration Items

Tactical Communications Node (TCN)

The TCN is operationally effective. The TCN demonstrated relatively high throughput, was highly regarded by the brigade, and was successful in decreasing TOC set up and teardown times by consolidating all the communications packages into a mobile platform. The TCN provided a connection to the VWP-equipped Command Post Platform (CPP). This enabled data updates while on-the-move for the mission command applications hosted on servers in the CPP.

The TCN demonstrated the Combat Net Radio (CNR) Gateway during the brigade TOC's displacement to Space Harbor. The CNR Gateway provides Increment 2 connectivity between geographically separated Single Channel Ground and Airborne Radio System (SINCGARS) networks. During movement, the TCN CNR Gateways were connected via a VoIP conference call. Moving vehicles with SINCGARS were able to connect to their TCN and to SINCGARS vehicles in other convoys via their TCNs.

Point of Presence (PoP)

The PoP is operationally effective. The PoP was successful in supporting the Soldiers' use of mission command applications, primarily Tactical Ground Reporting (TiGR) and Jabber chat, and provided VoIP connectivity to on-the-move commanders. The PoP lacks an

independent power source, which forces the continuous operation of the PoP vehicle's motor, even at-the-halt, to power WIN-T Increment 2 systems.

Soldier Network Extension (SNE)

The SNE is not operationally effective. The SNE was not able to provide reliable VoIP phone calls at-the-halt for Battalion Commanders, Company Commanders, and staff. On-the-move, the SNE provided poor support of VoIP phone calls. The SNE's bundled mission command applications provided little utility for Soldiers. As discussed above, the SNE's demonstrated throughput and packet completion rate performance was poor compared to the PoP. The Army should perform analysis and testing to determine the cause of the SNE's poor performance. Both the SNE and the PoP had identical software, and both relied heavily on the NCW network (the only waveform available for the SNE). In contrast, the NCW satellite antenna on the SNE is smaller than the antenna on the PoP, and the SNE's antenna tracking mechanism is less capable than the PoP's. The SNE lacks an independent power source for its WIN-T Increment 2 systems.

Colorless Core

The Colorless Core is operationally effective. It supported multiple security levels, simplified network management, and improved bandwidth allocation.

Satellite Tactical Terminal+ (STT+)

The STT+ was operationally effective. It demonstrated simultaneous connectivity on frequency division multiple access (FDMA) and NCW networks in support of at-the-halt operations. This configuration item has evolved over the last five years as a major configuration item of the Joint Network Node (JNN) program (WIN-T Increment 1) and was improved under the WIN-T increment 2 program. The STT+ comes with an onboard backup generator but requires the unit to provide an additional generator.

Data from the Force Development Test and Experimentation (FDT/E) demonstrate that operators accomplished 90 percent of the setup and teardown critical tasks on the first attempt for the STT+.

Tactical Relay-Tower (TR-T)

The TR-T is not operationally effective. At WSMR in a desert valley, the single TR-T assigned to the brigade was not sufficient to prevent fragmentation of the HNW network during commencement of offensive operations and displacement of the unit command posts. The brigade TR-T at WSMR was seldom used after the first week of the IOT&E. With more TR-Ts and associated force protection, the brigade may have been able to connect their network with HNW and reduce NCW satellite demand.

At Fort Campbell, the TR-T extended the range of the HNW network in vegetation by serving as a relay in an elevated location to connect the division JOC and the TAC, separated by 30 kilometers. The TR-T did not provide reliable HNW connectivity for on-the-move PoPs traveling between the JOC and the TAC due to forest vegetation.

Vehicle Wireless Package (VWP)

The VWP is operationally effective. The VWPs were operationally useful at the division and brigade levels. Soldiers used the VWP to provide wireless connectivity for the CPP during on-the-move operations.

The VWP was able to maintain line-of-sight connectivity with the TCN at-the-halt to a range of 2 to 4 kilometers. When both were moving, the range reduced to 200 to 800 meters. The VWP transmission range proved useful, but required users to travel with the TCN during movement.

The placement of VWPs in maneuver battalions limited the VWP's value during the IOT&E. In the maneuver battalions, the VWPs were assigned to the Assistant S3 and Fire Support Officer (FSO). The Assistant S3 was not supported during convoy movements. FSO VWP actually reduced their mission capability, because they were not part of the Battalion TAC movement and could not maintain connectivity (when separated from the TCN).

Network Operations and Security Center (NOSC)

The NOSC is operationally effective. Network management tools supported unit operators at the division NOSC and brigade NOSC. System self-monitoring, both locally and remotely from the NOSC, worked well. Users had several different ways of monitoring network status and could query network details as needed. The NOSC-reported status was consistent with the actual network. While the NOSC software toolkit was effective to execute network operations at the division and brigade, the Battalion network managers and the TCN operators do not have the sufficient network management tools to perform their mission.

Joint Gateway Node (JGN)

The JGN is operationally effective. WIN-T Increment 2 was connected through JGN to the Defense Switched Network, the Defense Red Switched Network, the Public Switched Telephone Network, NIPRNET, and the European Network.

Modular Communications Node – Basic (MCN-B)

The MCN-B is operationally effective. This configuration item, like the STT+, has evolved as part of the JNN program and the WIN-T Increment 1 and 2 programs. While the MCN-B provided acceptable subscriber services at the TOCs and the TACs, the user access cases making up the system are heavy and difficult to load on the TCN. With the addition of the TCN, much of the contents of the MCN-B could be installed in the TCN to improve the time required to set up and tear down the TOCs.

Section Four

Operational Suitability

Overall, the Warfighter Information Network – Tactical (WIN-T) Increment 2 is not operationally suitable. The Initial Operational Test and Evaluation (IOT&E) measured reliability and maintainability of eight of the ten WIN-T configuration items:¹

- Tactical Communications Node (TCN)
- Point of Presence (PoP)
- Soldier Network Extension (SNE)
- Vehicle Wireless Package (VWP)
- Tactical Relay – Tower (TR-T)
- Network Operations and Security Center (NOSC)
- Joint Gateway Node (JGN)
- Modular Communications Node – Basic (MCN-B)

The VWP and MCN-B are reliable. The other six WIN-T Increment 2 configuration items did not meet their reliability requirements. VWP and JGN are maintainable. The other six configuration items did not meet their maintainability requirements. None of the on-the-move platforms (i.e., TCN, PoP, or SNE) met their reliability requirements or their maintainability requirements. There were twice the number of Field Support Representatives (FSRs) performing maintenance during the IOT&E compared to the Army's support plan, and repair times for half of the configuration items were observed to take 2-4 times longer than the Army's Mean Time to Repair (MTTR) requirements. Four of six of the configuration items that did not meet reliability requirements have a reliability growth potential that is lower than the Army's threshold reliability requirement. This means that it is not likely that these CIs will reach their reliability requirements via executing a test-fix-test growth program exclusively. This should not discourage future test-fix-test cycles, but rather temper expectations for the reliability levels that can realistically be achieved by such means. The distribution of all essential function failures observed during the IOT&E is comprised of 46 percent software faults, 32 percent hardware failures, 15 percent operator/maintainer error, and 7 percent unknown or related to support equipment. The primary operational impacts of low reliability and long repair times on the WIN-T Increment 2 configuration items include more frequent loss of essential functions, increased life-cycle costs in terms of repair parts and maintenance man-hours, increased logistical footprint, and lower operational availability to Commanders and Soldiers.

Soldiers at brigade were able to maintain the system, but Soldiers at the Tactical Command Post (TAC), battalions, and companies were dependent on 12 contractor FSRs within the brigade to maintain the system. As stated above, the FSRs employed during IOT&E were twice the number specified in the Army's Maintenance Support Plan.

¹ For the purposes of suitability, the Satellite Tactical Terminal+ was considered part of the TCN.

Since the PoP, SNE, and VWP lack independent power, Soldiers operated their tactical vehicle motors continuously to provide power for these systems. This continuous operation of vehicles produced excessive noise, engine wear, and fuel consumption. WIN-T Increment 2 configuration items are transported by armored, wheeled vehicles, which prevents them from keeping up with armor formations moving through open terrain. WIN-T Increment 2 vehicles cannot be transported by rotary-wing aircraft, which limits their ability to accompany units that use aircraft for mobility.

Reliability data gathered during the IOT&E were adequate. Twelve WIN-T Increment 2 configuration items had onboard reliability data collectors. The remaining reliability data collectors rode in formation with the test unit and engaged operators on a regular basis to record test incidents. Demonstrated reliability estimates for the configuration items that had onboard data collectors are lower than reliability estimates for items that did not have onboard data collectors. This is an indication that failure data may be missing on configuration items that did not have onboard data collectors, and that reliability estimates may be optimistic.

Reliability

The VWP and MCN-B are reliable. The other six WIN-T Increment 2 CIs did not meet their reliability requirements. Following the Limited User Test (LUT) conducted in 2009, the Army changed the mission duration for WIN-T from 120 hours to 72 hours. This lowered the Mean Time Between Essential Function Failure (MTBEFF) requirements for the WIN-T Increment 2 configuration items. The new requirements and the demonstrated MTBEFF estimates from the IOT&E are shown in Table 4-1. In the tables, LCB stands for lower confidence bound. The MTBEFF growth potential is shown in the right-hand column. The growth potential is the theoretical upper-limit that constitutes a maximum on MTBEFF that can be achieved by addressing a specified fraction of a system's failure intensity via design improvements, and mitigating associated failure modes at a specified level of average fix effectiveness.

Table 4-1. Demonstrated MTBEFF from the IOT&E.

Configuration Item	Operating Hours	EFFs	MTBEFF 80% LCB	MTBEFF Requirement (hours)	MTBEFF Potential
TCN	4,366	29	127	664	452
PoP	2,175	13	128	385	457
SNE	7,797	50	137	529	489
VWP	1,426	6	157	94	561
TR-T	471	5	60	308	213
NOSC	855	7	84	463	298
JGN	390	1	130	308	465
MCN-B	5,962	1	1,991	463	7,111

The growth potential estimates given above are based on addressing 90 percent of the failure intensity observed during the IOT&E, and mitigating associated failure modes with 80 percent fix effectiveness on average. These development goals are very aggressive, and require extraordinary reliability growth efforts to be realized. The results show that the growth potential is lower than the Army's threshold reliability for four of the six configuration items (TCN, SNE, TR-T, and NOSC) that did not meet their requirement. When the growth potential is lower than the requirement, this means that it is not likely threshold MTBEFFs will be achieved via the execution of a test-fix-test process exclusively. An example to illustrate this point for WIN-T Increment 2 is the marginal increase in historical MTBEFF estimates shown in Table 4-3, given that the configuration items have been undergoing a test-fix-test process (as well as government-witness failure mode closure events) since the 2009 LUT.

Similar conclusions follow from Table 4-2 below, which compares the corresponding reliability requirements against the demonstrated reliabilities for each configuration item. The reliability growth potentials are also shown. According to the WIN-T Increment 2 Operational Mode Summary/Mission Profile, each of the items is only required to operate for a portion of a 72-hour mission. The required utilization within the 72-mission is shown in hours for each configuration item (second column of Table 4-2). The demonstrated reliability estimates express the probability that a given configuration item completes its specified utilization within a 72-hour mission, without incurring an essential function failure. For instance, the VWP has a 94 percent chance of operating for 10 hours within the 72-hour mission. The reliability requirement for each of the configuration items is 0.90 (90 percent).

Table 4-2. Demonstrated Reliability from the IOT&E.

Configuration Item	Utilization within a 72-hr Mission (Hours)	Demonstrated Reliability in IOT&E (80% LCB)	Reliability Growth Potential*
TCN	71	0.57	0.85
PoP	41	0.72	0.91
SNE	57	0.66	0.89
VWP	10	0.94	0.98
TR-T	36	0.55	0.84
NOSC	54	0.52	0.83
JGN	36	0.76	0.93
MCN-B	54	0.97	0.99

* The reliability growth potential represents the theoretical upper-limit on reliability that can be achieved based addressing 90 percent of the failure intensity with 80 percent average fix effectiveness.

As shown in Table 4-3, the PoP and SNE demonstrated an improvement in MTBEFF since the 2009 LUT. Although improved, the WIN-T Increment 2 did not achieve sufficient reliability growth to meet threshold requirements for the other configuration items. The TCN,

PoP, and SNE MTBEFF estimates demonstrated during IOT&E are less than a third of the Army's new requirements.

The Army published more optimistic reliability estimates than the DOT&E due to the Army's scoring of "Degraded Essential Function Failures" (DEFFs). The Army defines DEFFs as failures which could leave a piece of equipment mission-capable. For example, consider a PoP with its onboard HNW and NCW network connections. If the HNW radio failed, the PoP could maintain a network connection using NCW. By defining this as a degraded essential function failure, the Army discards this event in the sense that it does not contribute to their MTBEFF estimate. DOT&E factored all failures into the MTBEFF calculation, since WIN-T Increment 2 is designed to provide Soldiers the operational benefits of redundant capabilities, such as HNW and NCW, to function in diverse mission environments. Even with the Army's more optimistic MTBEFF estimates, the Army viewed the MCN-B as the only WIN-T Increment 2 configuration item as meeting its reliability requirement.

Table 4-3. Historical MTBEFF (in hours) Point Estimates.

Configuration Item	2009 LUT	2010 RRE-4	2011 PQT-G MTBEFF	Army IOT&E MTBEFF	DOT&E IOT&E MTBEFF
TCN	176	109	153	291	151
PoP	87	91	322	272	167
SNE	49	103	118	223	156
VWP	226	116	90	24	238
TR-T	N/A	N/A	540	94	94
NOSC	438	N/A	96	214	122
JGN	N/A	N/A	79	N/A	390
MCN-B	N/A	N/A	N/A	5,962	5,962

RRE-4 – Risk Reduction Event 4

PQT-G – Product Qualification Test – Government

Table 4-3 shows the historical MTBEFF as point estimates rather than the 80 percent LCBs given in Tables 4-1 and 4-2. The Army's VWP score is lower than DOT&E's because the Army used only on-the-move operational hours, but considered at-the-halt and on-the-move failures for scoring. This lowered the reliability score for the VWP. DOT&E used all operational hours in its reliability estimate for VWP, and concludes that the VWP met its reliability requirement.

The TCN, PoP, and SNE are all manned platforms. Although the TCN cabins do not have room for reliability data collector personnel, four of the PoPs and eight of the SNEs had data collectors onboard the vehicles. The rest of the PoPs and SNEs were accompanied by data collectors who trailed in different vehicles. The MTBEFF estimates for the PoPs and SNEs with onboard reliability data collectors are lower than the estimates for the other PoPs and SNEs. This is an indication that onboard data collectors can more accurately record test incidents since they are present, and that demonstrated MTBEFFs recorded at the IOT&E may be optimistic.

Figure 4-1 shows that there is a statistically significant difference between the MTBEFF estimates using the two reliability data collection methods.

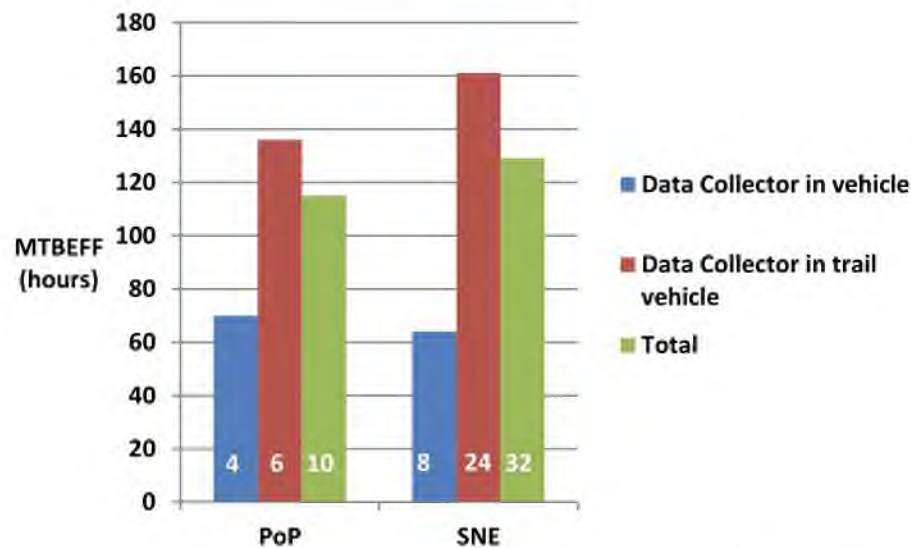


Figure 4-1. Measured MTBEFF Lower Confidence Limits (in Hours) for PoPs and SNEs for Onboard Reliability Data Collectors (Blue), Trail-vehicle Data Collectors (Red) and Total Average (Green). The Numbers on the Bottom of the Bars Represent the Number of Vehicles.

Maintainability

VWP and JGN are maintainable. The other six CIs did not meet their maintainability requirements. Table 4-4 summarizes the MTTR estimates for each of the CIs.

Table 4-4. MTTR Estimates from IOT&E.

Configuration Item	MTTR Point Estimate (minutes)	MTTR Requirement (minutes)
TCN	72	60
PoP	67	30
SNE	83	30
VWP	7	30
TR-T	126	30
NOSC	104	60
JGN	25	30
MCN-B	48	30

For most WIN-T Increment 2 repairs, the time spent waiting for a repair during the IOT&E was greater than 70 percent of the total down time. Table 4-5 compares the Average Logistics Delay Time (ALDT, i.e., the time spent waiting for repair parts) to the total down time,

which includes both ALDT and the repair time (i.e., MTTR). Although the Army has no specified requirements for ALDT, reducing logistics delays would reduce WIN-T Increment 2 down times.

Table 4-5. Down Time during the IOT&E.

Configuration Item	Operating Hours	Total Down Time (hours)	ALDT	% of Down Time Waiting for Repair (ALDT/Total Down Time)
TCN	4366	332	266	80%
PoP	2175	105	88	84%
SNE	7797	1265	1177	93%
VWP	1659	573	560	98%
TR-T	471	38	27	71%
NOSC	855	16	2	13%
JGN	486	2	0	0%
MCN-B	5962	25	24	96%

Power

The operational suitability of the WIN-T Increment 2 is dependent on reliable power sources for the WIN-T Increment 2 configuration items. The PoPs, SNEs, and VWPs do not have onboard power generation capability, and they rely upon the supporting vehicles' engines to supply power at-the-halt. During the IOT&E, Soldiers operated the supporting vehicles to provide power for their communications equipment. The Soldier's constant at-the-halt operation of vehicles to support WIN-T Increment 2 caused increased noise, fuel consumption, and wear and tear on the vehicle engines.

Training and Manpower Support

WIN-T Increment 2 New Equipment Training (NET) enabled brigade Soldiers to successfully plan and implement changes to the network driven by operationally realistic tactical scenarios (e.g., command post relocations and force movements). Trained brigade signal Soldiers installed, operated, and conducted maintenance of the WIN-T Increment 2 configuration items. Combat arms Soldiers (i.e., the primary operators for the PoP, SNE, and VWP) were able to execute startup and shutdown procedures. They had little capability to maintain WIN-T Increment 2 configuration items other than restarting the system following a failure.

The Army's NIE 12.2 tested and evaluated numerous communications systems other than the WIN-T Increment 2 configuration items. To address this complexity, the Army used the Brigade Modernization Command and contractors to conduct network planning, as well as to configure WIN-T Increment 2 configuration items. As the brigade had limited input, the IOT&E did not provide a complete assessment of the Increment 2 network planning tools and training to install an initial WIN-T Increment 2 network. Division and brigade network managers

demonstrated their ability to plan and execute network reconfigurations during the numerous movements of tactical command posts during the IOT&E.

WIN-T Increment 2 NET needs to improve the training provided on Combat Net Radio (CNR) Gateway operations, Information Assurance, computer network operations, and management of the Highband Networking Waveform (HNW). CNR Gateway training did not cover the basic requirements needed to employ the gateway. The brigade signal staff was able to employ the CNR Gateway late in the IOT&E but the capability was not demonstrated at the battalion or company level. Training improvements in Information Assurance, network operations, and HNW management would improve shortfalls described in the effectiveness and survivability sections of this report.

Environmental Performance

Environmental performance of most WIN-T Increment 2 CIs met specifications as demonstrated in the IOT&E, as well as previous production qualification testing. The TR-T was an exception. During the IOT&E, the TR-T demonstrated low reliability in rain because of a poor electronics container design. Table 4-6 presents the Army's environmental testing results published in the Production Qualification Test – Government (PQT-G) report. Blank fields indicate the developmental tests were not completed before entering operational test. Poor developmental test results, highlighted in red, indicate areas of concern in high temperature and solar radiation, humidity, and road shock and vibration. The Army should pursue corrective actions to these environmental performance considerations.

Table 4-6. Performance of some of the WIN-T Increment 2 CIs during Environmental Testing at the PQT-G.

Test	NOSC-B	NOSC-D	SNE	TCN	TR-T
Blowing Rain				M	M
Blowing Sand and Dust			M	M	M
Fording					M
High Temperature and Solar Radiation		P	M	M	N
Humidity		P		N	N
Low Temperature		M	M	M	M
Orientation				P	
Physical Characteristics		N	M	M	M
Rail Impact		M	M	M	M
Road Shock and Vibration		P	P	P	P
Roll Stability				NA	
Safety	M	M	M	P	M

Notes:

M= Met

P = Partially Met

N = Not Met

NA = Not Assessed

Transportability

The WIN-T Increment 2 TCN and NOSC configuration items are mounted on Family of Medium Tactical Vehicles (FMTV) platforms. The PoPs, SNEs, and VWP for Increment 2 are mounted in Mine Resistant Ambush Protected (MRAP) vehicles. During the IOT&E, the PoPs and the SNEs could not keep up with the advance of the armored formation, especially when moving across open terrain. MRAPs and FMTVs are not capable of being transported by Army rotary-wing aircraft. The size, weight, and mobility of WIN-T Increment 2 limit its ability to support a full range of mission scenarios.

MANPRINT

Table 4-7 highlights the Army's Manpower, Personnel, and Training (MANPRINT) assessment, which identifies four major Human Factors Engineering (HFE) issues, two safety concerns, and one personnel issue. In addition to these, the IOT&E highlighted:

- Safety hazard associated with TR-T mast extension that can cause the system to fail and bind in the up position.
- Soldiers were exposed to a radio frequency hazard from vehicle rooftop antennas supporting PoPs and SNEs.

Table 4-7. Summary of the MANPRINT Independent Assessment for WIN-T Increment 2.

Issue	MANPRINT Domain	Issue Risk Level
Contractor Filed Service Representatives are required to provide assistance in planning, routing, configuration management, information assurance (IA), and troubleshooting procedures due to the system's complexity.	Personnel	Major
Network Operations software is excessively complex.	HFE	Major
General Purpose User tasks in the Point of Presence (PoP), Soldier Network Extension (SNE), and the Vehicle Wireless Package (VWP) are excessively complex.	HFE	Major
Viewing the MDA display in the Tactical Communications Node is difficult	HFE	Major
The MDA processing speed is slow when multiple applications are running.	HFE	Major
Loss of situational awareness at the Division, Brigade, and Battalion as a result of information assurance/computer network operations threats including physical and electronic warfare threats.	HFE	Major
Noise. Acoustic Energy: Steady-state noise hazards are present in the Network Operations and Security Center Shelter and the Tactical Communications Node Shelter when generators or environmental control units are operating.	Health Hazard System Safety	High Risk Critical severity improbable Occurrence
Potential radio frequency radiation (RFR) hazard for the following components: 2.4 meter Lightweight antenna, Highband Network Radio, SATCOM on-the-move (OTM) RFR Systems and SATCOM Low cost Antenna OTM RFR Systems.	Health Hazard System Safety	Medium Risk

Section Five Survivability

The Warfighter Information Network – Tactical (WIN-T) Increment 2 is not survivable. WIN-T Increment 2 had significant Information Assurance vulnerabilities during Initial Operational Test and Evaluation (IOT&E) that would interfere with a unit's combat mission.

The Army Research Laboratory, Survivability/Lethality Analysis Directorate (ARL/SLAD) and the Army's Threat Systems Management Office (TSMO) conducted threat computer network operations and Information Assurance scans of the WIN-T Increment 2 network. The TSMO conducted open-air electronic warfare and testing against the WIN-T Increment 2. The results of these tests are discussed in a classified annex to this report.

The Army conducted threat computer network operations and Information Assurance testing in accordance with the DOT&E memorandum "Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs," dated January 21, 2009.

Threat Computer Network Operations (TCNO)

Two teams from the Information Assurance and Computer Network Defense branch of the ARL/SLAD performed the step 4 "blue team" evaluation of WIN-T Increment 2. The teams conducted vulnerability scans of the WIN-T Increment 2 configuration items, and reviewed Information Assurance system documentation. ARL/SLAD and TSMO conducted the step 5, "red team" threat computer network operations during the WIN-T Increment 2 IOT&E.

Electronic Warfare (EW)

TSMO conducted open-air, electronic jamming during the WIN-T Increment 2 IOT&E. Due to radio frequency limitations, the jamming for Net-Centric Waveform and Highband Networking Waveform was not representative of a capable and determined adversary.

Chemical, Biological, Radiological (CBR)

The Army's Chemical Test Division performed an analysis of the survivability of the WIN-T Increment 2 configuration items to CBR agents. The analysis consisted of a physical inspection of the Increment 2 Tactical Communications Node, Network Operations and Security Center – Division (NOSC-D), and NOSC-Brigade (NOSC-B) mounted on the Family of Medium Tactical Vehicles, the Point of Presence (PoP) and Soldier Network Extension (SNE) mounted on the High Mobility Multipurpose Wheeled Vehicle, the Tactical Relay – Tower, and the Satellite Tactical Terminal+, along with a review of documentation describing the materials and their construction. The assessment did not include Increment 2 PoPs and SNEs mounted in Mine Resistant Ambush Protected Vehicles.

The WIN-T Increment 2 is not expected to meet its decontamination criterion. The system has too many components made of rubber and soft plastic that will absorb and desorb chemical warfare agents. The system has many crevices in which agents will collect or pool and be shielded from decontaminants.

The WIN-T Increment 2 is expected to meet its hardness criterion. The system has components that are made of rubber and soft plastic materials (cables, wiring, and buttons) that may become brittle or weakened after multiple contamination/decontamination (CD) cycles. A single CD cycle should not impact functionality. The configuration items are expected to be compatible with Mission-Oriented Protective Posture (MOPP) 4 equipment, and operation in MOPP 4 is not expected to significantly degrade performance.

Section Six Recommendations

The Army should consider the following actions to improve the Warfighter Information Network – Tactical (WIN-T) Increment 2:

- **Improve Reliability.** The Army should dedicate resources to fix WIN-T Increment 2's demonstrated reliability and improve the network's ability support the probability of completing a 72-hour mission. Reliability improvements should be demonstrated during a future operational test event.
 - Consider appointing an independent reliability, availability, and maintainability (RAM) review panel to complete a reliability growth strategy that includes test-fix-test activities and where not capable of meeting reliability goals, recommend configurations for materiel redesign.
 - Perform a lifecycle cost analysis of the demonstrated Initial Operational Test and Evaluation (IOT&E) Mean Time Between Essential Function Failure values and determine the additional costs for maintenance support of the WIN-T Increment 2 due to poor reliability.
- **Soldier Network Extension (SNE).** The Army should identify the root causes of and correct the poor performance of the SNE and demonstrate its effectiveness in a future operational test event.
- **Improve WIN-T Increment 2 Waveforms.** The Army should conduct further testing, assessment and improvement of Highband Networking Waveform (HNW) and Net-Centric Waveform (NCW) to address deficiencies noted during the IOT&E. Waveform improvements should be demonstrated during a future operational test event.
 - Improve HNW transmission range. The HNW waveform has limited range in vegetation, urban, or complex terrain. The Army should consider solutions for increasing the HNW transmission range, such as using multiple frequency bands and/or increasing radio transmission power.
 - Improve HNW stability. As supported mobile platforms moved, the HNW network demonstrated instability that included bandwidth reductions, cycling issues with NCW and disruption of adjacent HNW node services. The Army should assess the cause of poor HNW network stability and correct these deficiencies.
 - Improve NCW stability (route drop). The Army should identify the root causes of and correct the NCW dropped routes demonstrated during IOT&E.
- **Tactical Relay – Tower (TR-T).** The single TR-T supporting the HNW network was not able to support the brigade's dispersion during offensive operations. In

addition to fixing the TR-T material deficiencies, the Army should assess the fielding quantities of TR-Ts to support brigade operations.

- **Survivability.** The Army should address the deficiencies and recommendations listed in the classified annex and the Army Research Laboratory, Survivability/Lethality Analysis Directorate report.
- **Electronic Warfare.** The Army should assess NCW and HNW under an operationally realistic electronic warfare threat during a future operational test event.
- **Network Management.** The Army should improve network management tools:
 - Improve the ability to manage the HNW network.
 - At the brigade Tactical Command Post, battalion, and Tactical Communications Node, provide the option to display the entire brigade network and train soldiers to assume network management in the absence of the brigade Tactical Operations Center.
 - Provide the ability to display status information for mission command applications and communications systems operating within the unit's area of responsibility.
- **Mission Command Applications.** The Army should create, and implement operationally, a mission command applications architecture that is based upon mission requirements (both on-the-move and at-the-halt) by echelon that is supportable by the WIN-T Increment 2 network.
- **Training.** The Army should improve WIN-T Increment 2 training to include operation of the Combat Net Radio Gateway, increased maintenance for operators, and basic network fundamentals for battalion and company network managers.
- **Mobility.** The Army should assess WIN-T Increment 2 mobility against its full range of potential missions and demonstrate combat vehicle integration in future operational test events.
- **Power.** The Army should provide independent power sources for WIN-T Increment 2 configuration items to prevent continuous operation of vehicle power.
- **Configuration Item Basis of Issue Plan.** The Army should reassess the distribution of Vehicle Wireless Package and SNE configuration items to support unit at-the-halt and on-the-move operations.



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

SEP 26 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:


(U) I have enclosed at TAB A the Operational Test and Evaluation Report on the Warfighter Information Network – Tactical (WIN-T) Increment 2, required by Sections 2399 of Title 10 United States Code. Enclosed at TAB B is the classified annex to this report, which discusses my evaluation of the network's survivability.

(U) WIN-T Increment 2 builds upon the WIN-T Increment 1 at-the-halt network to support on-the-move operations. The fundamental new capabilities provided in Increment 2 are the ability to use Voice over Internet Protocol (VoIP) communications and battle command software applications on-the-move. The WIN-T Increment 2 system contains multiple items of equipment and communications technologies, each of which performed at different levels of effectiveness during Initial Operational Test and Evaluation (IOT&E).

(U) In my report, I conclude the following WIN-T Increment 2 equipment and technologies are operationally effective:

- (U) Tactical Communications Node (TCN), a large "mobile cell phone tower" to provide communication and networking for all echelons.
- (U) Point of Presence (PoP), a smaller vehicle to provide a connection to the network for commanders at all echelons.
- (U) The Net-Centric Waveform (NCW) for ground-to-satellite communications. The Tactical Communications Node (TCN), Point of Presence (PoP), and Soldier Network Extension (SNE) vehicles use the NCW.
- (U) Colorless Core Security Architecture, to support multiple security levels and improve network efficiency.
- (U) Satellite Tactical Terminal+ (STT+), a trailer-mounted satellite terminal which provides greater satellite bandwidth to the TCN at-the-halt.
- (U) Network Operations and Security Center (NOSC), to support network management.
- (U) Vehicle Wireless Package (VWP), to provide a short-range wireless connection to TCNs on-the-move and at-the-halt.



- 
- (U) Modular Communications Node – Basic (MCN-B), a tactical fiber linked communications package that provides Non-secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) access up to 1 kilometer away from the TCN.
 - (U) Joint Gateway Node (JGN), to connect to Joint, strategic, allied, coalition, and commercial networks at large command centers.

(U) The following configuration items and technologies are not operationally effective:

- (U) Soldier Network Extension (SNE), to provide a network connection to company commanders.
- (U) Highband Networking Waveform (HNW), to provide terrestrial network connectivity to TCN and PoP vehicles to reduce demand on NCW satellite resources.
- (U) Tactical Relay – Tower (TR-T), a 30-meter mast to extend the range of the HNW line of sight communications network.

(U) WIN-T Increment 2 relies upon the TCN, PoP, and SNE to provide the Army's "initial on-the-move" network. The TCN and PoP met the unit's mission requirements for throughput and performance. The SNE did not meet the unit's mission requirements. SNE users experienced low VoIP success rates, delays when communicating, low file transfer rates, and poor quality of service. The SNE battle command applications were not useful to Soldiers due to insufficient SNE bandwidth.

(U) Given sufficient satellite bandwidth, the NCW supported unit operations both at-the-halt and on-the-move. The NCW consistently provided a large number of network connections, although unexpected drops of NCW routes between Increment 2 configuration items occurred. There is the potential for interrupted service for VoIP, chat, and mission command applications when NCW routes are dropped. The operational impact of dropped NCW routes was not evident during the IOT&E. However, if not corrected, dropped NCW routes could become a problem as the Army increases the size of the WIN-T network and uses more real-time applications that require higher bandwidth among numerous users.

(U) The terrestrial HNW line-of-sight network demonstrated poor transmission range in vegetation, rolling hills, and urban terrain. Because terrain and vegetation interfered with the HNW's line-of-sight, the number of HNW connections maintained by TCN and PoP vehicles dropped when the vehicles were on-the-move. While attempting to restore the dropped HNW connections, the WIN-T Increment 2 network cycled between NCW satellite communications and line-of-sight HNW, disrupting network connections across the HNW network. Network management during the IOT&E reduced the occurrence of network disruptions but also reduced network performance. If not corrected, the impact of HNW and NCW cycling will increase as the Army increases the size of the WIN-T Increment 2 network.

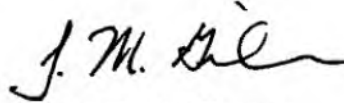
(U) Overall, WIN-T Increment 2 is not operationally suitable. None of the on-the-move platforms (i.e., TCN, PoP, or SNE) met their reliability or maintainability requirements. There were twice the number of Field Service Representatives (FSRs) performing maintenance during

[REDACTED]

the IOT&E relative to the Army's support plan, and repair times for half of the configuration items were observed to take two to four times longer than required. Four of six of the items (the TCN, SNE, TR-T and NOSC) that did not meet reliability requirements have a reliability growth potential that is lower than the Army's new, lower threshold reliability requirements. This means that it is unlikely these items of equipment will achieve their reliability requirements.

(U) WIN-T Increment 2 is not survivable; it has significant Information Assurance vulnerabilities that would degrade a unit's ability to succeed in combat. These vulnerabilities are discussed in the attached classified annex to the report.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; and the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.



J. Michael Gilmore
Director

Enclosures: As stated

cc: The Honorable Adam Smith
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

SEP 26 2012

The Honorable C. W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015


Dear Mr. Chairman:

(U) I have enclosed at TAB A the Operational Test and Evaluation Report on the Warfighter Information Network – Tactical (WIN-T) Increment 2, required by Sections 2399 of Title 10 United States Code. Enclosed at TAB B is the classified annex to this report, which discusses my evaluation of the network's survivability.

(U) WIN-T Increment 2 builds upon the WIN-T Increment 1 at-the-halt network to support on-the-move operations. The fundamental new capabilities provided in Increment 2 are the ability to use Voice over Internet Protocol (VoIP) communications and battle command software applications on-the-move. The WIN-T Increment 2 system contains multiple items of equipment and communications technologies, each of which performed at different levels of effectiveness during Initial Operational Test and Evaluation (IOT&E).

(U) In my report, I conclude the following WIN-T Increment 2 equipment and technologies are operationally effective:

- (U) Tactical Communications Node (TCN), a large "mobile cell phone tower" to provide communication and networking for all echelons.
- (U) Point of Presence (PoP), a smaller vehicle to provide a connection to the network for commanders at all echelons.
- (U) The Net-Centric Waveform (NCW) for ground-to-satellite communications. The Tactical Communications Node (TCN), Point of Presence (PoP), and Soldier Network Extension (SNE) vehicles use the NCW.
- (U) Colorless Core Security Architecture, to support multiple security levels and improve network efficiency.
- (U) Satellite Tactical Terminal+ (STT+), a trailer-mounted satellite terminal which provides greater satellite bandwidth to the TCN at-the-halt.
- (U) Network Operations and Security Center (NOSC), to support network management.
- (U) Vehicle Wireless Package (VWP), to provide a short-range wireless connection to TCNs on-the-move and at-the-halt.

- 
- (U) Modular Communications Node – Basic (MCN-B), a tactical fiber linked communications package that provides Non-secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) access up to 1 kilometer away from the TCN.
 - (U) Joint Gateway Node (JGN), to connect to Joint, strategic, allied, coalition, and commercial networks at large command centers.

(U) The following configuration items and technologies are not operationally effective:

- (U) Soldier Network Extension (SNE), to provide a network connection to company commanders.
- (U) Highband Networking Waveform (HNW), to provide terrestrial network connectivity to TCN and PoP vehicles to reduce demand on NCW satellite resources.
- (U) Tactical Relay – Tower (TR-T), a 30-meter mast to extend the range of the HNW line of sight communications network.

(U) WIN-T Increment 2 relies upon the TCN, PoP, and SNE to provide the Army's "initial on-the-move" network. The TCN and PoP met the unit's mission requirements for throughput and performance. The SNE did not meet the unit's mission requirements. SNE users experienced low VoIP success rates, delays when communicating, low file transfer rates, and poor quality of service. The SNE battle command applications were not useful to Soldiers due to insufficient SNE bandwidth.

(U) Given sufficient satellite bandwidth, the NCW supported unit operations both at-the-halt and on-the-move. The NCW consistently provided a large number of network connections, although unexpected drops of NCW routes between Increment 2 configuration items occurred. There is the potential for interrupted service for VoIP, chat, and mission command applications when NCW routes are dropped. The operational impact of dropped NCW routes was not evident during the IOT&E. However, if not corrected, dropped NCW routes could become a problem as the Army increases the size of the WIN-T network and uses more real-time applications that require higher bandwidth among numerous users.

(U) The terrestrial HNW line-of-sight network demonstrated poor transmission range in vegetation, rolling hills, and urban terrain. Because terrain and vegetation interfered with the HNW's line-of-sight, the number of HNW connections maintained by TCN and PoP vehicles dropped when the vehicles were on-the-move. While attempting to restore the dropped HNW connections, the WIN-T Increment 2 network cycled between NCW satellite communications and line-of-sight HNW, disrupting network connections across the HNW network. Network management during the IOT&E reduced the occurrence of network disruptions but also reduced network performance. If not corrected, the impact of HNW and NCW cycling will increase as the Army increases the size of the WIN-T Increment 2 network.

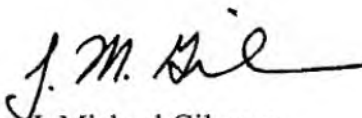
(U) Overall, WIN-T Increment 2 is not operationally suitable. None of the on-the-move platforms (i.e., TCN, PoP, or SNE) met their reliability or maintainability requirements. There were twice the number of Field Service Representatives (FSRs) performing maintenance during

[REDACTED]

the IOT&E relative to the Army's support plan, and repair times for half of the configuration items were observed to take two to four times longer than required. Four of six of the items (the TCN, SNE, TR-T and NOSC) that did not meet reliability requirements have a reliability growth potential that is lower than the Army's new, lower threshold reliability requirements. This means that it is unlikely these items of equipment will achieve their reliability requirements.

(U) WIN-T Increment 2 is not survivable; it has significant Information Assurance vulnerabilities that would degrade a unit's ability to succeed in combat. These vulnerabilities are discussed in the attached classified annex to the report.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; and the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosures:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

SEP 26 2012

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050


Dear Mr. Chairman:

(U) I have enclosed at TAB A the Operational Test and Evaluation Report on the Warfighter Information Network – Tactical (WIN-T) Increment 2, required by Sections 2399 of Title 10 United States Code. Enclosed at TAB B is the classified annex to this report, which discusses my evaluation of the network's survivability.

(U) WIN-T Increment 2 builds upon the WIN-T Increment 1 at-the-halt network to support on-the-move operations. The fundamental new capabilities provided in Increment 2 are the ability to use Voice over Internet Protocol (VoIP) communications and battle command software applications on-the-move. The WIN-T Increment 2 system contains multiple items of equipment and communications technologies, each of which performed at different levels of effectiveness during Initial Operational Test and Evaluation (IOT&E).

(U) In my report, I conclude the following WIN-T Increment 2 equipment and technologies are operationally effective:

- (U) Tactical Communications Node (TCN), a large "mobile cell phone tower" to provide communication and networking for all echelons.
- (U) Point of Presence (PoP), a smaller vehicle to provide a connection to the network for commanders at all echelons.
- (U) The Net-Centric Waveform (NCW) for ground-to-satellite communications. The Tactical Communications Node (TCN), Point of Presence (PoP), and Soldier Network Extension (SNE) vehicles use the NCW.
- (U) Colorless Core Security Architecture, to support multiple security levels and improve network efficiency.
- (U) Satellite Tactical Terminal+ (STT+), a trailer-mounted satellite terminal which provides greater satellite bandwidth to the TCN at-the-halt.
- (U) Network Operations and Security Center (NOSC), to support network management.
- (U) Vehicle Wireless Package (VWP), to provide a short-range wireless connection to TCNs on-the-move and at-the-halt.

- 
- (U) Modular Communications Node – Basic (MCN-B), a tactical fiber linked communications package that provides Non-secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) access up to 1 kilometer away from the TCN.
 - (U) Joint Gateway Node (JGN), to connect to Joint, strategic, allied, coalition, and commercial networks at large command centers.

(U) The following configuration items and technologies are not operationally effective:

- (U) Soldier Network Extension (SNE), to provide a network connection to company commanders.
- (U) Highband Networking Waveform (HNW), to provide terrestrial network connectivity to TCN and PoP vehicles to reduce demand on NCW satellite resources.
- (U) Tactical Relay – Tower (TR-T), a 30-meter mast to extend the range of the HNW line of sight communications network.

(U) WIN-T Increment 2 relies upon the TCN, PoP, and SNE to provide the Army's "initial on-the-move" network. The TCN and PoP met the unit's mission requirements for throughput and performance. The SNE did not meet the unit's mission requirements. SNE users experienced low VoIP success rates, delays when communicating, low file transfer rates, and poor quality of service. The SNE battle command applications were not useful to Soldiers due to insufficient SNE bandwidth.

(U) Given sufficient satellite bandwidth, the NCW supported unit operations both at-the-halt and on-the-move. The NCW consistently provided a large number of network connections, although unexpected drops of NCW routes between Increment 2 configuration items occurred. There is the potential for interrupted service for VoIP, chat, and mission command applications when NCW routes are dropped. The operational impact of dropped NCW routes was not evident during the IOT&E. However, if not corrected, dropped NCW routes could become a problem as the Army increases the size of the WIN-T network and uses more real-time applications that require higher bandwidth among numerous users.

(U) The terrestrial HNW line-of-sight network demonstrated poor transmission range in vegetation, rolling hills, and urban terrain. Because terrain and vegetation interfered with the HNW's line-of-sight, the number of HNW connections maintained by TCN and PoP vehicles dropped when the vehicles were on-the-move. While attempting to restore the dropped HNW connections, the WIN-T Increment 2 network cycled between NCW satellite communications and line-of-sight HNW, disrupting network connections across the HNW network. Network management during the IOT&E reduced the occurrence of network disruptions but also reduced network performance. If not corrected, the impact of HNW and NCW cycling will increase as the Army increases the size of the WIN-T Increment 2 network.

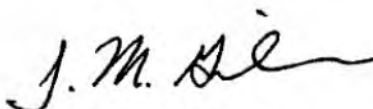
(U) Overall, WIN-T Increment 2 is not operationally suitable. None of the on-the-move platforms (i.e., TCN, PoP, or SNE) met their reliability or maintainability requirements. There were twice the number of Field Service Representatives (FSRs) performing maintenance during

[REDACTED]

the IOT&E relative to the Army's support plan, and repair times for half of the configuration items were observed to take two to four times longer than required. Four of six of the items (the TCN, SNE, TR-T and NOSC) that did not meet reliability requirements have a reliability growth potential that is lower than the Army's new, lower threshold reliability requirements. This means that it is unlikely these items of equipment will achieve their reliability requirements.

(U) WIN-T Increment 2 is not survivable; it has significant Information Assurance vulnerabilities that would degrade a unit's ability to succeed in combat. These vulnerabilities are discussed in the attached classified annex to the report.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; and the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.



J. Michael Gilmore
Director

Enclosures:
As stated

cc:
The Honorable John McCain
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

SEP 26 2012

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510


Dear Mr. Chairman:

(U) I have enclosed at TAB A the Operational Test and Evaluation Report on the Warfighter Information Network – Tactical (WIN-T) Increment 2, required by Sections 2399 of Title 10 United States Code. Enclosed at TAB B is the classified annex to this report, which discusses my evaluation of the network's survivability.

(U) WIN-T Increment 2 builds upon the WIN-T Increment 1 at-the-halt network to support on-the-move operations. The fundamental new capabilities provided in Increment 2 are the ability to use Voice over Internet Protocol (VoIP) communications and battle command software applications on-the-move. The WIN-T Increment 2 system contains multiple items of equipment and communications technologies, each of which performed at different levels of effectiveness during Initial Operational Test and Evaluation (IOT&E).

(U) In my report, I conclude the following WIN-T Increment 2 equipment and technologies are operationally effective:

- (U) Tactical Communications Node (TCN), a large "mobile cell phone tower" to provide communication and networking for all echelons.
- (U) Point of Presence (PoP), a smaller vehicle to provide a connection to the network for commanders at all echelons.
- (U) The Net-Centric Waveform (NCW) for ground-to-satellite communications. The Tactical Communications Node (TCN), Point of Presence (PoP), and Soldier Network Extension (SNE) vehicles use the NCW.
- (U) Colorless Core Security Architecture, to support multiple security levels and improve network efficiency.
- (U) Satellite Tactical Terminal+ (STT+), a trailer-mounted satellite terminal which provides greater satellite bandwidth to the TCN at-the-halt.
- (U) Network Operations and Security Center (NOSC), to support network management.
- (U) Vehicle Wireless Package (VWP), to provide a short-range wireless connection to TCNs on-the-move and at-the-halt.

- 
- (U) Modular Communications Node – Basic (MCN-B), a tactical fiber linked communications package that provides Non-secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) access up to 1 kilometer away from the TCN.
 - (U) Joint Gateway Node (JGN), to connect to Joint, strategic, allied, coalition, and commercial networks at large command centers.

(U) The following configuration items and technologies are not operationally effective:

- (U) Soldier Network Extension (SNE), to provide a network connection to company commanders.
- (U) Highband Networking Waveform (HNW), to provide terrestrial network connectivity to TCN and PoP vehicles to reduce demand on NCW satellite resources.
- (U) Tactical Relay – Tower (TR-T), a 30-meter mast to extend the range of the HNW line of sight communications network.

(U) WIN-T Increment 2 relies upon the TCN, PoP, and SNE to provide the Army's "initial on-the-move" network. The TCN and PoP met the unit's mission requirements for throughput and performance. The SNE did not meet the unit's mission requirements. SNE users experienced low VoIP success rates, delays when communicating, low file transfer rates, and poor quality of service. The SNE battle command applications were not useful to Soldiers due to insufficient SNE bandwidth.

(U) Given sufficient satellite bandwidth, the NCW supported unit operations both at-the-halt and on-the-move. The NCW consistently provided a large number of network connections, although unexpected drops of NCW routes between Increment 2 configuration items occurred. There is the potential for interrupted service for VoIP, chat, and mission command applications when NCW routes are dropped. The operational impact of dropped NCW routes was not evident during the IOT&E. However, if not corrected, dropped NCW routes could become a problem as the Army increases the size of the WIN-T network and uses more real-time applications that require higher bandwidth among numerous users.

(U) The terrestrial HNW line-of-sight network demonstrated poor transmission range in vegetation, rolling hills, and urban terrain. Because terrain and vegetation interfered with the HNW's line-of-sight, the number of HNW connections maintained by TCN and PoP vehicles dropped when the vehicles were on-the-move. While attempting to restore the dropped HNW connections, the WIN-T Increment 2 network cycled between NCW satellite communications and line-of-sight HNW, disrupting network connections across the HNW network. Network management during the IOT&E reduced the occurrence of network disruptions but also reduced network performance. If not corrected, the impact of HNW and NCW cycling will increase as the Army increases the size of the WIN-T Increment 2 network.

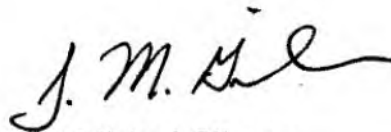
(U) Overall, WIN-T Increment 2 is not operationally suitable. None of the on-the-move platforms (i.e., TCN, PoP, or SNE) met their reliability or maintainability requirements. There were twice the number of Field Service Representatives (FSRs) performing maintenance during

[REDACTED]

the IOT&E relative to the Army's support plan, and repair times for half of the configuration items were observed to take two to four times longer than required. Four of six of the items (the TCN, SNE, TR-T and NOSC) that did not meet reliability requirements have a reliability growth potential that is lower than the Army's new, lower threshold reliability requirements. This means that it is unlikely these items of equipment will achieve their reliability requirements.

(U) WIN-T Increment 2 is not survivable; it has significant Information Assurance vulnerabilities that would degrade a unit's ability to succeed in combat. These vulnerabilities are discussed in the attached classified annex to the report.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; and the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.



J. Michael Gilmore
Director

Enclosures:
As stated

cc:
The Honorable Thad Cochran
Ranking Member

AH-64D Apache Block III (AB3) Attack Helicopter

Combined Initial Operational Test and Evaluation and Live Fire Test and Evaluation Report



August 2012

This report on the AH-64D Apache Block III (AB3) Attack Helicopter fulfills the provisions of Title 10, United States Code, Sections 2399 and 2366. It assesses the adequacy of testing and the operational effectiveness, operational suitability, and survivability of the AB3.


J. Michael Gilmore
Director

The marginal cost of producing this report is estimated to be approximately \$52.5K. The estimated acquisition cost of the program which this report addresses is \$36B.

Improved Drive System:

New Transmission Design
Increase Power
Increase Performance

AB3 Avionics:

Expand Communication Options
Add Instrument Flight Capability
Eliminate Obsolescence
Expand Processing Capability

**Improved Helmet and
Display Sight System:**

Avoid Obsolescence

UAS Interoperability:

Receive UAS Video
Control UAS Sensors
Reposition UAS Air Vehicle

Radar Electronics Unit:

Enhance Radar Processing Capacity
Replace Obsolescent Components



New Capabilities of Lot 1 Apache Block III

Executive Summary

This is my evaluation on the test adequacy, operational effectiveness, operational suitability, and survivability of the Lot 1 increment of the Army's AH-64D Apache Block III (AB3) attack helicopter. This evaluation is based on data from an Initial Operational Test and Evaluation (IOT&E) conducted in March and April 2012 in which teams of two AB3 helicopters and teams of two legacy Apache Block II (hereinafter referred to in this report only as AB2) helicopters conducted force-on-force attack and reconnaissance missions, Live Fire Test and Evaluation (LFT&E), and augmented by developmental testing conducted from June 2009 through July 2012.

The AB3 is operationally effective. AB3 has improved flight performance compared to legacy Apache aircraft. And, when aided by real-time unmanned aircraft system (UAS) video containing actionable intelligence, AB3 teams demonstrated greater target acquisition ranges, greater Hellfire engagement ranges, and the potential for greater mission success than AB2 teams. The AB3 is operationally suitable. AB3 exceeded reliability thresholds with statistical confidence and met all current maintainability requirements. The AB3 is at least as survivable as the AB2. AB3 retains the infrared countermeasure effectiveness and ballistic protection of legacy Apache aircraft.

Mission

Attack Reconnaissance units equipped with AB3 helicopters conduct reconnaissance, security, and attack missions in support of ground combat forces. AB3 helicopters are employed in units of two or more aircraft to conduct reconnaissance to locate and report enemy forces and limit or prevent enemy activity. AB3 units conduct security operations by employing weapons to further locate and restrict enemy action, thereby providing reaction time, maneuver space, and protection for air or ground maneuver forces. AB3 units employ their own guns, rockets, and missiles in coordination with friendly ground forces and unmanned aircraft systems to attack and destroy the enemy.

System Description

The legacy AB2 is a four-bladed, twin-engine attack helicopter with tandem cockpit for a crew of two. The Longbow Apache entered production in 1995 and features a nose-mounted sensor suite for day/night target acquisition and an optional mast-mounted Fire Control Radar for target acquisition in dust, fog, or smoke. The AH-64D is armed with a 30 mm chain gun and carries a mixture of Hellfire missiles and 2.75-inch rockets. Legacy Apache aircraft also feature double- and triple-redundant aircraft systems and armor shielding to improve survivability for the aircraft and crew.

AB3 will modernize the existing Apache fleet of 690 aircraft and add capabilities. The AB3 improved drive system will accommodate the added weight of new capabilities and enable safe operations in mountains, as in Afghanistan or Korea, with an operational load of ammunition and fuel. Modernized AB3 avionics will retain all existing functionality, remove

obsolete components, and improve communications and computing capabilities. AB3 can be employed in three configurations: “slick” (no mast-mounted radar/antenna), with an optional mast-mounted Fire Control Radar, or with a data link antenna in the mast-mounted dome that enables interoperability with unmanned aircraft systems. All three AB3 configurations are illustrated in Figure 1.



Figure 1. AB3 Configurations: Slick, with Data Link Antenna, and with Fire Control Radar

Test Adequacy

Operational and live fire testing were adequate to determine the effectiveness, suitability, and survivability of the AB3 aircraft in anticipated combat environments. The IOT&E was preceded by four years of developmental testing that included analysis, modeling and simulation, component qualification testing, testing in environmental extremes, system-level flight testing, weapons qualification, and live fire testing. At the conclusion of developmental flight testing, the Army’s airworthiness authority certified that the AB3 was safe for operational testing by typical combat pilots. All testing was completed as described in the Test and Evaluation Master Plan approved by DOT&E on August 11, 2010.

Operational Effectiveness

The AB3 is operationally effective. AB3 has improved flight performance compared to legacy Apache aircraft. AB3 hover performance exceeds that of legacy aircraft by 35 percent and enables AB3 units to operate at higher altitudes and temperatures with larger payloads. An AB3 with new specification engines meets the hover performance Key Performance Parameter in that the aircraft can hover out of ground effect (OGE) at 6,000 feet pressure altitude at 95 degrees Fahrenheit with 3,400 pounds of payload.

During testing, there was no significant difference (in the statistical sense) in overall mission success between the AB3 and the AB2. In fact, missions conducted with UAS support were less successful than those conducted without UAS support. In particular, when teamed with a Gray Eagle UAS providing no actionable combat information, AB3 crews were not successful. Nonetheless, test data indicate the ability of the AB3 to team with a UAS has the potential to enhance AB3 effectiveness relative to AB2. When aided by real-time unmanned aircraft system (UAS) video containing actionable intelligence, AB3 teams demonstrated greater Hellfire engagement ranges than AB2 teams.

On four AB3 and two AB2 missions, the UAS had no actionable information when Apache crews arrived on station. Rather than ignore the UAS as the AB2 crews did, the AB3 crews continued to monitor the UAS video or took control of the UAS sensor in an attempt to find threat targets. Post-test surveys showed that UAS video is distracting to AB3 crews when the data link fails or the video contains no useful information. These results should inform the development of tactics, techniques, and procedures for AB3-UAS teaming. The IOT&E results demonstrate that AB3-UAS teaming should not be undertaken unless the UAS has actionable combat information. Interaction with the UAS at any level of control can be an unwanted distraction to AB3 crews if the UAS does not provide useful information to the Apache crew. From the perspective of UAS procedures, crew changes at the beginning of AB3-UAS teaming should be avoided. The UAS operators should be fully informed of the tactical situation and prepared to share that information with the AB3 at the first moment that the AB3-UAS team is formed.

AB3 crews were consistently able to establish a data link with Gray Eagle to receive UAS video. Crews had less success establishing and maintaining control of the Gray Eagle sensor. On nine IOT&E missions, Grey Eagle UAS teamed with AB3 to assist with mission execution. During these missions, AB3 received 9 hours of UAS video and exercised control of the Gray Eagle sensor for 1.5 of those 9 hours of video. AB3 crews did not attempt to reposition UAS aircraft during IOT&E missions. On two missions, pilots reported that after gaining control of the sensor, the data link was lost and could not be restored for the rest of the mission. Once the link was lost, the AB3 crews were not able to receive UAS video or use the UAS sensor to locate and attack enemy targets. The Army should improve the stability of the tactical command data link for control of unmanned aircraft sensors.

Operational Suitability

The AB3 is operationally suitable. AB3 exceeded reliability thresholds with statistical confidence and met all current maintainability requirements. The redesigned Apache helmet offers improved comfort and performance compared to the legacy helmet. Overall, flight safety is enhanced by AB3's increased power margins.

AB3 pilots have less flexibility and require more time to load and retrieve mission data than from AB2 aircraft because of the design of a new memory device, called the Removable Memory Module. The AB3 has less capability for storing targets, waypoints, and control measures compared to legacy aircraft. In AB2 aircraft, pilots can store 1,000 targets, waypoints, or control measures on the aircraft. AB3 aircraft and mission planning software limit the AB3 to 50 targets, 50 waypoints, and 50 control measures. During training and the IOT&E, pilots found that this limitation degraded their ability to share situational awareness, identify and engage targets, and conduct reliefs-on-station.

Survivability

The AB3 is at least as survivable as the AB2. AB3 retains the infrared countermeasure effectiveness and ballistic protection of legacy Apache aircraft.¹ New AB3 subsystems met KPP survivability requirements and demonstrated ballistic tolerance similar to legacy Apache aircraft. Vulnerability analyses indicate that AB3 is slightly less vulnerable than AB2 aircraft. Improved hover performance and teaming with unmanned aircraft enables AB3 to employ tactics and maintain standoff that improves survivability. Infrared countermeasures provide protection against most man-portable rocket system threats, but the laser and radar warning systems could be improved. The APR-39A(V)4 radar warning receiver was not effective during IOT&E. Radar warning receiver performance in IOT&E was consistent with its history of performance deficiencies, which has included inaccurate threat identification, poor reliability, and high false alarm rates. False alarms were so pervasive during the IOT&E that the pilots ignored or turned off the APR-39. The APR-39 caused two missions failures and one mission abort. The AB3 is vulnerable to computer network attack. A computer network red team discovered threat vectors by which AB3 computer information could be compromised, corrupted, or exploited.

The Army conducted ballistic testing of the AB3 Composite Main Rotor Blade (CMRB) from May to July 2011 at Aberdeen Proving Ground, Maryland. The two dynamic shots were against a fully functional AH-64D Longbow Apache equipped with a full set of CMRBs. During dynamic testing, the CMRB demonstrated the capability to withstand a single hit from selected threats and meet its post-shot 30-minute get home capability. The CMRB has very low vulnerability to most small arms threats. However, larger threats directed at the blade spar proved to be the most stressing. A larger threat impacted the blade spar on the second dynamic shot and removed a substantial portion of the spar's cross-sectional area. The blade completed 30-minutes of operation, despite a loss of structural flapwise stiffness. While spinning, the centrifugal forces kept the blade aloft, but on the last revolution, the blade folded downward. It is unclear if the observed damage would have resulted in catastrophic blade failure within 30 minutes under actual flight conditions and if equivalent damage located at another span location would have resulted in the same outcome. Consequently, to obtain a better understanding of the results of this testing, the Army should conduct a structural analysis of the blade damaged during the second dynamic test and apply the results to the load limits that are expected under various flight operations conditions and at various spanwise locations.

Transmission Design

The AB3 transmission design poses safety concerns for pilots. It has a single tail rotor output pinion that provides power for the tail rotor, hydraulic pump, and electric generator. A failure of this one pinion would result in the simultaneous loss of the tail rotor, electric generator, and hydraulic power. Legacy Apache transmissions have two pinions that provide redundant power to electric and hydraulic components. While engineering estimated the probability of

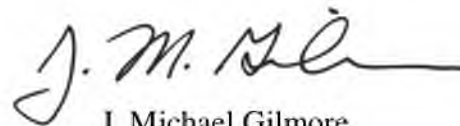
¹ DOT&E reported on the AN/AAR-57 Common Missile Warning System (CMWS) IOT&E in April 2006. The system was found to be operationally effective and suitable for combat operations in Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF) as integrated on the CH-47, UH-60, and C-12 series aircraft. CMWS performance on AB3 is similar to the performance on these other Army platforms.

failure for the tail rotor output pinion as remote (10^{-9}), a prototype design failed in a 5-foot hover during pilot training. Although the pilots landed safely in this incident, AB3 pilots continue to perceive the single tail rotor output pinion as an avoidable single point of failure. The AB3 improved drive system has performed as intended and enables increased payload capability.

Recommendations

The Army should consider the following recommendations and should verify the corrections to deficiencies in follow-on test and evaluation.

- Continue to refine tactics, techniques, and procedures for teaming with unmanned aircraft.
- Address pilot concerns about the transmission design. Conduct physics of failure analysis to provide an independent analysis of the probability of failure of the new tail rotor pinion design. Investigate the feasibility of alternate transmission designs that provide automatic redundant hydraulic and electrical power in the event of loss of power to the tail rotor.
- Redesign the Removable Memory Module and restore the capability to simultaneously retain updated mission data and download recorded mission data. Video files should have more efficient formats and interfaces with planning systems improved.
- Increase the number of available targets, waypoints, and control measures for mission planning and execution.
- Determine the root cause for data link dropouts and improve the stability of the tactical command data link for control of unmanned aircraft sensors.
- Consider incorporating improvements to current threat warning systems as they are developed. Upgrade radar and laser warning systems and provide for adjustable volume controls for each warning system. Employ appropriate tactics and reduce infrared signature to improve protection against advanced infrared missile threats.
- Perform a structural analysis of the CMRB to better understand the load carrying capabilities of the blade that was damaged during ballistic testing
- Address the Information Assurance vulnerabilities identified.
- Develop instrumentation for future training and testing to allow real-time adjudication of manned-unmanned engagements.



J. Michael Gilmore
Director

This page intentionally left blank.

Contents

System Overview 1

Test Adequacy 5

Operational Effectiveness 11

Operational Suitability 21

Survivability..... 29

Recommendations..... 35

This page intentionally left blank.

Section One

System Overview

This is my evaluation of test adequacy, operational effectiveness, operational suitability, and survivability of the Army's AH-64D Apache Block III (AB3) attack helicopter. The evaluation is based on data from the Initial Operational Test and Evaluation (IOT&E) that the Army Test and Evaluation Command conducted in March – April 2012 and the Live Fire Test and Evaluation (LFT&E), and is augmented by developmental testing conducted June 2009 through July 2012.

Mission Description and Concept of Employment

Attack Reconnaissance units are equipped with AB3 helicopters and conduct reconnaissance, security, and attack missions in support of ground combat forces. AB3 helicopters are employed in units of two or more aircraft to conduct reconnaissance to locate and report enemy forces and limit or prevent enemy activity. AB3 units conduct security operations by employing weapons to locate and restrict enemy action to provide reaction time, maneuver space, and protection for air or ground maneuver forces. AB3 units employ their own guns, rockets, and missiles in coordination with friendly ground forces to attack and destroy enemy forces.

AB3 Attack Reconnaissance units are integrated into the air-ground team scheme of maneuver. AB3 units conduct attack missions in close proximity to friendly ground forces, attack enemy forces at distant locations, support helicopter assaults, and provide reconnaissance and security support day and night, in any terrain, and in adverse weather. AB3 is designed to gain and employ situational awareness, move rapidly to positions of advantage, assimilate critical information, and deliver precision fires. AB3 units employ their own weapons or coordinate artillery fire to conduct effective combat operations and avoid collateral damage. AB3 units establish and maintain connectivity with ground forces through the use of airborne line-of-sight and satellite digital communications.

AB3 crews employ onboard sensors to locate and engage targets. A nose-mounted sensor provides infrared and electro-optical images to the pilot and co-pilot. This targeting and display system is integrated with lasers for ranging, locating, and designating targets for engagement. The optional mast-mounted Fire Control Radar employs millimeter radar to detect and classify moving and stationary vehicular and aircraft targets. When aircraft survivability equipment detects threat weapon signatures, crews have the ability to automatically cue sensors and weapons to the threat detection.

AB3 crews can be teamed with the Gray Eagle unmanned aircraft system (UAS) to locate and engage enemy targets. By establishing a high speed data link with the unmanned aircraft system, AB3 crews can receive video, locate and store targets using the infrared or electro-optical sensor aboard the unmanned system, employ the unmanned aircraft laser to designate targets for engagement, or reposition the unmanned aircraft. Attack Reconnaissance Battalions operate from established airfields and unimproved field sites. The battalion provides command

and control, logistics, ammunition and fuel resupply, ground transportation, and maintenance support necessary for sustained combat operations in any theater in the world.

System Description

The AB3 is a modernized version of the AH-64D attack helicopter. AB3 enhancements are planned in three major capability increments. The first capability increment (Lot 1) completed IOT&E in 2012. A second capability increment (Lot 4) is scheduled for operational testing in 2014 and the full capability (Lot 6) aircraft is scheduled for operational testing in 2015.

The legacy AH-64D Longbow Apache Block II (hereinafter referred to in this report only as AB2) is a four-bladed, twin-engine attack helicopter with tandem cockpit for a crew of two. The Longbow Apache entered production in 1995 and features a nose-mounted sensor suite for day/night target acquisition and an optional mast-mounted Fire Control Radar for target acquisition in dust, fog, or smoke. The AH-64D is armed with a 30 mm chain gun and carries a mixture of Hellfire missiles and 2.75-inch rockets. Legacy Apache aircraft have double- and triple-redundant aircraft systems and armor shielding to provide protection for critical aircraft systems and the crew. AB2 receives UAS information via tactical radio communication updates from the UAS operators; it does not have the capability to receive live video or control the UAS sensors or air vehicle.

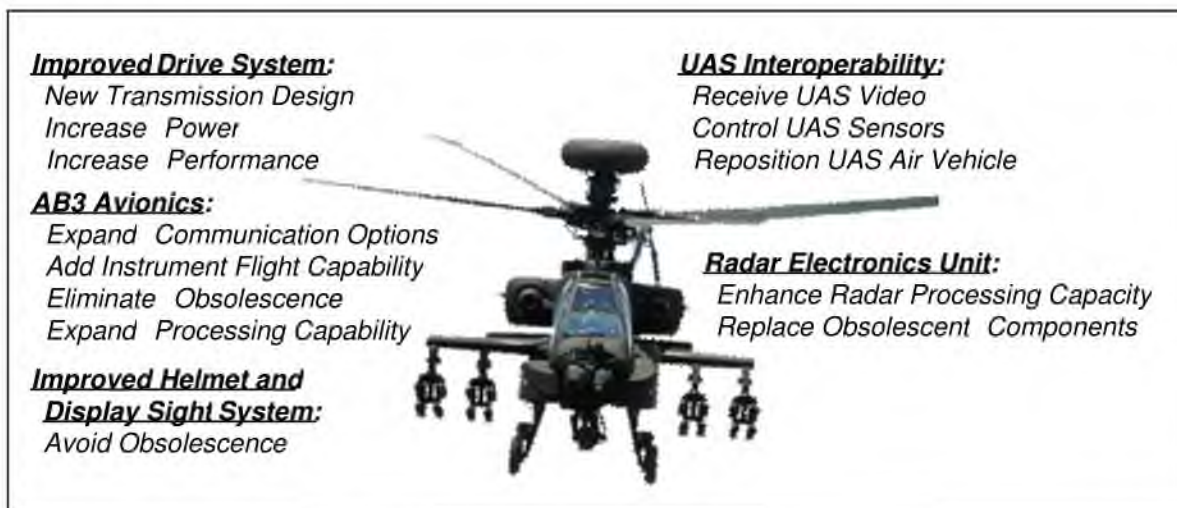
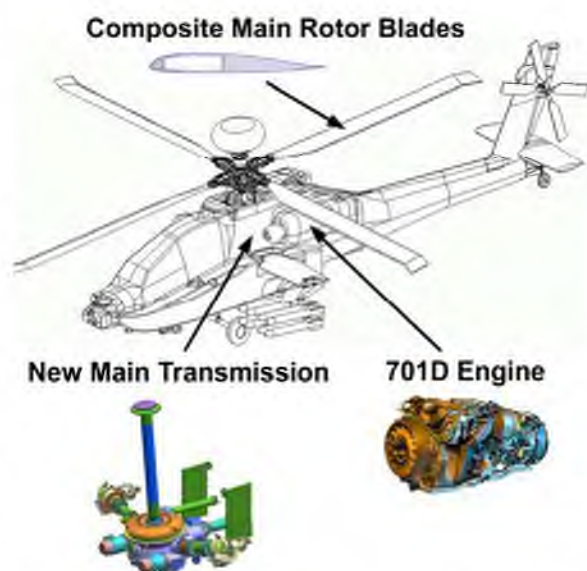



Figure 1-1. New Capabilities of Lot 1 AB3

AB3 will modernize the Apache fleet of 690 aircraft with new capabilities illustrated in Figure 1-1. The Lot 1 improved drive system will accommodate the added weight of new capabilities and enable safe operations in mountains such as in Afghanistan or Korea, with an operational load of ammunition and fuel. Modernized AB3 avionics retain existing functionality, remove obsolete components, and increase communications capabilities. Lot 1 avionics have the spare computing capacity to process the software-intensive upgrades envisioned for Lot 4 and Lot 6 aircraft. AB3 replaces an infrared helmet tracking system with a more accurate and more responsive magnetic head tracking system. The optional mast-mounted Fire Control Radar can be replaced by a mast-mounted data link antenna that enables interoperability with unmanned

aircraft systems on an AB3. Important features of the new capabilities are explained in more detail below:

- **Improved Drive System:** A new main transmission is the centerpiece of the improved drive system. The sturdier transmission and drive system components are capable of transferring greater torque (from 2,856 horsepower on AB2 to 3,400 horsepower on AB3) to the rotor system and fits within the space of the legacy transmission. New electronic controls allow the General Electric T700-GE-701D engines to operate at maximum horsepower (1,700 horsepower each) to take advantage of the increased capacity of the AB3 transmission. New composite main rotor blades (CMRBs) that are six inches longer with a new airfoil shape and greater twist generate more aerodynamic lift for the same input of power from the drive system. The combination of increased torque at the main transmission coupled with greater blade efficiency results in improved aircraft flight performance.
- A technical diagram showing the main rotor blades, the new main transmission, and the 701D engine. The main rotor blades are shown in a perspective view, with one blade highlighted in blue. The new main transmission is shown in a perspective view, with a blue and green color scheme. The 701D engine is shown in a perspective view, with a blue and orange color scheme. Arrows point from the labels to the respective components.
- **Increased Interoperability with Unmanned Aircraft Systems (UAS):** This capability enables the AB3 crew to receive real-time UAS video, control UAS sensors, and reposition UAS air vehicles. The existing Fire Control Radar antenna must be removed and replaced with a tactical command data link antenna. The AB3 crew uses this data link antenna to establish and maintain a high-speed data link and exercise control of UAS air vehicles.
- A diagram showing the UAS Data Link antenna. It is a small, rectangular antenna with a yellow and blue color scheme. An arrow points from the label to the antenna.
- **AB3 Avionics:** The AB3 aircraft has an updated and improved electronics system architecture that replaces obsolescent components and provides increased computer throughput to prepare for Lot 6 requirements. The mission computer, sensors, and gun system controller were among the components with newer and faster electronic components. Two of four legacy radios have been replaced with two multi-band ARC-231 radios. The new radios expand the frequency range and spacing, incorporate secure modes, and enable satellite communications. These radios, plus an improved Embedded Global Positioning System and Inertial Navigation Unit, provide the requisite communication and navigation capabilities to qualify AB3 aircraft to operate in worldwide air corridors and airfields reserved for instrument-rated aircraft.
 - **Radar Electronics Unit:** The radar electronics unit replaces obsolescent analog components with expanded digital processor capacity. The radar electronics unit is

designed to replicate or improve the target acquisition performance of the legacy Longbow Apache Fire Control Radar for Lot 1 aircraft. The radar electronics unit is required to increase the radar target detection range and expand the target set by Lot 6.

- **Integrated Helmet and Display Sight System:** The new Apache helmet employs a magnetic field to track each pilot's helmet during flight. It replaces the legacy Apache infrared-based helmet tracking system that is approaching obsolescence. The helmet projects flight data in front of the pilot's right eye and aligns sensors or weapons to the pilot's line of sight. The helmet is lighter and more comfortable than the legacy Apache helmet.
- **AB3 Aircraft Survivability Equipment:** The AB3 is protected by an integrated suite of radar, laser, and missile warning systems, electronic countermeasures, and countermeasures dispensing systems described in Table 1-1. The individual survivability components are the same as those on AB2 aircraft. They are integrated into the AB3 cockpit by a new aircraft gateway processor. This processor integrates all system operations, system test indications, and warnings (visual and aural) into a single display system.

New AB3 Helmet



Table 1-1. Aircraft Survivability Equipment

Subsystem	Subsystem Description
AAR-57 Common Missile Warning System	A missile warning system that detects and reports infrared-guided missile threats. Consists of a processor and five electro-optic sensors.
APR-39A(V)4 Radar Warning Receiver	Passively detects and reports threat radar emitters. Consists of a digital processor and five antennas.
AVR-2A Laser Warning Receiver	Detects, identifies, and reports laser signals. Consists of a processor and four sensors.
ALQ-136 Electronic Countermeasure System	Detects threat radar signals, determines appropriate countermeasures, and transmits appropriate electronic signals. Consists of a receiver-transmitter assembly with two antennas.
Countermeasures Dispenser	Dispenses flares from two ALQ-212(V) dispensers and chaff from an M-141 chaff dispenser in response to missile detections.

The AB3 (and its preceding versions) incorporates a variety of vulnerability reduction features, such as self-sealing fuel lines and fuel tank, aircrew armor, and fire-suppression system. The rotor blades, drive shaft system, structure, and main rotor hub are designed to be ballistically tolerant. All versions of the Apache incorporate redundancy for the engines, nose gearboxes, hydraulic systems, electric systems, flight controls, and suction-fed fuel system. The main transmission and drive system are designed to operate for 30 minutes following loss of lubrication.

Section Two Test Adequacy

Operational and live fire testing were adequate to determine the effectiveness, suitability, and survivability of the AB3 aircraft in anticipated combat environments. The Initial Operational Test and Evaluation (IOT&E) was preceded by four years of developmental testing that included analysis, modeling and simulation, component qualification testing, testing in environmental extremes, system-level flight testing, weapons qualification, and live fire testing. At the conclusion of developmental flight testing, the Army's airworthiness authority certified that the AB3 was safe for operational testing by typical combat pilots. All testing was completed as described in the Test and Evaluation Master Plan approved by DOT&E on August 11, 2010. Members of the DOT&E staff observed the IOT&E, live fire testing, and selected developmental test events and have analyzed all available test data and reports.

Operational Testing

The Army conducted pre-test training and tactics development from February 22, 2012 to March 14, 2012 and the IOT&E from March 16, 2012 to April 13, 2012 at the National Training Center, Fort Irwin, California. The testing was conducted in accordance with the IOT&E test plan that was approved by DOT&E on February 24, 2012.

The Army Test and Evaluation Command established a headquarters element at the Barstow-Daggett Airfield near Barstow, California, to exercise control of the training and testing. The headquarters element provided mission orders to the Apache battalion commander who planned and conducted operations with the AB3 and AB2 crews and maintainers. The test headquarters established secure communications networks, a Blue Force Tracker network, satellite communications, and coordinated for interoperability testing with Joint Surveillance Target Attack Radar System and Airborne Early Warning and Control System aircraft. All AB2 and AB3 missions began and ended at Barstow-Daggett Airfield, shown in Figure 2-1.



Figure 2-1. Four AB3 Aircraft Preparing to Launch from Barstow-Daggett Airfield

Over the seven-week period of training and testing, five AB3 aircraft flew 367 flight hours. Two of the AB3 aircraft were configured with Fire Control Radars, two with mast-mounted assemblies for controlling unmanned aircraft, and one without a mast-mounted assembly. During the initial operational test, the five AB3 aircraft and five legacy AB2 aircraft conducted 28 missions with conditions shown in Table 2-1. The conditions were selected using Design of Experiments methodology with four factors: aircraft type (AB3 or AB2), mission type (recon or attack), unmanned aircraft system (UAS) support (with or without), and light level (day or night). A single Gray Eagle UAS operated from and under the control of operators at Edwards Air Force Base, California, to provide UAS support when needed.

Table 2-1. IOT&E Missions Configurations

		UAS Support		No UAS Support			
		Day	Night	Day	Night		
AB2	Recon	1	0	2	2	5	12
	Attack	3	2	2	0	7	
AB3	Recon	1	1	1	2	5	16
	Attack	4	3	2	2	11	
Total Missions		9	6	7	6	28	
		15		13			

The mountainous, arid terrain at Fort Irwin is sandy with scattered vegetation and varies in elevation from 2,000 to 4,000 feet above sea level. Wind gusts to 45 knots and heavy rain resulted in 10 cancelled UAS test days and two cancelled Apache test days. Temperatures ranged from 32 to 82 degrees Fahrenheit.

The operational test was supported by Soldiers from the Army's 11th Armored Cavalry Regiment who act as the opposing forces in brigade training exercises at the National Training Center. An armored cavalry troop with five threat tanks, five threat armored personnel carriers, and five friendly Bradley Fighting Vehicles supported the training and the operational test. The threat forces were well trained and used camouflage and deception to avoid detection and skillfully employed their weapons to engage and kill the Apaches. During pre-test training, a man-portable infrared missile simulator, a radar-guided missile simulator, and a laser beam rider threat simulator were employed to stimulate AB3 threat warning systems. In the final two days of operational testing, actual threat radar systems were employed with simulated missile launches against detected unmanned aircraft and Apache aircraft.

All Apache aircraft and ground vehicles were instrumented for real-time casualty assessment during force-on-force training and IOT&E missions. The instrumentation used laser or geometric pairing to adjudicate force-on-force engagements. The results of these adjudications were transmitted by network in near-real time to the mission participants and test headquarters to provide awareness of how the missions were progressing.

The IOT&E included two weeks of range training and live fire gunnery. AB3 crews fired live 30 mm chain gun ammunition, 2.75-inch rockets, and Hellfire missiles against stationary targets on the Fort Irwin ranges. Operators employed active laser designators from AB3 and Gray Eagle aircraft for autonomous and remote engagements. The battalion master gunner reviewed gunnery tapes following each mission and scored gunnery timeliness and accuracy.

During the conduct of each IOT&E mission, the data collectors developed a log recording the significant events and weather conditions. Upon completion of each mission, pilots, commanders, and soldier maintainers completed post-mission questionnaires. The Army recorded cockpit video and audio from each aircraft, selected aircraft state data, real-time casualty assessment data from all instrumented systems, and UAS video. Throughout training and testing, data collectors recorded all AB3 reliability failures and maintenance actions. The Army videotaped all pre- and post-mission briefings. All textual and quantitative data were consolidated into a set of digital files and reviewed by the Army evaluator, program manager representative, and Army user representative for accuracy. Video files were recorded and reviewed to provide better understanding of what took place during each mission.

The 10 AB3 and 10 AB2 IOT&E pilots from the 1st Attack Reconnaissance Battalion, 1st Infantry Division had similar flight experience in Apache helicopters. AB3 and AB2 pilots were not significantly different in comparisons of total flight hours, total combat flight hours, and hours using night vision goggles. The least experienced pilot had 114 total flight hours and no combat experience and the most senior pilot had 5,400 total flight hours and 2,000 combat flight hours. The individual cockpit total flight times for both AB2 and AB3 were also not significantly different in total flight experience levels. Before flight training, the AB3 crews had three weeks of classroom and simulator training at Boeing's plant in Mesa, Arizona. The AB2 crews participated in unit training at their home station before the IOT&E.

Gray Eagle operators were not experienced in operating Gray Eagle. At the time of the AB3 IOT&E, the supporting Gray Eagle unit had just begun operator flight and qualification training. During AB3 missions, the new Gray Eagle operators were supervised by over-the-shoulder trainers and were frequently rotated to allow multiple operators to train with the Apache units. At times, the operators were rotated just as a teaming mission with AB3 began. On six occasions, teaming with AB3 began at a time when the Gray Eagle operator had no better or worse situational awareness of enemy disposition than did the AB3 crew. DOT&E and the Army understood that the Gray Eagle operators were not yet proficient and were undergoing initial training at Edwards Air Force Base.

Information Assurance Testing

During the last week of the AB3 IOT&E, an Army computer network operations red team conducted limited penetration testing of AB3 computer networks. The four-person red team considered three attack vectors to gain access to the AB3 networked systems: the Blue Force Tracker, the Aviation Mission Planning System, and aircraft maintenance ports. Penetration testing took place while AB3 aircraft were powered up, but without engines or rotors turning to avoid compromising flight safety. The red team avoided actions that could affect an

AB3's ability to conduct flight operations. Red team activities were limited to computer network scanning (passive and active).

Live Fire Testing

Live fire ballistic testing and analysis provided adequate information to compare AB3 system-level vulnerability with user-specified requirements and AB2 system-level vulnerabilities. In accordance with the DOT&E-approved Alternate Live Fire Strategy, ballistic testing and evaluation focused on new or modified components and subsystems identified in Figure 2-2.

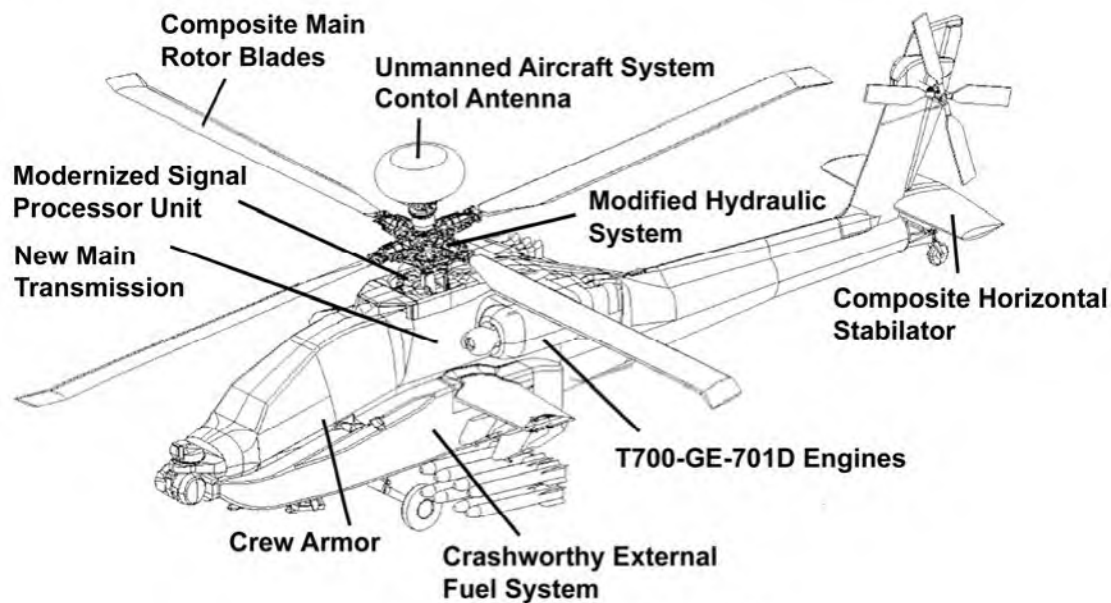


Figure 2-2. Focus of AB3 LFT&E

The Army conducted ballistic testing of production-representative AB3 improved drive system and composite main rotor blades (CMRBs) in May – July 2011 at Aberdeen Proving Ground, Maryland. The tests included both static and dynamic shots from a variety of small caliber threats. The dynamic tests were conducted against a ground-mounted AH-64D Longbow Apache with engines running and rotors turning and pitched to generate flight-representative loads. The targeted subsystem was mounted in a test stand for static shots.

The Army conducted ballistic shots against 20 crew armor panels on December 7, 2010, to verify their performance against the key performance parameter force protection threat. This requalification effort was necessary because crew airframe armor was damaged in combat or degraded from normal use.

At the conclusion of ballistic testing, the Army completed a system-level vulnerability analysis using a modeling and simulation suite that models target-threat interaction for direct fire and small projectiles on air and ground systems. The geometry, criticality, and functionality of the aircraft components define the target in the model. The initial conditions (velocity, impact angle, etc.) and physical characteristics (mass, materials, fuzing, etc.) define the ballistic threat

for each simulated shot against the aircraft model. The Army developed system-level vulnerability results for the AB3 and AB2 using the latest high-fidelity component descriptions of both aircraft. Estimates for the probability of kill given component damage ($P_{k/cd}$) in the model were validated by the results from ballistic testing.

Test Limitations

The Army was not able to simulate or adjudicate remote UAS engagements during the force-on-force portion of the IOT&E. The Gray Eagle was instrumented with the intention of employing its laser to designate targets for remote AB3 weapons engagement. This instrumentation did not work as intended and was not able to overcome multiple software fail-safes in the Gray Eagle and AB3 aircraft that prevent accidental firing of the Gray Eagle non-eye safe laser. As a result of this limitation, the Army was not able to demonstrate a new capability that is unique to AB3 during the training and force-on-force portions of IOT&E. The UAS remote designation capability was demonstrated seven times during the live gunnery phase of IOT&E.

Other force-on-force real-time casualty instrumentation worked intermittently, adjudicating some engagements and failing to adjudicate others. As a result, crews on both sides of force-on-force battles on occasion used inappropriate tactics while trying to score a kill. Frustrated at their inability, at times, to kill threat tanks at long range with simulated Hellfire missiles, Apache crews maneuvered to within point blank range to engage tanks with 30 mm guns in an attempt to score kills. Engagement of armor at point-blank range is not operationally realistic. There were two occasions in which the Gray Eagle UAS could have been engaged and destroyed by threat equipment. The UAS was deemed vital to the test and was permitted to remain in service to facilitate test objectives for the AB3.

This page intentionally left blank.

Section Three

Operational Effectiveness

The AB3 is operationally effective. AB3 has improved flight performance compared to legacy Apache aircraft. AB3 hover performance exceeds that of legacy aircraft by 35 percent and enables AB3 units to operate at higher altitudes and temperatures with larger payloads. An AB3 with new specification engines meets the hover performance Key Performance Parameter in that the aircraft can hover out of ground effect (OGE) at 6,000 feet pressure altitude at 95 degrees Fahrenheit with 3,400 pounds of payload. And, when aided by real-time unmanned aircraft system (UAS) video containing actionable intelligence, AB3 teams demonstrated greater target acquisition ranges, greater Hellfire engagement ranges, and the potential for greater mission success than AB2 teams.

This evaluation is based on the ability of AB3-equipped units – at times teamed with Gray Eagle UAS – to complete assigned missions compared to AB2-equipped units that were also teamed with Gray Eagle on some missions. AB3 crews received UAS video when teamed with Gray Eagle. AB2 crews received verbal reports and target grids when teamed with Gray Eagle because the legacy system could not receive live UAS video. AB3 aircraft and subsystem performance is compared to KPPs, user-specified requirements, and legacy system performance. Net readiness assessments and the observed ability of AB3 crews to complete missions in a stressful and challenging operational test using voice and data networks illustrate the operational effectiveness of an AB3-equipped unit.

Mission Effectiveness

There was no significant difference (in the statistical sense) in overall mission success between the AB3 and the AB2. In fact, missions conducted with UAS support were less successful than those conducted without UAS support. In particular, when teamed with a Gray Eagle UAS providing no actionable combat information, AB3 crews were not successful. Nonetheless, test data indicate the ability of the AB3 to team with a UAS has the potential to enhance AB3 mission effectiveness relative to AB2.

In several cases the test showed when AB3 crews were teamed with UAS, the real time video from the UAS sensor increased the AB3 target detection/acquisition ranges up to ten times greater than with the legacy on board acquisition systems. During three missions AB3 crews received real time threat descriptions and targetable coordinates from an area of interest over 75 kilometers away while preparing to depart from the airfield. While enroute to the target area, the AB3 crew maintained situational awareness while monitoring UAS video and updated target locations prior to arriving at their battle positions. This feature of the AB3 facilitated engagement of targets by providing added standoff for protection and by reducing engagement/exposure times. Without UAS video, AB2 aircrews maneuvered into the target area to locate the threats and make positive identification, subsequently exposing themselves to threat system detection and engagement. AB3 aircrews provided positive comments in their post-test surveys about the improved situational awareness from this UAS video.

Although AB2 teams received target grids by voice from UAS before arriving on station, those aircraft still needed to close within range to clearly identify targets before engagement. This difference in situational awareness meant that AB3 crews were able to initiate Hellfire engagements from a greater range than AB2 crews. The average Hellfire engagement range for AB3 was 2,393 meters greater than the average AB2 Hellfire engagement range. By engaging targets earlier, AB3 crews maintained a safe standoff from threat systems longer.

Mission success scores were assigned to the 28 missions of the force-on-force phase of IOT&E by the Army evaluator, Army user representative, and program manager representative using the criteria in Table 3-1. DOT&E staff members, using the same criteria in Table 3-1, conducted an independent assessment and came to the same conclusion regarding mission success scores. These scores were assigned at the end of the test after reviewing recorded data on real-time casualty assessments, cockpit video, UAS video, engagement and target acquisition video, post-mission debriefings, and mission logs.

Table 3-1. Mission Scoring Criteria

Mission Score	Outcome	General Criteria
5	Complete Success	The Apache team quickly located and neutralized most or all of the threat systems without either aircraft being destroyed. The team used very good tactics.
4	Partial Success	The Apache team located and neutralized some threat systems. If engaged, only one or neither aircraft was destroyed. The team accomplished most but not all assigned mission tasks and employed good tactics.
3	Neutral Outcome	The Apache team located and neutralized some of threat systems. Aircraft were engaged, but only one was destroyed. The team accomplished some assigned mission tasks and employed good and poor tactics.
2	Partial Failure	The Apache team located and attempted to engage some threat systems. One aircraft was destroyed. The team accomplished some assigned mission tasks and used poor tactics.
1	Complete Failure	The Apache team was destroyed without locating or neutralizing any threats. The team accomplished no assigned mission tasks and used poor tactics.

The analysis of variance indicates, at an 80 percent confidence level, that aircraft type and mission type had no effect on average mission success scores. The average mission scores and 80 percent confidence intervals are plotted in Figure 3-1 for each of the four test design factors. A p-value, the probability the difference between levels is due to chance alone, is shown for each factor.² Apache crews were more likely to succeed at night than in the daytime because

² For example, a p-value of 0.08 indicates that the observed result would have occurred only 8 percent of the time by chance alone. In this evaluation, p-values less than 0.10 are considered as having a significant effect by that factor; a p-value of 0.22 was moderately or nearly significant with a 22 percent chance of observing that difference if that factor was not a significant influence on performance. Clearly p-values of 0.83 and 0.97 indicate those factors are not having an effect on the outcome of the trials.

Apaches have superior night vision sensors compared to night sensors employed by the ground threat forces. All but one night mission were successful. In contrast, half of the day missions were partial or complete failures, with all complete failures occurring with UAS support. Threat vehicles were difficult to detect during the day for Apaches and the UAS, especially when the threats were stationary. Mission success scores were similar, whether Apaches were conducting attack or reconnaissance missions. The only statistically significant result with high confidence was that teaming with UAS was more likely to lead to mission failure than to mission success.

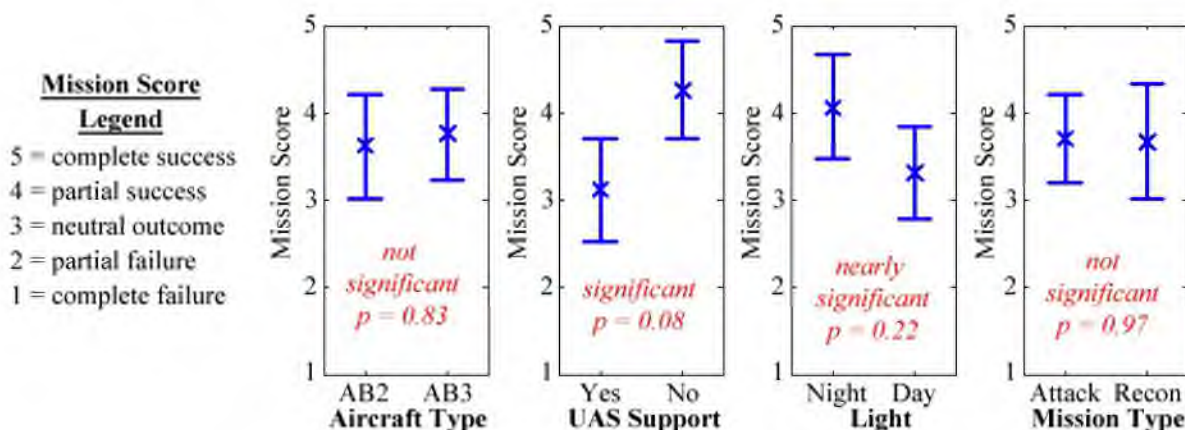


Figure 3-1. Average Mission Scores Based on All Missions

Mission Success Comparison: Aircraft Type

As demonstrated by the large p-value and overlapping confidence intervals in Figure 3-1, there was no statistical difference in the average mission success scores between the AB3 and AB2 teams, but the distribution of mission scores for AB3 and AB2 were in fact different.³ Figure 3-2 illustrates that AB3 missions tended to be scored as complete successes (bright green) or complete failures (bright red). AB2 mission scores were more evenly distributed from good to bad. This difference is explained by a closer examination of UAS teaming.

³ The Likelihood Ratio confirms that the two distributions are statistically different with a p-value of 0.143.

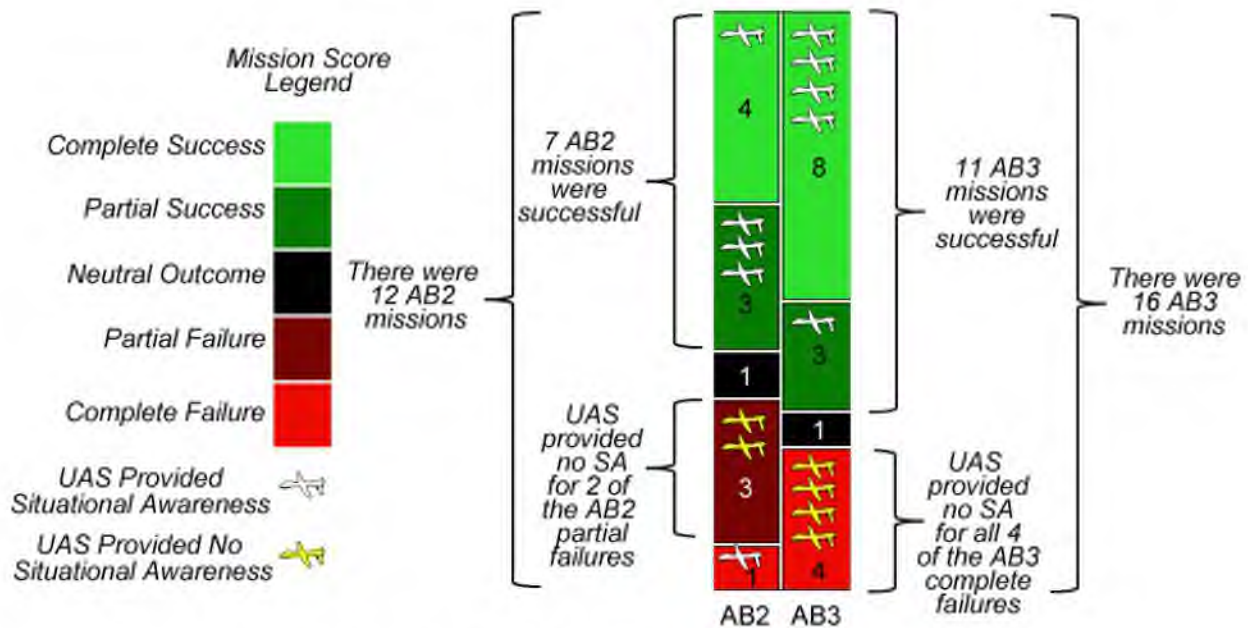


Figure 3-2. Distribution of AB3 and AB2 Mission Success Scores

UAS Teaming

AB3 mission success scores had greater polarity because UAS support enabled more complete successes for the AB3 when the UAS had accurate situational awareness, but led to more complete failures for the AB3 when the UAS provided no added situational awareness. The UAS icons in Figure 3-2 indicate when the UAS provided useful information (white icons) and when not (yellow icons). On four AB3 and two AB2 missions, the UAS had no actionable information when Apache crews arrived on station. Rather than ignore the UAS as the AB2 crews did, the AB3 crews continued to monitor the UAS video or took control of the UAS sensor in an attempt to find threat targets. Post-test surveys showed that UAS video is distracting to AB3 crews when the data link fails or the video contains no useful information. These results should inform the development of tactics, techniques, and procedures for AB3-UAS teaming. The IOT&E results demonstrate that AB3-UAS teaming should not be undertaken unless the UAS has actionable combat information. Interaction with the UAS at any level of control can be an unwanted distraction to AB3 crews if the UAS does not provide useful information to the Apache crew. From the perspective of UAS procedures, crew changes at the beginning of AB3-UAS teaming should be avoided. The UAS operators should be fully informed of the tactical situation and prepared to share that information with the AB3 at the first moment that the AB3-UAS team is formed.

System Performance

Mission effectiveness was enhanced by improved flight performance stemming from the improved drive system, increased engine horsepower, and the composite main rotor blade (CMRB). The increases in AB3 flight performance meet user-specified requirements and enabled AB3 crews to operate with greater payloads at higher altitudes and temperatures and

turbulent winds than with legacy Apache aircraft. Enhanced flight performance enables AB3 aircraft to operate safely above 6,000 feet pressure altitude in the summertime temperatures in the mountains of Afghanistan or Korea with an operational load of ammunition or fuel. AB2 cannot hover or carry the required AB3 payload at these conditions at all. AB2 flight performance limits crews to operate at summertime temperatures below 4,000 feet pressure altitude and with smaller payloads.

Hover Payload, Speed, and Endurance

By having increased performance for hover out of ground effect, AB3 aircraft can operate safely in mountainous terrain, as in Afghanistan or Korea, with an operational load of ammunition and fuel. With new engines, AB3 can hover with a 3,798-pound payload at 6,000 feet pressure altitude and 95 degrees Fahrenheit. As engines age (engine design life is 10,000 hours) and degrade to the minimum acceptable performance level for a new engine, AB3 crews will still be able to operate in mountainous areas, but will be able to carry about 1,000 pounds less fuel or ammunition, delay coming to a hover until later in the mission after burning off fuel, monitor torque levels carefully, and maintain forward flight to avoid exceeding maximum available engine power. Before new engines are installed on AB3, each engine is tested to determine its Engine Torque Factor (ETF) rating. New AB3 engines with an average ETF of 1.09 can generate 2,964 shaft horsepower at payload at 6,000 feet pressure altitude and 95 degrees Fahrenheit. As engines age, they eventually degrade to an ETF of 1.0 and generate 2,703 shaft horsepower, capable of hovering at the same altitude and temperature conditions with a reduced payload of 2,784 pounds (about 500 pounds short of the threshold requirement). The published AB3 operator's manual estimates performance based on engines with an ETF of 1.0.

Whether equipped with minimally acceptable engines or new engines, AB3 remains capable of conducting combat operations as intended at 6,000 feet, 95 degrees with a meaningful operational payload; in these conditions, AB3 crews will be able to conduct a 2-hour mission while carrying the Fire Control Radar, 8 Hellfire missiles, and 250 rounds of 30 mm ammunition. By comparison, AB2 crews would not be able to complete this mission at all.

Figure 3-3 illustrates AB3 hover range, endurance, and dash speed performance at 6,000 feet pressure altitude, 95 degrees Fahrenheit. The right side of Figure 3-3 compares AB3 to AB2 performance for typical IOT&E conditions (2,000 feet pressure altitude, 68 degrees). During IOT&E, AB3 range, endurance, and dash speed were comparable to AB2 when both aircraft carried the same payload (3,900 pounds). But AB3 has more power and therefore greater hover capability with a larger hover payload (34 percent or 1,700 pounds) than AB2.

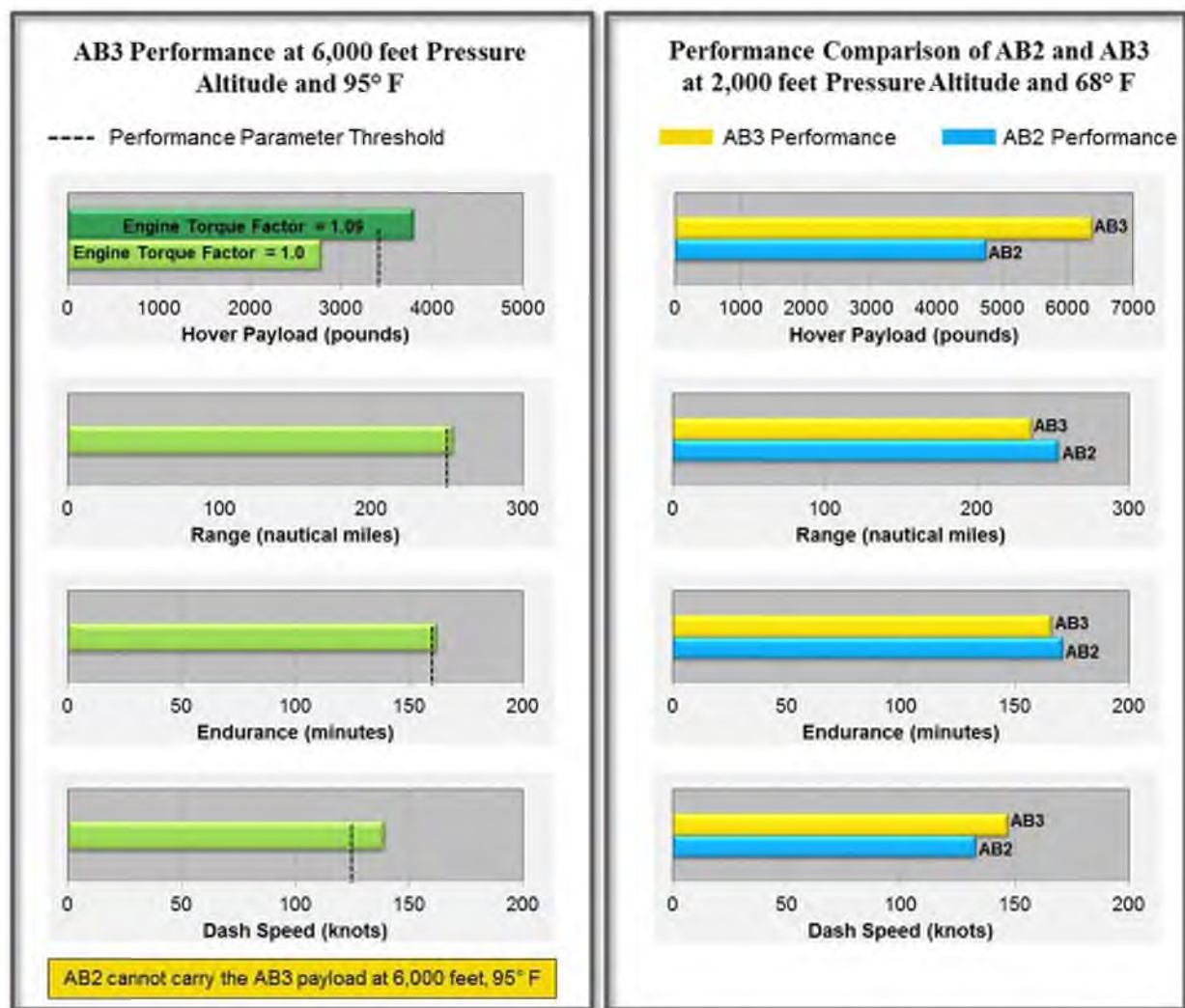


Figure 3-3. AB3 Performance (Left) and AB3 versus AB2 at IOT&E Conditions (Right)

AB2 aircraft cannot hover at 6,000 feet pressure altitude and 95 degrees with the AB3 payload at all and has difficulty operating above 4,000 feet. AB3 hover performance was demonstrated during December 2010 developmental flight testing and documented in hover performance charts in the AB3 operator's manual.⁴ The accuracy of the performance charts was verified during IOT&E where AB3 performance matched or exceeded performance predicted by the operator's manual.

China Lake Missions

During the IOT&E, AB3 and AB2 teams conducted two interdiction attack missions to China Lake, California. The mission was to detect, identify, and destroy radar threat systems located at China Lake. On the day these missions were conducted, the Gray Eagle UAS was on station as planned to provide targeting information. Before the missions began, the threat radars detected and engaged the Gray Eagle. UAS support could have been terminated by the threat

⁴ Technical Manual for Longbow Apache AH-64D Block III, TM 1-1520-251-10-3, February 2012.

engagements. In order to fully utilize test range assets, the test continued. On following days, the plan was to conduct these missions without UAS support, but later missions at China Lake were cancelled by bad weather.

Both aircraft teams launched from the Barstow-Daggett airfield and flew 100 kilometers to China Lake. Upon entering the China Lake range, the AB3 aircraft approached the threat systems flying slowly and low to the terrain to avoid detection. At the time of this mission, winds at China Lake were gusting to 40 knots, the temperature was 70 degrees, and the aircraft was operating at 3,000 to 4,000 feet pressure altitude. In spite of the altitude, temperature, and winds, the AB3 crews maneuvered with AB3 power settings of approximately 65 percent torque. Using target locations from a Gray Eagle UAS, the AB3 crews engaged several threat systems and departed undetected from China Lake. Had the UAS support been destroyed by threat systems, detection of threat targets would have been more difficult for AB3 crews, and might have resulted in mission failure. The power margin enabled AB3 crews to focus their attention on avoiding the threat and successfully completing the mission.

AB2 crews were not successful on this mission because the AB2 was near its performance limit. As AB2 crews approached the radar threat systems, their aircraft were operating at near 100 percent torque. Near their torque limit, AB2 crews could not hover and had to remain in forward flight well above the terrain (to avoid crashing) and constantly monitor power settings to avoid over-torqueing the AB2 transmission. The UAS provided target locations, but the AB2 crews were unable to get within Hellfire range (8 kilometers) before they were detected and engaged by the threat systems. Had the UAS support been destroyed by threat systems, AB2 team success would have been even more difficult. The AB2 teams attempted three times to get within engagement range but were detected and engaged by the threat each time. Lacking power to hover with this altitude, temperature, and winds, AB2 crews were not able to employ the tactics that would keep them hidden from the threat and achieve mission success.

Fire Control Radar Performance

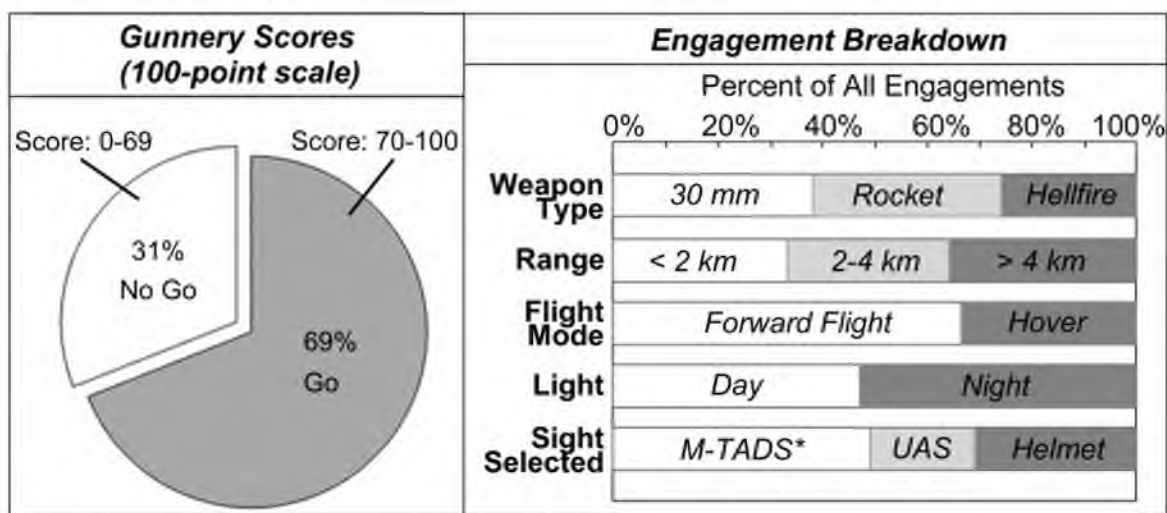
The AB3 Fire Control Radar met all specified requirements and performed as well or better than the legacy Fire Control Radar in developmental testing of ground and air targeting modes. Fire Control Radar detection performance during IOT&E was consistent with the developmental test results. Fire Control Radar performance anomalies that were discovered before Milestone C have been corrected and retested, and they no longer degrade system performance.

In 2009 developmental testing, detection of moving and hovering helicopters in the ground targeting mode was degraded by an error in signal processing. The radar electronics unit was not properly adjusting range data during Moving Target Indicator processing. As a result, near-range hovering helicopter targets were not detected very often. This problem has been corrected and met requirements for detection of near-range targets in 2010 developmental flight testing.

Developmental testing in 2009 also revealed a false alarm rate by the reporting of an excessive number of hovering helicopter false alarms. The radar incorrectly interpreted multiple radar echoes from distant terrain as hovering helicopters. This problem was corrected and did not reoccur in 2010 developmental flight testing of the Fire Control Radar or during IOT&E.

Lethality

AB3 demonstrated that it retains all legacy capabilities for weapons employment and destruction of threat targets. When linked to Gray Eagle, AB3 can receive targets from UAS or find targets by controlling the UAS sensor. The AB3 can use automated cues from the integrated aircraft survivability equipment to locate targets. During day and night live fire gunnery, AB3 crews met Army gunnery standards on the 57 scored live fire events as shown in Figure 3-4. Crews used multiple target acquisition and designating sources including night vision goggles, on-ship targeting and designating system, Fire Control Radar, crew helmets, Gray Eagle, and wingman. Crews employed the 30 mm gun, rockets, and Hellfire missiles at short, medium, and long range. Scores for timeliness and accuracy of these engagements were consistent with gunnery scores for legacy Apache aircraft. All 17 Hellfire missiles hit and destroyed the intended targets.



*Modernized Target Acquisition Designator Sight

Figure 3-4. AB3 Live Fire Gunnery Events

Gunnery standards for target engagement when teamed with a UAS have not been established. The unit master gunner used the approved Army Helicopter Gunnery standards for timeliness and accuracy, but noted that there was no approved standard for the acceptable engagement time when using UAS to acquire and designate targets. The Army should develop training and test instrumentation for real-time adjudication of manned-unmanned engagements.

Net Readiness

Voice Communication

Secure and non-secure voice communications using two ARC-231 multi-band radios and two ARC-201D Single Channel Ground and Airborne Radio Set (SINCGARS) radios were effective during the IOT&E. Voice connectivity was established at various times on all four radios and maintained as needed throughout all AB3 IOT&E missions. Communication was successful between AB3s, between AB3 and an Army network with operations cells, and between AB3 and UAS operators. Procedures for initializing voice communications systems were routine. AB3 pilots exchanged voice and digital messages with Airborne Early Warning and Control System and Joint Surveillance Target Attack Radar System aircraft.

During pre-IOT&E training, AB3 pilots reported radio interference, bleed over, and excess noise on the ARC-231 multi-band radios. These problems occurred when multiple radio networks operated on a narrow band of frequencies. To avoid these problems, mission planners established radio frequencies with wider channel separation (greater than 25 kilohertz). Pilots were satisfied with the quality of radio communications during IOT&E.

Voice communications by satellite were established and demonstrated during the two missions to China Lake.

Digital Communication

The AB3 successfully transmitted and received digital messages on the Blue Force Tracker network. Automatically-generated position reports and various messages generated or received by the pilots supported mission execution during the operational test. Location of friendly or enemy units, mission changes, and text messages were shared between aircraft and ground stations. Pilots found Blue Force Tracker to be the only reliable method of communication with the test headquarters when operating beyond line-of-sight. Aircrews preferred voice communications to digital messaging when timeliness was critical and the aircraft was within line-of-sight.

Early in IOT&E, pilots reported problems with loading Blue Force Tracker data, unexpected expiration of passwords, and network connectivity. As pilots gained familiarity and experience with Blue Force Tracker, digital messaging became routine during long-range missions.

Certifications

The AB3 is on track for meeting the Net Readiness KPP by Lot 4 as required. The AB3 completed an interoperability demonstration test at the Central Test Support Facility in June 2012. All digital message protocol requirements were demonstrated. Formal Army Interoperability Certification testing is scheduled for completion in August 2012. The Army Chief Information Officer (CIO)/G6 provided a memorandum stating that the AB3 is at low risk for being certified in August 2012.

Some communications shortfalls were identified during IOT&E that will require correction before Lot 4 to fully meet the Net Readiness KPP. AB3 cannot transmit digital

messages as required using the ARC-231 radio. The program manager plans to incorporate this capability into AB3 by Lot 2b. As mentioned earlier, premature password expiration frustrated pilot efforts to connect to the Blue Force Tracker network. Neither of these shortcomings had a significant effect on mission effectiveness.

UAS Interoperability

AB3 crews were consistently able to establish a data link with Gray Eagle to receive UAS video. Crews had less success establishing and maintaining control of the Gray Eagle sensor. On nine IOT&E missions, Grey Eagle UAS teamed with AB3 to assist with mission execution. During these missions, AB3 received 9 hours of UAS video and exercised control of the Gray Eagle sensor for 1.5 of those 9 hours of video. AB3 crews did not attempt to reposition UAS aircraft during IOT&E missions. On two missions, pilots reported that after gaining control of the sensor, the data link was lost and could not be restored for the rest of the mission. Once the link was lost, the AB3 crews were not able to receive UAS video or use the UAS sensor to locate and attack enemy targets. The Army should improve the consistency of the tactical command data link for control of unmanned aircraft sensors.

In post-mission surveys, pilots were generally positive about the added situational awareness from Gray Eagle. Pilots found the capability to receive UAS video of the target area while the helicopters were still preparing to launch particularly valuable. In those instances, accurate pre-launch information on the enemy's disposition enabled the AB3 crews to successfully plan and execute the mission.

Pilot workload when using the UAS was manageable when the system was operating normally. Pilot workload increased slightly when the data link could not be established or maintained, but was manageable.

Section Four Operational Suitability

The AB3 is operationally suitable. AB3 exceeded reliability thresholds with statistical confidence and met the maintainability requirement. Overall flight safety is enhanced by AB3's increased power margins. The redesigned Apache helmet offers improved comfort and performance compared to the legacy helmet. However, pilots are concerned that the new transmission design has introduced an avoidable single point of failure and, the Removable Memory Module has added more time and less operational flexibility to legacy mission planning and execution procedures.

Reliability

The AB3 exceeded current Lot 1 and future Lot 4 reliability requirements by a wide margin. The AB3 has a Key Performance Parameter (KPP) for Mean Time Between Mission Failures (MTBF(M)) and a key system attribute for Mean Time Between Essential Maintenance Actions (MTBEMA). A mission failure or mission abort results in early termination or the inability to start a mission. An Essential Maintenance Action (EMA) is any incident or malfunction that results in the loss of one or more mission essential functions. Once discovered, EMAs must be corrected before flight can resume. During 367.1 flight hours of IOT&E, the AB3 aircraft had 10 mission aborts and 25 EMA events. As indicated in Table 4-1, the AB3 performed better than the required threshold for both requirements.

Table 4-1. AB3 Reliability at the IOT&E

	Threshold Requirements (hours)		Demonstrated (hours)	Lower 80% Confidence Interval (hours)	Statistical Confidence that Lot 1 requirement has been met
	Lot 1	Lot 4			
MTBF(M)	15.3	17	36.7	23.8	99.9%
MTBEMA	2.6	2.9	4.9	4.2	99.9%

The observed MTBF(M) of 36.7 hours supports a mission reliability estimate of 91 percent for a 3.5-hour mission, exceeding the required mission reliability KPP of 80 percent. Mission reliability is the probability of completing a 3.5-hour mission without a single abort, assuming mission aborts are exponentially distributed with a mean of 36.7 hours.

AB3 IOT&E reliability estimates are better than the reliability estimates for the legacy Apache. Figure 4-1 compares AB3 IOT&E reliability results to the legacy AH-64D Block I/II reliability. Legacy Apache reliability estimates are based on 8713.7 flight hours of historical data collected from November 2000 through October 2001. Confidence intervals for the two estimates do not overlap, indicating that the AB3 reliability is better than the legacy platform.

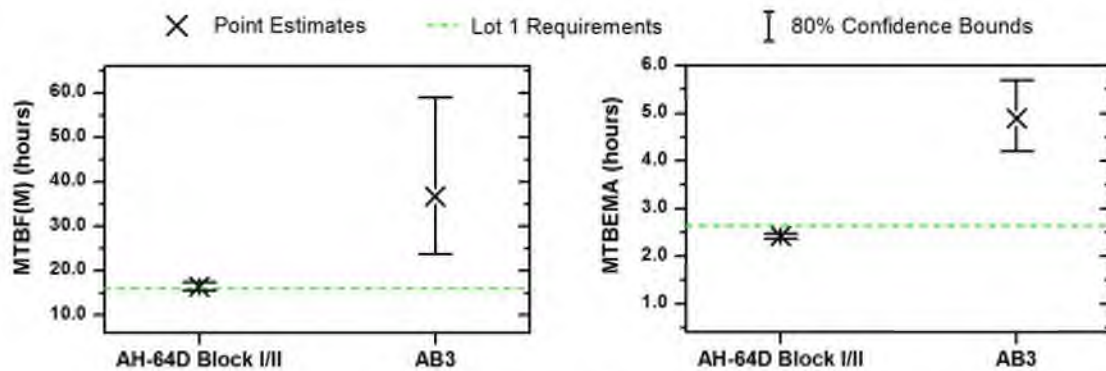


Figure 4-1. Comparison of AB3 and AB2 Reliability

The AB3 IOT&E reliability estimates are better than the projected reliability growth curves for MTBF(M) and MTBEMA. Figure 4-2 illustrates projected growth curves for MTBEMA with IOT&E point estimates and 80 percent confidence intervals. The confidence interval falls above the growth planning curves, indicating that the program is currently exceeding the growth curve, and the Lot 1 and Lot 4 requirements. The noticeable improvement in reliability between earlier Limited User Test (LUT) and developmental testing (DT) coincides with a change in test aircraft. The LUT and DT reliability estimates were based on testing of two prototype AB3 aircraft. All five IOT&E aircraft were production-representative and recently rolled off the Boeing production line with all reliability improvements from system development.

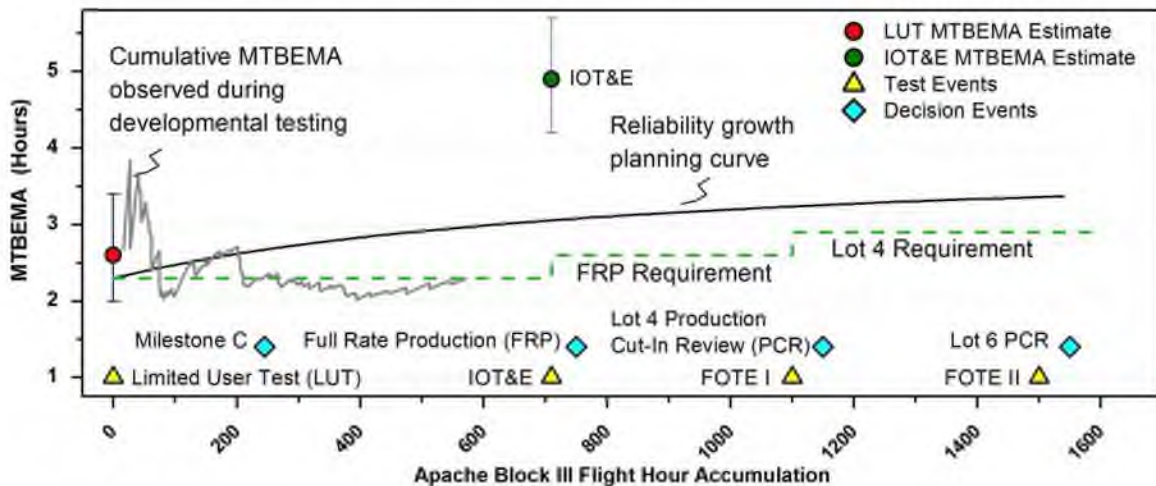


Figure 4-2. AB3 Reliability Growth Curves for MTBEMA

The program should continue to focus reliability improvement efforts on the drive system. Figure 4-3 illustrates that the new drive system had more failures and required more maintenance than the other subsystems. The majority of those failures were worn or broken drive system seals that resulted in oil leaks. One input seal failed six times during IOT&E. Boeing identified sand ingress through the input seal O-ring as the root cause for these failures and is redesigning the O-ring to correct the problem.

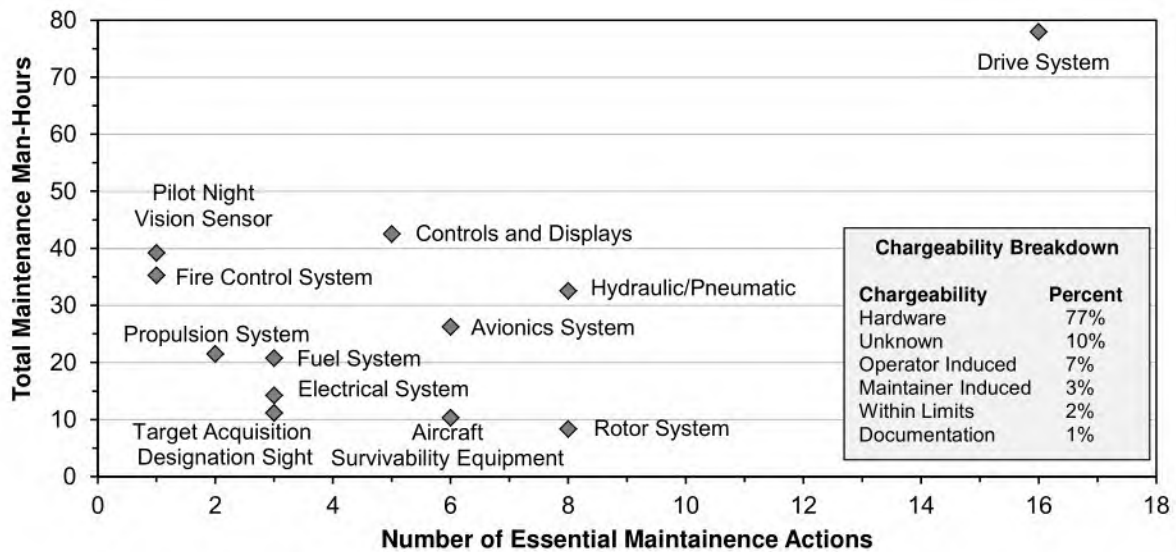


Figure 4-3. EMA and Maintenance Data by AB3 Subsystem and Chargeability

Many of the failure modes for other subsystems observed at the November 2009 LUT did not occur in the IOT and appear to have been corrected. For example, 48 percent of the LUT failures were charged to software. The IOT&E aircraft did not experience any chargeable software failures. Boeing implemented software upgrades that addressed high-rate failure modes for the mission processor and gun system controller. Hardening of mission processor components and redesigned generator seals eliminated two of the most frequent LUT hardware failure modes.

Maintainability

The AB3 met Lot 1 and Lot 4 maintainability requirements for Maintenance Man-Hours per Flight Hour (MMH/FH). This metric measures the amount of scheduled and unscheduled maintenance hours required for soldier maintainers. Apache aircraft have periodic maintenance inspections and services (at 25 hours, 100 hours, 500 hours, etc.) that require scheduled maintenance hours. Maintenance man-hours that result from reliability failures are unscheduled. The unscheduled MMH/FH was 1.1 hours, well below the 3.8-hour Lot 1 requirement because there were few reliability failures during IOT&E. As shown in Table 4-2, the AB3 meets the future MMH/FH requirement for Lot 4.

Table 4-2. AB3 Maintainability at the IOT&E

	Demonstrated	Requirements	
		Lot 1	Lot 4
MMH/FH (total)	1.8	n/a	≤ 7.6
MMH/FH (unscheduled)	1.1	≤ 3.8	≤ 3.4

System Design

Transmission Design

The AB3 transmission design poses safety concern for Apache pilots. As illustrated in Figure 4-4, a single tail rotor output pinion transfers power from the main transmission planetary ring gear to the tail rotor drive shaft. In addition to providing power for the tail rotor, this pinion supplies power for the accessory gears to the primary hydraulic pump and two electric generators. A failure of this one pinion results not only in immediate loss of the tail rotor thrust, but also in loss of primary hydraulic power and generators, requiring immediate crew response to safely land the aircraft.

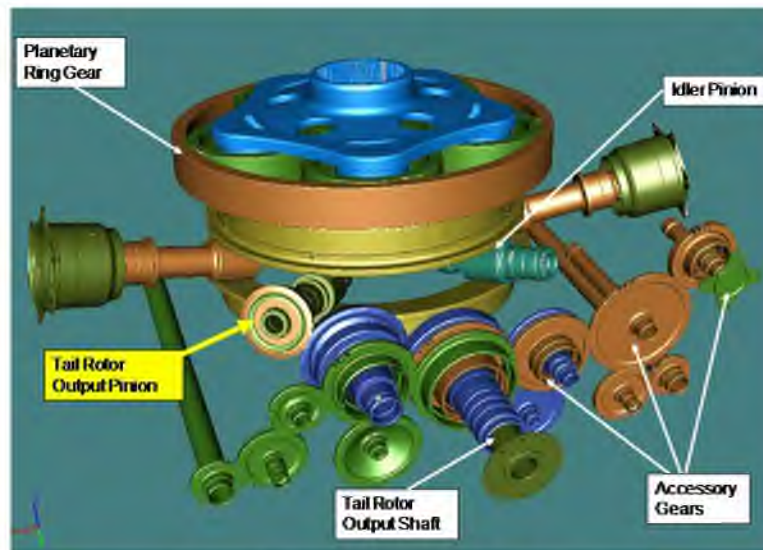


Figure 4-4. AB3 Transmission Design

During initial flight training at Boeing's plant in Mesa, Arizona, an early prototype design of the tail rotor output pinion failed as pilots were in a 5-foot hover. By landing immediately, the pilots were able to survive the landing with no damage to themselves or the aircraft even though they spiraled to the ground with no hydraulic, electrical, or tail rotor thrust. Subsequent to this incident, the AB3 program redesigned and replaced the tail rotor output pinion with a sturdier design that demonstrated in its first 200 hours of bench testing that it did not show signs of wear as had the prototype pinion design.

AB3 crews remain concerned with the single pinion design notwithstanding the redesign of the tail rotor output pinion. Prior to the failure of the prototype pinion, Boeing transmission engineers estimated that the probability of a tail rotor output pinion failure was remote (probability of occurrence in the life of the transmission is 10^{-9}). The probability of a failure of the new tail rotor pinion is also characterized as remote (10^{-9}), but the credibility of those estimates is suspect since there already has been one failure.

To experienced Apache pilots, the single tail rotor output pinion represents a loss of redundant capability inherent to legacy Apache transmission designs and creates an avoidable single point of failure. The legacy transmission has an output pinion that drives the tail rotor and accessory gearbox and a second pinion that provides redundant power to the accessory gearbox. AB3 engineers explain that the change from two pinions to one is based on a proven design in use by the Army's MH-6 and AH-6 Little Bird lift/attack aircraft. Other than these aircraft, we know of no other medium helicopter in use by the Department of Defense that has a similar design in which the failure of a single tail rotor pinion results in the simultaneous loss of tail rotor, primary hydraulics, and electrical power. Concern about the viability of the single tail rotor output pinion design is supported by evidence that multiple legacy Apache transmissions have suffered the failure of the output pinion that drives the accessory gearbox. The redundant design of the legacy transmission has prevented the simultaneous loss of tail rotor thrust, hydraulics, and electrical power, and no catastrophic loss of legacy aircraft has been chargeable to the dual pinion design. The Army should address pilot concerns about the transmission design by conducting an independent physics of failure analysis of the probability of failure of the new tail rotor pinion design, and should investigate the feasibility of alternate transmission designs that provide automatic redundant hydraulic and electric power in the event of power loss to the tail rotor.

Mission Planning – Removable Memory Module

The AB3 mission data loading and data retrieval process is not as flexible and is more time-consuming than the legacy system. Legacy Apache aircraft use one memory card to load and record mission data and another memory device to record cockpit video. The legacy mission card can be loaded or removed from inside the cockpit, making it possible for crews to quickly share mission loads between aircraft or change mission cards. Removing the video recording device from legacy aircraft in mid-mission does not compromise the mission data card. AB3 pilots were not satisfied to learn that the mission data loading and recording flexibility inherent in legacy aircraft was not retained in the AB3 design.

The consolidation of all mission planning and recorded cockpit video onto a single Removable Memory Module (RMM) resulted in new operational restrictions and a loss of existing capability. As illustrated in Figure 4-5, the RMM must be loaded and unloaded from the aft avionics bay to transfer mission planning data (maps, flight routes, target lists, waypoints, operational graphics, frequencies, etc.) onto the aircraft before each mission. During the mission, the RMM records cockpit video and audio and updates mission planning data as the mission progresses. At mission completion or during refueling, the unit removes the RMM to review the cockpit video.

During IOT&E, pilots had difficulty loading and retrieving mission data from the RMM. The RMM requires special non-standard cables for connection to the mission planning system and to download the data. At times, pilots were not able to properly format the RMM or load the data onto the aircraft. The video files can be very large and can take from 30 to 60 minutes to download from the RMM because of the format chosen for the video files. If the RMM is removed from the aircraft for any reason, mission data that has changed since mission initiation no longer resides on the aircraft. A replacement RMM will not contain the updated mission data. The Army should redesign the RMM and restore the capability to simultaneously retain updated mission data and download recorded mission data. Video files should have more efficient formats and interfaces with planning systems improved.



Figure 4-5. Removable Memory Module in Aft Avionics Bay

Mission Data Capacity

The AB3 has less capability for storing targets, waypoints, and control measures compared to legacy aircraft. In AB2 aircraft, pilots can store 1,000 targets, waypoints, or control measures on the aircraft. AB3 aircraft and mission planning software limit the AB3 to 50 targets, 50 waypoints, and 50 control measures. During training and the IOT&E, pilots found that this limitation degraded their ability to share situational awareness, identify and engage targets, and conduct reliefs-on-station. With a small number of targets, multiple aircraft often assigned the same target number to different targets. When sharing that information between aircraft, the sending aircraft would overwrite the data on the receiving aircraft. With more target numbers to choose from, units can allocate blocks of control measures to each aircraft to avoid this problem. The Army should increase the number of available targets, waypoints, and control measures for mission planning and execution.

Human Factors

AB3 Helmet

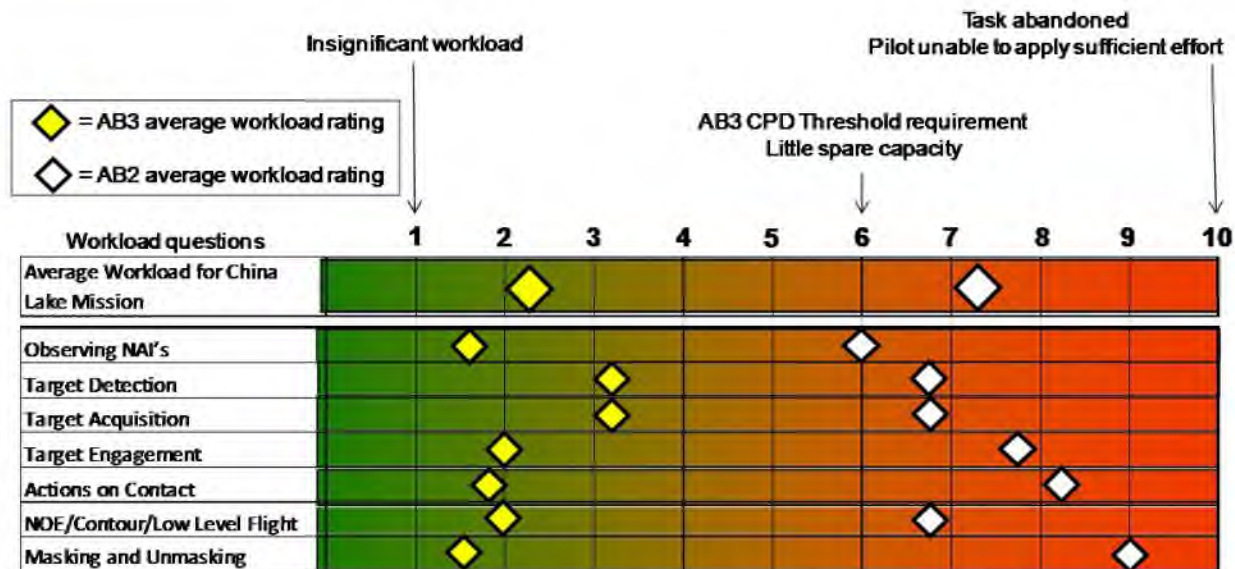
AB3 helmet comfort and performance have improved over the legacy helmet. The heads-up display projects flight-critical information such as heading, speed, engine performance, and altitude in front of the pilot's eye, making it unnecessary for the pilot to look inside the cockpit for piloting information. IOT&E pilots reported that the new helmet provides better comfort, boresight accuracy, tracking performance, and reliability than legacy Apache helmets.

The AB3 helmet has improved since it was tested in the LUT before Milestone C. At that time, the AB3 helmet did not fit well and limited visibility of the heads-up display. In post-mission questionnaires, LUT pilots indicated that the heads-up display or its cable frequently struck their right shoulder, the restraint harness, and the seat back. Pilots also noted/observed the heads-up display sight picture was partially obstructed. Portions of the heading tape, torque indicator, or the altimeter reading were not visible at all times. In response to these problems, the AB3 program redesigned the helmet. IOT&E pilots did not observe these problems and were uniformly enthusiastic about helmet comfort, performance, and reliability.

The new helmet visor design is not compatible with the expected operational environment. The helmet visor is flimsy and two assemblies cracked during the IOT&E. At dawn or dusk, day and night visors must be switched out. Various thumb screws, spacers, and retaining nuts make it difficult to change visors in flight with gloves. When not flying, pilots store helmets with visors attached in helmet bags that do not provide dedicated protection to the visors. Pilots reported difficulty mounting the visor on the helmet, even when not in flight.

Workload

AB3 pilot workload was low to moderate for flight and mission tasks throughout operational testing and met workload requirements. Pilots rated their workload on the Bedford Workload Scale from level 1 (insignificant workload) to level 10 (the task was abandoned because the pilot was unable to apply sufficient effort). Average workload ratings during IOT&E were well below the maximum allowable workload limit (6) for missions with UAS (2.1) and without UAS (2.0). These low mission workload ratings illustrate that the AB3 crews experienced a manageable workload while operating the aircraft and communicating/controlling the UAS, and were typically able to focus their effort on finding and engaging enemy forces while maneuvering to avoid enemy fire and other aircraft. The highest average workload rating for any mission was 4.5 and there were no significant workload differences between different AB3 configurations or between the front seat and back seat of the aircraft. Pilots reported higher workload when communications failed, when the UAS data link was lost, when survivability equipment declared false alarms, and when the Fire Control Radar failed to detect targets.



Based on four AB3 and four AB2 crewmember responses per question on a Bedford workload rating scale.

Figure 4-6. Workload Comparison: Interdiction Attack Mission to China Lake

AB3 pilots reported significantly lower workload than AB2 pilots during the interdiction attack mission to China Lake. Because of the high density altitude and turbulent wind at the objective, AB2 crews operated near 100 percent torque, requiring pilots to constantly monitor torque settings while continuing to maneuver at low levels among craggy peaks in turbulent air while searching for threat targets and avoiding other aircraft. As illustrated in Figure 4-6 by the white icons, AB2 workload ratings for this mission were high and well above the workload threshold for AB3. In contrast, the AB3 operated at about 65 percent torque throughout this mission. Having no concerns about exceeding torque limits, AB3 pilots were able to remain hidden by maneuvering close to the terrain and had enough spare workload capacity to assist with other critical mission tasks. Workload ratings for AB3 crews are shown in Figure 4-6 by the yellow icons.

Safety

No health hazards to the aircrew or maintainers were identified beyond those normally associated with aviation operations. Flight safety was enhanced by the increased power margin when compared to the AB2. During the China Lake mission, the AB3 was able to maintain a stable hover in spite of high altitudes, high temperatures, and gusty winds with plenty of power margin to recover from in-flight emergencies when the AB2 could not. Additionally, AB3 aircraft are certified to file an instrument flight plan, allowing AB3 crews to plan flights into or through clouds and expanding their operational envelope. Legacy Apache aircraft cannot intentionally fly into clouds and must execute emergency procedures if they suddenly find themselves in a cloud or fog.

Section Five Survivability

The AB3 is at least as survivable as the AB2. AB3 retains infrared countermeasure effectiveness and ballistic protection of legacy Apache aircraft.⁵ New AB3 subsystems met Key Performance Parameter (KPP) survivability requirements for continued safe operation (no forced landing) for at least 30 minutes after damage from a single hit by threshold projectiles, ballistic tolerance in the main rotor and drive components and required probability of successfully surviving all Band IV man-portable air defense systems (MANPADS) infrared (IR) missile engagements by preventing successful lock-on or causing missile to miss.⁶ The aircraft demonstrated ballistic tolerance similar to the legacy Apache aircraft. The Army should perform a structural analysis of the composite main rotor blade (CMRB) to better understand the load carrying capabilities of the blade that was damaged during ballistic testing. Vulnerability analyses indicate that AB3 is less vulnerable than AB2 aircraft. Improved hover performance and teaming with unmanned aircraft enable AB3 to employ tactics and maintain standoff that improves survivability. Infrared countermeasures provide protection against most man-portable rocket system threats, but the laser and radar warning systems should be replaced with more capable warning systems. The Army should integrate more capable threat warning systems onto AB3 in anticipation of future threats, upgrade radar and laser warning systems, provide for adjustable volume controls for each warning system, and employ appropriate tactics and reduce infrared signature to improve protection against advanced infrared missile threats. The AB3 is vulnerable to computer network attack. The Army should address the Information Assurance vulnerabilities. Details on the LFT&E program, the survivability assessment, and Information Assurance findings are included in the classified annex.

Countermeasure Effectiveness

Infrared Countermeasures

AB3 meets the infrared countermeasure KPP requirement against all but the most advanced MANPADS threats. This conclusion is supported by a hardware-in-the-loop simulation to evaluate the susceptibility of the AB3 at various flight speeds, atmospheric conditions, and engagement geometries. The Army's simulation facility employed actual threat missile seekers integrated with measured AB3 in-flight infrared signatures. The simulation replicates threat missile launch detection by the Common Missile Warning System, dispense of flare countermeasures, and threat response to the countermeasures. Additionally, some of the AB3 flight profiles (e.g., 500-foot hover) are tactically unsound and are unlikely to occur in combat. The results of the simulation indicate that the AB3 achieves the KPP threshold for all but the most advanced MANPADS threat. Susceptibility to the advanced threat can be mitigated

⁵ DOT&E reported on the AN/AAR-57 Common Missile Warning System (CMWS) IOT&E in April 2006. The system was found to be operationally effective and suitable for combat operations in Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF) as integrated on the CH-47, UH-60, and C-12 series aircraft. CMWS performance on AB3 is similar to the performance on these other Army platforms.

⁶ See classified annex for details.

by the use of appropriate tactics and reduction of the AB3 infrared signature. The Army already employs an optional exhaust suppressor for legacy Apache aircraft that could be installed on AB3. Additional details on this analysis are in the classified annex.

Electronic Countermeasures

The APR-39A(V)4 radar warning receiver was not effective during IOT&E. Radar warning receiver performance in IOT&E was consistent with its history of performance deficiencies, which has included inaccurate threat identification, poor reliability, and high false alarm rates. False alarms were so pervasive during the IOT&E that the pilots ignored or turned off the APR-39. The APR-39 caused two missions failures and one mission abort. Poor performance and reliability of the APR-39A(V)4 and its older variants have been observed on other helicopter platforms including the CH-47F, the UH- 60M, MV-22, and legacy Apache aircraft.

The integrated volume control for all threat warning systems decreased the overall effectiveness of AB3 aircraft survivability equipment. In the AB3, the volume of all audible threat warnings is controlled by a single knob. Because of the excessive false alarm rate of the APR-39, AB3 pilots turned down the volume of all warning systems, including warnings from trusted threat warning systems. Post-mission review of cockpit video confirms that during IOT&E training, pilots received but ignored multiple valid warnings from the laser warning receiver and missile warning receiver. The consolidation of all volume controls has degraded the effectiveness of all AB3 threat warning systems.

The AN/AVR-2A Laser Warning Receiver demonstrated in developmental and operational testing that it can detect laser threat systems, including laser rangefinders, laser designators and laser beamriders. During IOT&E training, pilots received multiple audible warnings of an active beam-rider threat, but the pilots ignored the warnings. Improved laser warning systems have already been developed and fielded, such as the AN/AVR-2B. To provide better protection against laser threats, the Army should equip AB3 with one of the newer warning systems that has been proven to be more effective, more reliable, smaller and lighter, requiring less power.

The performance of the AN/ALQ-136(V)5 radar jammer was not demonstrated during the IOT&E because the Army was not able to obtain the clearance to conduct active jamming. AB3 was equipped with a radar jammer to defeat or degrade the tracking capabilities of hostile pulsed radars. The radar jammer was operated during IOT&E in the training (no active jamming) mode and passed system self-test and gave indications that the system was functional.

Vulnerability

Information Assurance

The AB3 is vulnerable to computer network attack. The computer network red team discovered threat vectors by which AB3 computer information could be compromised, corrupted, or exploited. The classified annex of this report contains a more detailed discussion of the vulnerabilities and recommended actions.

Vulnerability Analysis

Vulnerability analysis indicates that the AB3 retains low vulnerability to small-caliber threats and is slightly less vulnerable (i.e., slightly better) than the AB2. The vulnerability analysis compared the overall system-level vulnerability of AB3 to the AB2.

The vulnerability analysis model indicates that the AB3 performs at least as well as the AB2 for the user specified KPPs for ballistic survivability and force protection. There are two KPPs for ballistic survivability and two KPPs for force protection, as shown in Table 5-1. The first KPP specifies an overall system-level ballistic tolerance capability. Model results suggest that the probability of being able to operate for at least 30 minutes after damage from the specified system-level threat is very high for both the AB3 and AB2. The model determined that there was small amount of vulnerable area for the flight controls, propulsion, and rotors against the KPP threat.

For the second KPP in Table 5-1, the model suggests that vulnerable area for the main rotor drive and rotor components for the AB3 was marginally lower (better) compared to the AB2. This KPP considers the vulnerable area for abort, meaning that it includes any ballistic damage that would cause pilots to abort a mission. Modeling results indicated that the vulnerable areas for AB3 and AB2 exceeded the requirement, and that the estimated vulnerability is primarily associated with oil coolant lines in the main transmission. Ballistic damage to these lines could result in an oil leak, causing loss of lubricant and a subsequent mission abort. Loss of lubricant is not expected to result in attrition or forced landing because the main transmission is capable of running for 30 minute in a fluid depleted state.

Ballistic tests for the crew armor confirmed that it is effective at stopping the threat, meeting the force protection KPP. This KPP relates to protection of the crew afforded by the crew armor. The vulnerability analysis model considered shots that impact the bottom hemisphere of the aircraft. The armor was modeled to be capable of stopping all impacting rounds. The model indicates that the AB3 and AB2 have comparable crew survivability.

For the last KPP, the transparent barrier between the crew is the same as that installed on the legacy aircraft and has been shown in previous testing to be capable of meeting the criteria specified in the KPP. The purpose of this KPP is to ensure that both crewmembers would not be incapacitated if engaged by the specified threat.

Table 5-1. Summary of Modeling Results for AB3 Ballistic Survivability KPPs

Ballistic Survivability KPP*	Description of Results
The AB3 should be capable of continued safe operation (no forced landing) for at least 30 minutes after damage from the threat projectile.	AB3 performed similar to the AB2 against the specified threat; both met this requirement for most (but not all) shotlines. Primary contributors to vulnerable area were flight controls, propulsion, and rotors.
Damage to main rotor drive components and rotor blades from the threat projectile must not exceed the specified vulnerable area.	The vulnerable area for the main rotor drive and rotor components for AB3 was marginally lower (better) compared to the AB2.
Armor or equivalent protection against threat projectiles within the bottom hemisphere of the crew position while the aircraft is in a level flight attitude.	AB3 armor is effective at stopping the specified threat, but the airframe structure and other intervening components do not provide complete (100 percent) protection.
A transparent armor barrier will be installed between the two crew members that precludes incapacitation of both crewmembers from the threat projectile.	In prior legacy aircraft ballistic testing, the transparent protective barrier between the pilots demonstrated the capability to stop most specified threat projectile fragments without bulging, stretching, or cracking.

* See classified annex for details.

Improved Drive System

The Army conducted ballistic testing of the AB3 improved drive system (IDS) from May to July 2011 at Aberdeen Proving Ground, Maryland. The tests included two dynamic shots against the engine nose gearbox and main transmission, followed by 20 static shots against the main transmission and main rotor drive shaft. There were four test phases, as described in Table 5-2.

Table 5-2. Summary of Ballistic Tests on the AB3 Improved Drive System

Phase	Component	Test Setup and Execution
1 (1 shot)	Engine Nose Gearbox	Dynamic test using the left engine nose gearbox installed on an AB3 representative aircraft, with a single shot into the roller bearing followed by 30 minutes of operation at flight-representative loading conditions (95 percent dual engine torque).
2 (1 shot)	Main Transmission	Dynamic test using the main transmission as installed on the AB3 representative aircraft, with a single shot into the upper face gear followed by 30 minutes of operation at flight-representative loading conditions (95 percent dual engine torque).
4 (14 shots)	Main Transmission	Static tests involving 14 shots against the main transmission secured in a test stand. The shots ballistically impacted a variety of components (e.g., gears, bearings, etc.).

For the two dynamic tests, the Army conducted ballistic testing against a fully-functional AH-64D Longbow Apache ground test vehicle equipped with the legacy AH-64D metal rotor blades, the new AB3 IDS, and new 701D engines. The legacy metal blades were used instead of the new composite main rotor blade (CMRB) in order to save the newer blades for later ballistic

testing; the use of the metal blades had no impact on the dynamic testing of the IDS components. During the dynamic tests, the engines were running and rotors turning at load levels representative of AB3 in-flight operations. The Army established a 30-minute post-shot operating schedule to be representative of an AB3 helicopter operating under ambient conditions of 6,000 feet pressure altitude and 95 degrees Fahrenheit, at a gross weight of 16,000 pounds. The 30-minute operating schedule involved a hover out of ground effect at 95 percent torque prior to ballistic impact, followed by two minutes of evasive maneuvers at 100 percent torque after ballistic impact, followed by level flight at 80 to 100 knots at 50 to 60 percent torque for 23 minutes, followed by a 5-minute roll-on landing at 40 to 60 knots at 30 percent torque.

With input from DOT&E staff, the Army used modeling and engineering judgment to select the shotlines and impact conditions for the ballistic shots. Consideration was given to the criticality and accessibility (i.e., direct line of sight) of the targeted components. For the dynamic test on the engine nose gearbox, the shotline intersected the roller bearing. For the main transmission dynamic shot, the upper face gear was the critical impact location.

During dynamic testing, the engine nose gearbox and main transmission completed the 30-minute post-shot operating schedule following impact from the KPP threat. Both subsystems demonstrated the capability to operate for 30 minutes after the shot in a fluid-depleted state despite the presence of metal fragments. This result was consistent with the capabilities demonstrated during prior oil-out testing for the engine nose gearbox and main transmission; both systems proved capable of operating for 30 minutes after being drained of lubricating fluid. Neither subsystem experienced a jam or loss of functionality after the shot, but in both tests, loss of oil caused the low oil pressure warning light to activate in the cockpit. This warning signal instructs the pilots to take precautionary procedures to continue to safely operate the aircraft and return to base as soon as practical. The main transmission also activated the metallic chip detection warning light. For this warning, the AH-64D operator's manual advises pilots to land as soon as possible without delay prior to returning to base.

Because the AB3 has two engine nose gearboxes, loss of one engine nose gearbox would most likely result in a mission abort rather than attrition or forced landing. The failed engine nose gearboxes would no longer be capable of providing input to the main transmission for the engine. Fortunately, the main transmission has an overrunning clutch that allows the main transmission to continue operating if one of the two engine nose gearboxes or engines fails.

The AB3 has only one main transmission; disabling it would result in an inability to drive the main rotor. However, if the main transmission were to jam, the main rotor drive shaft incorporates a shear section that is designed to break so that the main rotor will continue turning, providing pilots with the opportunity to initiate an auto-rotational descent landing.

Composite Main Rotor Blades (CMRBs)

The Army conducted ballistic testing of the AB3 CMRB from May to July 2011 at Aberdeen Proving Ground, Maryland. The tests consisted of eight events as described in Table 5-3. The two dynamic shots were against a fully functional AH-64D Longbow Apache equipped with a full set of CMRBs, the new AB3 IDS, and new 701D engines.

Table 5-3. Summary of Ballistic Tests on the AB3 CMRB

Phase	Component	Test Setup and Execution
1 (2 shots)	Full CMRB	Dynamic shots against the full CMRB operating at flight representative load levels on an AB3 representative aircraft with blade turning during the shots.
2 (6 shot)	CMRB blade segments	Static shots against undamaged 4-foot blade segments cut from previously shot blades restrained in test fixtures.

During dynamic testing, the CMRB demonstrated the capability to withstand a single hit from selected threats and meet its post-shot 30-minute get home capability. The CMRB has very low vulnerability to most small arms threats. However, larger threats directed at the blade spar proved to be the most stressing. A larger threat impacted the blade spar on the second dynamic shot and removed a substantial portion of the spar's cross-sectional area. The blade completed 30-minutes of operation, despite a loss of structural flapwise stiffness. While spinning, the centrifugal forces kept the blade aloft, but on the last revolution, the blade folded downward and struck the left side of the tail boom. It is unclear if the observed damage would have resulted in catastrophic blade failure within 30 minutes under actual flight conditions. It is also unclear if equivalent damage located at another span location would have resulted in the same outcome. Consequently, to obtain a better understanding of the results of this testing, the Army should conduct a structural analysis of the blade damaged during the second dynamic test and apply the results to the load limits that are expected under various flight operations conditions and at various spanwise locations.

Each of the dynamic shots resulted in a measureable increase in the helicopter post-shot vibrations. These vibrations did not cause airframe damage and were well below the vibration limit specified in rotor track and balance procedures to avoid flying the aircraft. If pilots felt a noticeable increase in vibration levels, they would most likely land the aircraft as soon as practical.

Crew Armor

In response to the unavailability of the armor material for the Apache from the original manufacturer, the Army initiated an alternative, but very similar, materiel qualification effort to replace currently fielded, externally mounted, airframe armor that has been damaged in combat or become worn as a result of normal use. The new armor panels are also being installed on the AB3 (five on each side of the airframe) around the pilot and copilot/gunner cockpit area, as highlighted in yellow in Figure 5-1. The seat armor, shaded in blue, remains the same as that installed on the legacy aircraft.

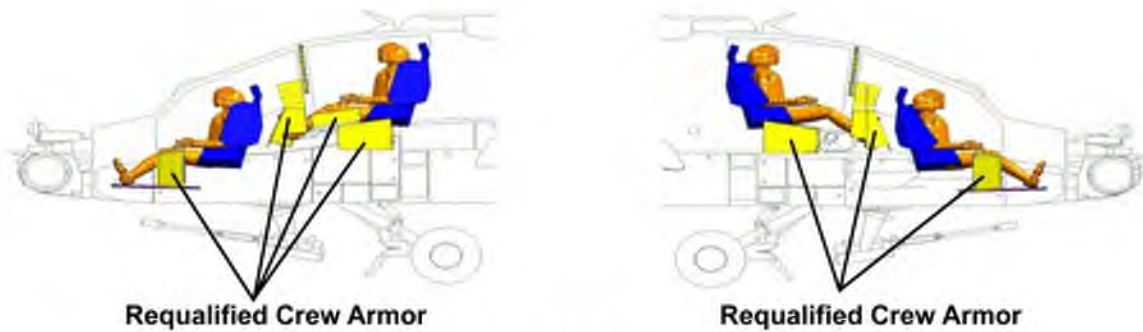


Figure 5-1. AB3 Crew Armor

The new vendor selected in the qualification effort provided an alternate armor solution that passed the Army's initial qualification tests in 2010 against a 0.50 caliber round. To address questions about armor performance against the higher energy KPP threat, the Army tested an additional 20 panels on December 7, 2010 against the KPP threat. With the addition of just 10 pounds, the new airframe crew armor material shows dramatic improvement in the ballistic protection capability over the legacy system. The classified annex of this report presents a more detailed discussion of this test.

This page intentionally left blank.

Section Six Recommendations

The Army should consider the following recommendations and should verify the corrections to deficiencies in follow-on test and evaluation.

- Continue to refine tactics, techniques, and procedures for teaming with unmanned aircraft.
- Address pilot concerns about the transmission design. Conduct physics of failure analysis to provide an independent analysis of the probability of failure of the new tail rotor pinion design. Investigate the feasibility of alternate transmission designs that provide automatic redundant hydraulic and electrical power in the event of loss of power to the tail rotor.
- Redesign the Removable Memory Module and restore the capability to simultaneously retain updated mission data and download recorded mission data. Video files should have more efficient formats and interfaces with planning systems improved.
- Increase the number of available targets, waypoints, and control measures for mission planning and execution.
- Determine the root cause for data link dropouts and improve the stability of the tactical command data link for control of unmanned aircraft sensors.
- Consider incorporating improvements to current threat warning systems as they are developed. Upgrade radar and laser warning systems and provide for adjustable volume controls for each warning system. Employ appropriate tactics and reduce infrared signature to improve protection against advanced infrared missile threats.
- Perform a structural analysis of the CMRB to better understand the load carrying capabilities of the blade that was damaged during ballistic testing
- Address the Information Assurance vulnerabilities identified.
- Develop instrumentation for future training and testing to allow real-time adjudication of manned-unmanned engagements.



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

AUG 20 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

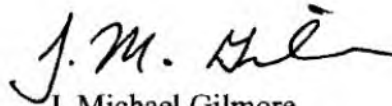
(U) I have enclosed at TAB A the Combined Operational and Live Fire Test and Evaluation Report on the AH-64D Apache Block III (AB3) Attack Helicopter, required by Sections 2399 and 2366 of Title 10 United States Code. Enclosed at TAB B is the classified annex to this report, which discusses my evaluation of the helicopter's survivability in detail. In the report, I conclude the following:

- (U) The AB3 is operationally effective. It has improved flight performance compared to legacy Apache aircraft, and, when aided by real-time unmanned aircraft system (UAS) video containing actionable intelligence, AB3 teams demonstrated greater target acquisition ranges, greater Hellfire engagement ranges, and the potential for greater mission success than Apache Block II (AB2) teams.
- (U) AB3 is operationally suitable. The helicopter exceeded its reliability thresholds with statistical confidence and met all current maintainability requirements. The redesigned Apache helmet offers improved comfort and performance compared to the legacy helmet. Overall, flight safety is enhanced by AB3's increased power margins relative to AB2.
- (U) The AB3 is at least as survivable as the legacy AB2. New AB3 subsystems met survivability requirements and demonstrated ballistic tolerance similar to legacy Apache aircraft. AB3 retains the infrared countermeasures effectiveness of AB2.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the

[REDACTED]

Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosures:
As stated

cc:
The Honorable Adam Smith
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

AUG 20 2012

The Honorable C. W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

Dear Mr. Chairman:

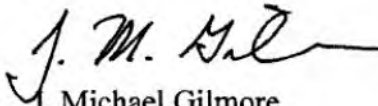
(U) I have enclosed at TAB A the Combined Operational and Live Fire Test and Evaluation Report on the AH-64D Apache Block III (AB3) Attack Helicopter, required by Sections 2399 and 2366 of Title 10 United States Code. Enclosed at TAB B is the classified annex to this report, which discusses my evaluation of the helicopter's survivability in detail. In the report, I conclude the following:

- (U) The AB3 is operationally effective. It has improved flight performance compared to legacy Apache aircraft, and, when aided by real-time unmanned aircraft system (UAS) video containing actionable intelligence, AB3 teams demonstrated greater target acquisition ranges, greater Hellfire engagement ranges, and the potential for greater mission success than Apache Block II (AB2) teams.
- (U) AB3 is operationally suitable. The helicopter exceeded its reliability thresholds with statistical confidence and met all current maintainability requirements. The redesigned Apache helmet offers improved comfort and performance compared to the legacy helmet. Overall, flight safety is enhanced by AB3's increased power margins relative to AB2.
- (U) The AB3 is at least as survivable as the legacy AB2. New AB3 subsystems met survivability requirements and demonstrated ballistic tolerance similar to legacy Apache aircraft. AB3 retains the infrared countermeasures effectiveness of AB2.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the

[REDACTED]

Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosures:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

AUG 20 2012

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

Dear Mr. Chairman:

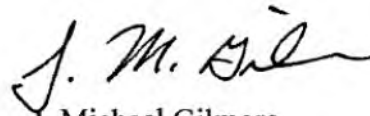
(U) I have enclosed at TAB A the Combined Operational and Live Fire Test and Evaluation Report on the AH-64D Apache Block III (AB3) Attack Helicopter, required by Sections 2399 and 2366 of Title 10 United States Code. Enclosed at TAB B is the classified annex to this report, which discusses my evaluation of the helicopter's survivability in detail. In the report, I conclude the following:

- (U) The AB3 is operationally effective. It has improved flight performance compared to legacy Apache aircraft, and, when aided by real-time unmanned aircraft system (UAS) video containing actionable intelligence, AB3 teams demonstrated greater target acquisition ranges, greater Hellfire engagement ranges, and the potential for greater mission success than Apache Block II (AB2) teams.
- (U) AB3 is operationally suitable. The helicopter exceeded its reliability thresholds with statistical confidence and met all current maintainability requirements. The redesigned Apache helmet offers improved comfort and performance compared to the legacy helmet. Overall, flight safety is enhanced by AB3's increased power margins relative to AB2.
- (U) The AB3 is at least as survivable as the legacy AB2. New AB3 subsystems met survivability requirements and demonstrated ballistic tolerance similar to legacy Apache aircraft. AB3 retains the infrared countermeasures effectiveness of AB2.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the

[REDACTED]

Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosures:
As stated

cc:
The Honorable John McCain
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

AUG 20 2012

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-602

Dear Mr. Chairman:

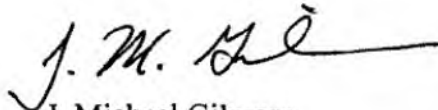
(U) I have enclosed at TAB A the Combined Operational and Live Fire Test and Evaluation Report on the AH-64D Apache Block III (AB3) Attack Helicopter, required by Sections 2399 and 2366 of Title 10 United States Code. Enclosed at TAB B is the classified annex to this report, which discusses my evaluation of the helicopter's survivability in detail. In the report, I conclude the following:

- (U) The AB3 is operationally effective. It has improved flight performance compared to legacy Apache aircraft, and, when aided by real-time unmanned aircraft system (UAS) video containing actionable intelligence, AB3 teams demonstrated greater target acquisition ranges, greater Hellfire engagement ranges, and the potential for greater mission success than Apache Block II (AB2) teams.
- (U) AB3 is operationally suitable. The helicopter exceeded its reliability thresholds with statistical confidence and met all current maintainability requirements. The redesigned Apache helmet offers improved comfort and performance compared to the legacy helmet. Overall, flight safety is enhanced by AB3's increased power margins relative to AB2.
- (U) The AB3 is at least as survivable as the legacy AB2. New AB3 subsystems met survivability requirements and demonstrated ballistic tolerance similar to legacy Apache aircraft. AB3 retains the infrared countermeasures effectiveness of AB2.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the

[REDACTED]

Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosures:
As stated

cc:
The Honorable Thad Cochran
Ranking Member



OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JUL 23 2012

The Honorable C.W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

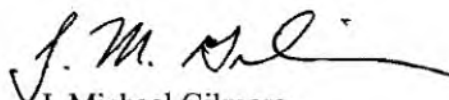
Dear Mr. Chairman:

(U) I have enclosed my report on the Navy MK XIIA Mode 5 Identification Friend or Foe (IFF) system as required by Sections 2399 and 2366, Title 10, United States Code.

(U) The paucity of data collected during severely truncated operational testing makes it impossible to fully assess Mode 5 IFF effectiveness under realistic conditions. Poor weather greatly truncated testing. The data that were obtained are sufficient to assess only the performance of the individual interrogator and transponder used in the Navy Mode 5 system under a limited set of conditions. In the truncated test, the interrogators and transponders functioned correctly. However, problems with their integration within the Navy's Aegis system were identified that could cause incorrect engagement decisions with potentially severe consequences. Substantial additional testing is required to assess the performance of Mode 5 interoperating with the full complement of the Department's existing and planned IFF systems. The next opportunity to conduct that testing is now planned for the third quarter of fiscal year 2013.

(U) I am unable to fully assess the Mode 5 system's suitability due to the truncated test. Although no hardware or software failures occurred, important deficiencies were observed including short battery life, anti-tamper features that can be triggered much too easily, and difficulty in loading cryptographic keys.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Secretary of the Army; the Secretary of the Navy; the Secretary of the Air Force; the Under Secretary of Defense for Acquisition, Technology and Logistics; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable Norman D. Dicks
Ranking Member





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JUL 23 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

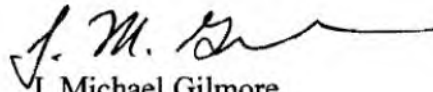
Dear Mr. Chairman:

(U) I have enclosed my report on the Navy MK XIIA Mode 5 Identification Friend or Foe (IFF) system as required by Sections 2399 and 2366, Title 10, United States Code.

(U) The paucity of data collected during severely truncated operational testing makes it impossible to fully assess Mode 5 IFF effectiveness under realistic conditions. Poor weather greatly truncated testing. The data that were obtained are sufficient to assess only the performance of the individual interrogator and transponder used in the Navy Mode 5 system under a limited set of conditions. In the truncated test, the interrogators and transponders functioned correctly. However, problems with their integration within the Navy's Aegis system were identified that could cause incorrect engagement decisions with potentially severe consequences. Substantial additional testing is required to assess the performance of Mode 5 interoperating with the full complement of the Department's existing and planned IFF systems. The next opportunity to conduct that testing is now planned for the third quarter of fiscal year 2013.

(U) I am unable to fully assess the Mode 5 system's suitability due to the truncated test. Although no hardware or software failures occurred, important deficiencies were observed including short battery life, anti-tamper features that can be triggered much too easily, and difficulty in loading cryptographic keys.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Secretary of the Army; the Secretary of the Navy; the Secretary of the Air Force; the Under Secretary of Defense for Acquisition, Technology and Logistics; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable Adam Smith
Ranking Member





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JUL 23 2012

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

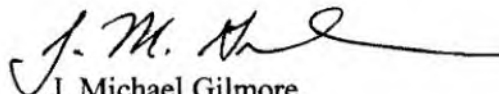
Dear Mr. Chairman:

(U) I have enclosed my report on the Navy MK XIIA Mode 5 Identification Friend or Foe (IFF) system as required by Sections 2399 and 2366, Title 10, United States Code.

(U) The paucity of data collected during severely truncated operational testing makes it impossible to fully assess Mode 5 IFF effectiveness under realistic conditions. Poor weather greatly truncated testing. The data that were obtained are sufficient to assess only the performance of the individual interrogator and transponder used in the Navy Mode 5 system under a limited set of conditions. In the truncated test, the interrogators and transponders functioned correctly. However, problems with their integration within the Navy's Aegis system were identified that could cause incorrect engagement decisions with potentially severe consequences. Substantial additional testing is required to assess the performance of Mode 5 interoperating with the full complement of the Department's existing and planned IFF systems. The next opportunity to conduct that testing is now planned for the third quarter of fiscal year 2013.

(U) I am unable to fully assess the Mode 5 system's suitability due to the truncated test. Although no hardware or software failures occurred, important deficiencies were observed including short battery life, anti-tamper features that can be triggered much too easily, and difficulty in loading cryptographic keys.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Secretary of the Army; the Secretary of the Navy; the Secretary of the Air Force; the Under Secretary of Defense for Acquisition, Technology and Logistics; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable John McCain
Ranking Member





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JUL 23 2012

OPERATIONAL TEST
AND EVALUATION

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6025

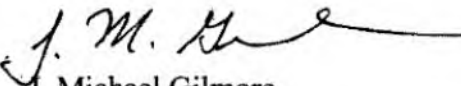
Dear Mr. Chairman:

(U) I have enclosed my report on the Navy MK XIIA Mode 5 Identification Friend or Foe (IFF) system as required by Sections 2399 and 2366, Title 10, United States Code.

(U) The paucity of data collected during severely truncated operational testing makes it impossible to fully assess Mode 5 IFF effectiveness under realistic conditions. Poor weather greatly truncated testing. The data that were obtained are sufficient to assess only the performance of the individual interrogator and transponder used in the Navy Mode 5 system under a limited set of conditions. In the truncated test, the interrogators and transponders functioned correctly. However, problems with their integration within the Navy's Aegis system were identified that could cause incorrect engagement decisions with potentially severe consequences. Substantial additional testing is required to assess the performance of Mode 5 interoperating with the full complement of the Department's existing and planned IFF systems. The next opportunity to conduct that testing is now planned for the third quarter of fiscal year 2013.

(U) I am unable to fully assess the Mode 5 system's suitability due to the truncated test. Although no hardware or software failures occurred, important deficiencies were observed including short battery life, anti-tamper features that can be triggered much too easily, and difficulty in loading cryptographic keys.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Secretary of the Army; the Secretary of the Navy; the Secretary of the Air Force; the Under Secretary of Defense for Acquisition, Technology and Logistics; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable Thad Cochran
Ranking Member



Director, Operational Test and Evaluation

**Direct Attack Moving Target Capability
(DAMTC)**

Initial Operational Test and Evaluation Report



June 2012

This report on the Direct Attack Moving Target Capability (DAMTC) fulfills the provisions of Title 10, United States Code, Section 2399. It assesses the adequacy of testing and the operational effectiveness and operational suitability of the DAMTC program.

J. Michael Gilmore
Director

The marginal cost of producing this report is estimated to be approximately \$16K. The estimated acquisition cost of the program which this report addresses is \$114M.



**Direct Attack Moving Target Capability
Laser Joint Direct Attack Munition
GBU-54/B**

Executive Summary

This document reports on the evaluation of test adequacy, operational effectiveness, and operational suitability of the Direct Attack Moving Target Capability (DAMTC) program. The evaluation is based primarily on data from the Navy's Operational Test and Evaluation Force (OPTEVFOR) and Air Test and Evaluation Squadron Nine's (VX-9) Initial Operational Test and Evaluation (IOT&E) conducted from October 2011 to April 2012. The evaluation also uses some data for assessing reliability obtained during Integrated Test (IT)-C1 that occurred between May 2010 and April 2011, and Developmental Test (DT)-C1 that occurred in August and September 2011. An Operational Assessment was conducted during IT-C1 between May and September 2010.

System Description and Mission

DAMTC uses Laser Joint Direct Attack Munition (JDAM) (GBU-54/B) with the updated Block 8 Operational Flight Program (OFP) software as its material solution for a Navy and Marine Corps dual-mode weapon capable of attacking moving as well as stationary targets.

The Navy plans to employ DAMTC's laser designation capability against moving and maneuvering targets during missions conducting Close Air Support, Strike Coordination and Armed Reconnaissance, and attacking Time Sensitive Targets.¹ When moving and maneuvering targets are not present or a higher priority stationary target is identified, the weapon may be used as a standard JDAM, providing a dual-mode weapon capability.

DAMTC provides enhanced capability compared to baseline JDAM weapons by enabling the successful engagement of both moving and maneuvering targets and eliminating Global Positioning System (GPS) Target Location Error when using precise laser designation.

Test Adequacy

The operational testing of the DAMTC was adequate to support an evaluation of the weapon's operational effectiveness and suitability. A comprehensive Live Fire Test and Evaluation program was not needed because the underlying munition upon which the Laser JDAM weapon is built (500-pound general purpose bomb body) has known lethality. However, VX-9 employed four live weapons and data from these tests validated that the estimates of lethality for JDAM contained in the Joint Munitions Effectiveness Manual (JMEM) are applicable to DAMTC.

Prior to operational test and evaluation (OT&E), Air Test and Evaluation Squadron 31 (VX-31) completed a short developmental test (DT) phase sufficient to demonstrate that the new laser sensor sapphire lens, which replaced the glass lens because of excessive deterioration in inclement weather conditions, retained the same performance characteristics as the prior material.

¹ A maneuvering target is a target that is moving but changes velocity, direction, or both during the time it is engaged.

The DAMTC Initial Operational Test and Evaluation (IOT&E) was begun in accordance with a DOT&E-approved Test and Evaluation Master Plan (TEMP) and test plan. However, after coordinating with DOT&E, VX-9 made changes during test execution on moving target profiles because of emerging operational tactics proposed by the Navy's TOPGUN School. Additionally, IT test conditions were not operationally realistic; therefore IT data on weapon effectiveness were not used in this evaluation as had been planned. Despite deviations from the approved test plan, VX-9 gathered adequate data from 22 test events to evaluate the weapon's operational effectiveness and suitability.

Operational Effectiveness

DAMTC is operationally effective against moving (non-evasive) and maneuvering (evasive) targets when employed in the self-lasing mode (that is, when the aircraft delivering the weapon uses its own laser to designate the target). Against moving but non-maneuvering targets, the median miss distance from the averaged-center of the laser spot during the last 3.5 seconds of flight was 5.8 meters and 6.4 meters from the target's geometric center. Against maneuvering targets, DAMTC demonstrated a median miss distance of 4.3 meters from the laser spot and 5.3 meters from the target center. These delivery accuracies are sufficient to assure lethal effects against the set of relatively soft targets, such as commercial vehicles, against which DAMTC will be employed.

DAMTC did not demonstrate operational effectiveness against moving and maneuvering targets when employed in the buddy-lasing mode.² DAMTC median miss distance in this mode was 24.3 meters from the laser spot and 26.3 meters from the target center. However, due to test execution issues, these large miss distances may also be due in part to range restrictions on attack headings and engagement geometries during the three buddy-lasing trials. Therefore, the operational effectiveness of DAMTC using buddy-lasing deliveries is unknown.

Operational Suitability

DAMTC is operationally suitable. During operational testing, the Laser JDAM weapon exceeded the threshold for material reliability and achieved a 100 percent pass rate in built-in test function. Evaluations of DAMTC's logistics supportability, compatibility, training program, safety, and documentation revealed no deficiencies and consistently received satisfactory (or better) survey results. Aircraft and weapon bomb body compatibility requirements were also met. Testers discovered deficiencies related to interoperability with the two newest versions of the F/A-18 aircraft software, H8E and 23X, during initial weapon power up on the ground. Also, placement of the wiring in the fuze-well physically hinders visual verification of fuze arming and function settings. Simple work-arounds such as earlier ground checks and better lighting currently exist to enable reliable mission completion until a more permanent solution is implemented. Human factors difficulties were reported by aircrew in maintaining precise laser

² Buddy-lasing is when one aircraft drops laser-guided weapons that are guided by the second aircraft's laser. This can be an effective tactic, where one aircraft can dedicate his efforts to accurate targeting and providing a stable lasing platform, while the second aircraft can focus solely on weapons delivery.

designation on a moving target throughout weapon delivery; manual tracking is necessary because the auto-track mode will easily break lock while tracking a moving target.

Recommendations

The Navy should implement the following recommendations:

Operational Effectiveness

- Conduct additional testing using buddy-lasing from rear aspect geometries to distinguish between the effects of adverse target geometry and the use of the buddy-lasing on DAMTC accuracy.

Operational Suitability

- Incorporate changes to subsequent releases of future F/A-18 aircraft software to correct interoperability deficiencies with weapon identification and selection of aircraft navigation mode.
- Re-design the wiring bundle in the weapon's tail compartment to facilitate a visual pre-flight check of the weapon's fuze settings.



J. Michael Gilmore
Director

This page intentionally left blank.

Contents

System Overview1

Test Adequacy5

Operational Effectiveness9

Operational Suitability17

Recommendations.....21

This page intentionally left blank.

Section One System Overview

This document reports on the evaluation of test adequacy, operational effectiveness, and operational suitability of the Direct Attack Moving Target Capability (DAMTC) program. The evaluation is based primarily on data from the Navy's Operational Test and Evaluation Force (OPTEVFOR) and VX-9 Squadron's Initial Operational Test and Evaluation (IOT&E) conducted from October 2011 to April 2012. The evaluation is augmented by developmental testing, including Integrated Test (IT)-C1 that occurred between May 2010 and April 2011, and Developmental Test (DT)-C1 that occurred in August and September 2011. An Operational Assessment was conducted during IT-C1 between May and September 2010.

Mission Description and Concept of Employment

The Navy plans to employ DAMTC's laser designation capability against moving and maneuvering targets during Close Air Support, Strike Coordination and Armed Reconnaissance, and Time Sensitive Target missions.³ When moving and maneuvering targets are not present or a higher priority stationary target is identified, the weapon may be used as a standard Joint Direct Attack Munition (JDAM), providing a dual-mode weapon capability.

DAMTC will be employed off of all F/A-18 variants and the AV-8B Harrier by the Navy and Marine Corps. Employment modes using laser designation include self-designation by the aircraft delivering the weapon, buddy-lasing from another aircraft, or via ground designation by a Joint Terminal Attack Controller (JTAC).⁴

System Description

DAMTC uses Laser JDAM (GBU-54/B) with the updated Block 8 Operational Flight Program (OFP) software as its material solution for a Navy and Marine Corps dual-mode weapon. This is a non-developmental program using Laser JDAM, incorporating improvements to the weapon fielded in 2008 as part of an Urgent Operational Need.

DAMTC provides enhanced capability compared to baseline JDAM weapons by enabling the successful engagement of both moving and maneuvering targets and eliminating Global Positioning System (GPS) Target Location Error when using precise laser designation. Additionally, it will enhance weapon load-out flexibility by having the capability of both a coordinate-seeking weapon and a laser-guided weapon in a single munition.

The DAMTC weapon uses the JDAM, GBU-38 variant (500-pound bomb body Mk-82), as the baseline configuration. A field-installed DSU-38/B Precision Laser Guidance Set (PLGS)

³ A maneuvering target is a target that is moving but changes velocity, direction, or both during the time it is engaged.

⁴ Buddy-lasing is when one aircraft drops laser-guided weapons that are guided by the second aircraft's laser. This can be an effective tactic, where one aircraft can dedicate his efforts to accurate targeting and providing a stable lasing platform, while the second aircraft can focus solely on weapons delivery.

kit, when added to the GBU-38, is designated as a Laser JDAM GBU-54/B as indicated in Figure 1-1. The DSU-38/B PLGS enhances the basic JDAM functionality of prosecuting preplanned fixed targets by adding the ability to execute attacks against lased fixed targets and lased moving and maneuvering targets.

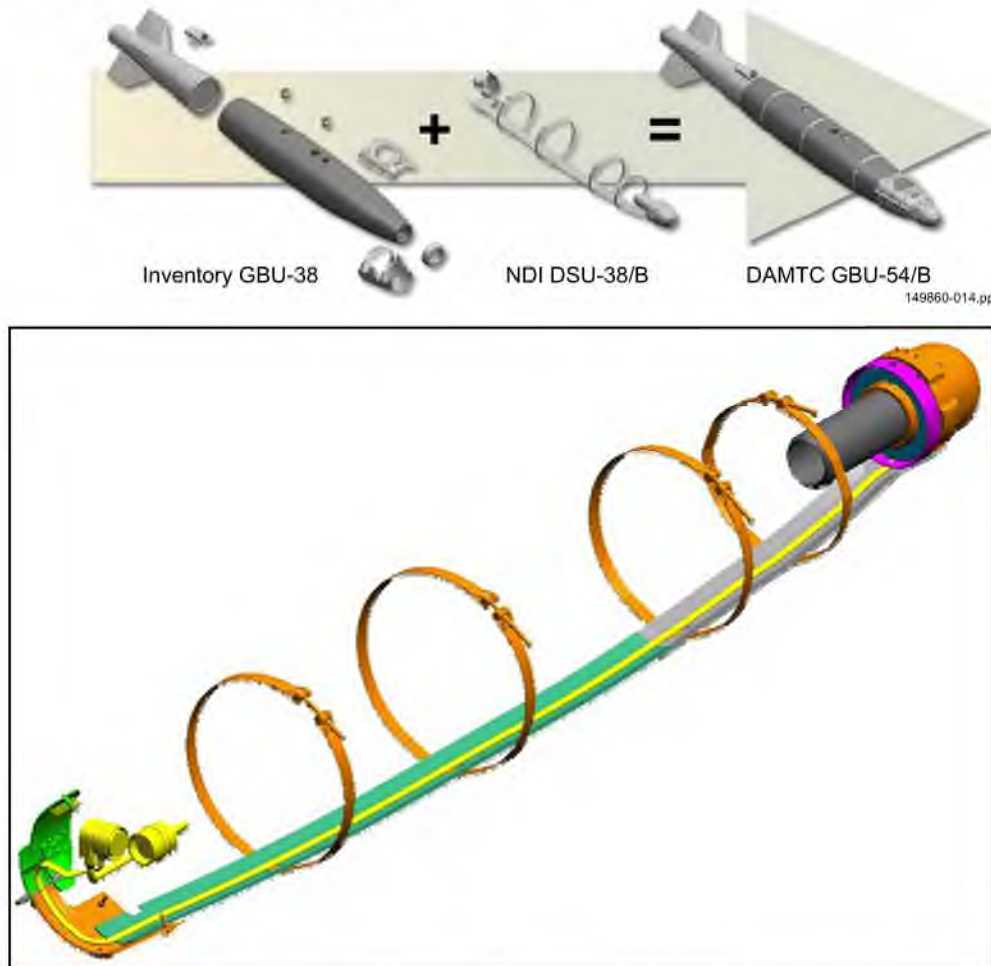


Figure 1-1. DAMTC Components

After receiving an initial target velocity and direction from the aircraft or crew, the weapon is released from inside a Launch Acceptability Region (LAR) and initially guides to calculated intercept coordinates using baseline GPS-aided Inertial Navigation System (INS) guidance. Upon receipt of laser energy, the weapon's laser sensor provides azimuth and elevation angle measurements to the weapon guidance set. The weapon guidance set uses the angle measurements, along with estimates of target velocity, to continually update the original target coordinates provided at release. During the terminal phase, the weapon transitions to proportional guidance and guides to the latest updated target coordinates in order to intercept and destroy the target. Figure 1-2 shows the relationship between the aircraft, the weapon, and the various modes to guide it to the moving target in an operational scenario.

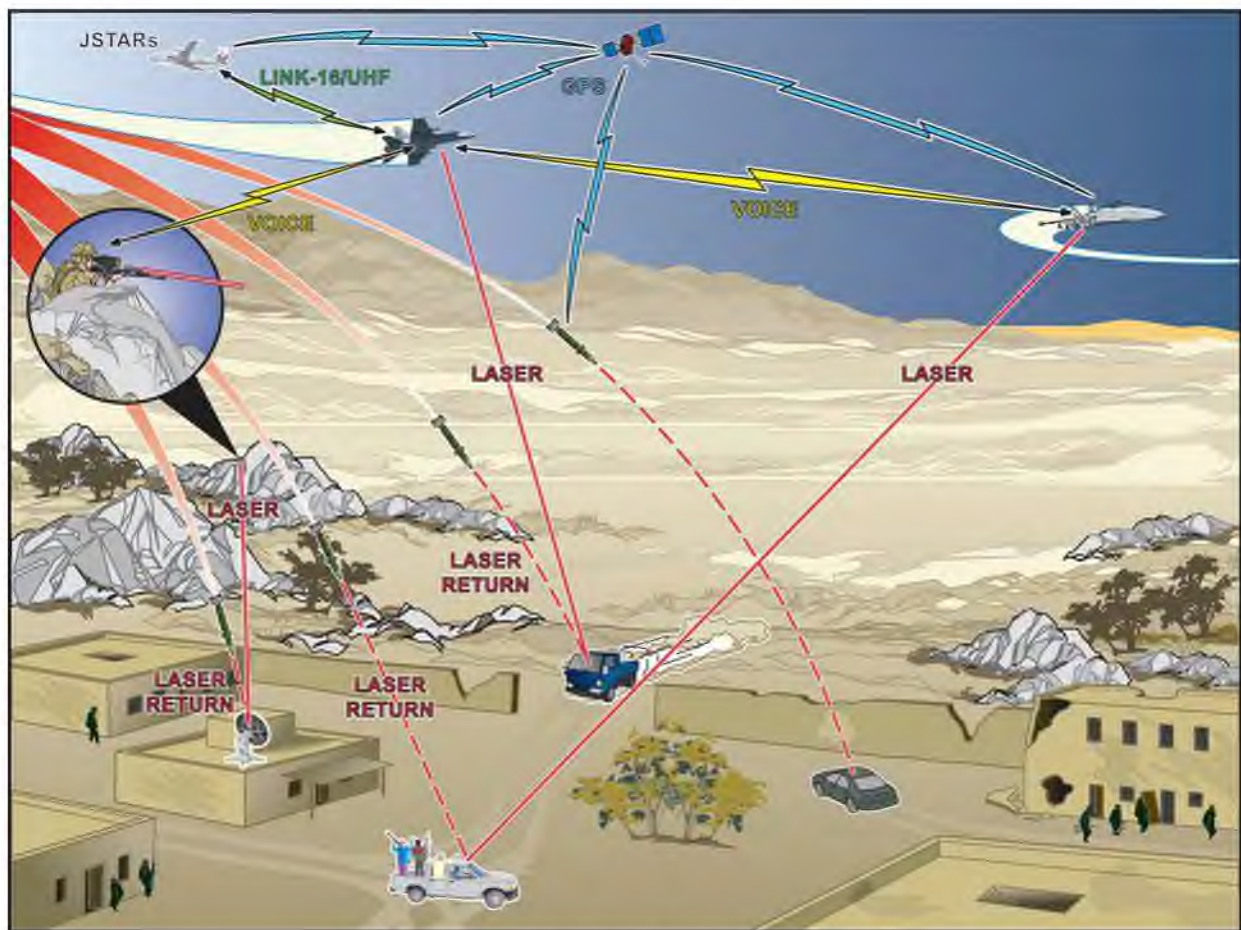


Figure 1-2. DAMTC Operational View

DAMTC uses the JDAM and Laser JDAM maintenance/support concept of a factory warranty and replacement for storage and captive carry reliability failures with no onsite maintenance required. Weapon assembly consists of attaching the DSU-38/B laser sensor kit to the existing GBU-38 JDAM configuration.

Mission planning for DAMTC is performed on the Joint Mission Planning System (JMPS). During the mission, the F/A-18 receives stationary, moving, and maneuvering target tracks via Link 16, while the AV-8B Harrier, without Link 16 capability, receives stationary target information through the Variable Message Format CAS 9 line. Both platforms may receive additional Forward Air Control or JTAC voice updates for moving and maneuvering targets. On the aircraft, the Laser JDAM weapon interfaces with the F/A-18 and AV-8B aircraft through the MIL-STD-1760 aircraft/stores databus on the weapons carriage rack.

This page intentionally left blank.

Section Two Test Adequacy

The operational testing of the DAMTC was adequate to support an evaluation of DAMTC's operational effectiveness and suitability. A Live Fire Test and Evaluation program was not conducted because the Laser JDAM weapon is built on the 500-pound general purpose bomb body, which has known lethality. However, VX-9 employed four live weapons and data from these tests validated that the estimates of lethality for JDAM contained in the Joint Munitions Effectiveness Manual (JMEM) are applicable to DAMTC.

Prior to operational test and evaluation (OT&E), VX-31 Squadron completed a short developmental test (DT) phase sufficient to demonstrate that the new laser sensor sapphire lens, which replaced the old glass lens because of excessive deterioration in inclement weather conditions, retained the same performance characteristics as the prior material.

The DAMTC Initial Operational Test and Evaluation (IOT&E) was begun in accordance with a DOT&E-approved Test and Evaluation Master Plan (TEMP) and test plan. However, after coordinating with DOT&E, VX-9 made changes during test execution on moving target profiles because of emerging operational tactics proposed by the Navy's TOPGUN School. Additionally, Integrated Test (IT) data were not operationally realistic and thus not used in the operational effectiveness analysis as planned. Despite deviations from the approved test plan, VX-9 gathered adequate data from 22 test events to evaluate the weapon's operational effectiveness and suitability.

Integrated and Developmental Testing

The DAMTC Program Office conducted developmental tests against maneuvering targets, designated as IT-C1, between May 2010 and April 2011. VX-31 Squadron conducted the tests under the guidance of the Program Office from the Naval Air Warfare Center (NAWC) China Lake, California, test ranges flying F/A-18D/E/F and AV-8B aircraft. A total of 19 weapons were used during this phase of testing.

Operational units using previously fielded Laser JDAM weapons (from the Urgent Operational Need (UON)) reported environmental degradation, consisting of pitting and the onset of opaqueness, of the laser seeker lens. This degradation required replacement of the existing glass lens with a more durable sapphire lens; a short regression test was conducted to ensure that the new lens detected laser energy at equivalent ranges as the original lens material. This testing, designated as DT-C1, was conducted by VX-31 Squadron at China Lake in August and September 2011 using six weapons; three with the original lens and three with the new sapphire lens. VX-31 released the weapons in pairs for direct side-by-side comparison of laser energy acquisition ranges. Successful completion of this phase allowed progression to operational testing.

The VX-9 Squadron evaluated the IT-C1 and DT-C1 missions as not operationally representative for evaluation of weapon accuracy and mission accomplishment because each mission featured several rehearsal runs that allowed the aircrew to become familiar with the

scenario, which reduced the tactical uncertainty necessary for operational realism. Nonetheless, the IT events revealed no anomalous performance; one failure was observed because of clouds masking the laser and preventing weapon guidance. The IT and DT missions also produced useful reliability data, which were incorporated into this evaluation.

Operational Testing

OPTEVFOR, using VX-9 Squadron as their lead test agency, conducted operational testing from October 2011 through April 2012 at NAWC China Lake.

Table 2-1 below indicates the three different phases of testing, the inclusive dates and locations, and the number of weapons used in each phase. VX-9 released a total of 22 weapons during IOT&E. Three of the weapons were not scored, resulting in 19 scored weapon releases. The three no-score events were: one event when ground crew improperly entered the weapon laser code preventing the weapon from detecting any laser energy; one weapon was released out of the launch acceptability region (LAR); and finally, while lasing the weapon, the aircraft maneuvered in such a manner as to cause the laser pod to shut off as a safety measure.

Table 2-1. Phases of Testing for Operational Evaluation

Test Phase	Dates	Location	Weapons Released
IT-C1	May 2010 – April 2011	NAWC China Lake	19
DT-C1	August 2011 – September 2011	NAWC China Lake	6
Developmental Test and Evaluation			25
IOT&E	October 2011 – April 2012	NAWC China Lake	22
Operational Test and Evaluation			22
Total Weapons Tested			47

Maneuvering Target Accuracy, or median miss distance, was measured as a function of target posture: maneuvering (evasive, non-evasive, stationary) and maneuver initiation timing (10 or 20 seconds). Evasive maneuvers are those a target might perform in a scenario where they were aware that they were being targeted and were trying to avoid threats. Examples of evasive maneuvers include maximum performance decelerations, weaving turns, and turns of large heading changes. Non-evasive maneuvers are those a target might perform in normal driving conditions when they were unaware they were being targeted. Examples of non-evasive maneuvers include normal linear accelerations and decelerations, and turns of smaller heading changes. Maneuver initiation timing was intended to discern a difference if the target commences its maneuver after the weapon is receiving laser energy or prior to receiving it.

Due to emerging tactics recommendations from the Navy TOPGUN School, VX-9 deviated from the original Design of Experiments test matrix. The Navy TOPGUN School recommended employing all but one weapon using the self-lasing mode from a rear aspect

heading (near zero degrees). VX-9 incorporated the recommendation and therefore employed only one weapon from a forward (180 degrees) aspect.

In addition, range limitations required modification to the high speed turns performed by the targets. Also, familiarity with the starting conditions of the targets during testing reduced the operational realism of the missions. Therefore, testers used an oval racetrack pattern for the last six events thus varying the starting test conditions based on where the target was on the oval track at mission initiation. This change to the oval racetrack was only accomplished using the buddy-lasing mode, which prevented system evaluators from determining the extent buddy-lasing mode had on system performance under these conditions compared to the self-lasing mode.

Finally, VX-9 conducted DAMTC weapon drops against both stationary and constant velocity targets (non-maneuvering targets). The complete IOT&E shot matrix is shown in Table 2-2.

Table 2-2. IOT&E Shot Matrix

Target Type	Target Actions	Guidance Mode	# of Drops
Stationary	N/A	GPS/INS, INS only, Buddy-Lase	4
Constant Velocity	4 x 70 mph 1 x 40 mph	Self-Lase	5
Maneuvering	4 x accelerate or decelerate 1 x 30° turn 2 x 60° turn	Self-Lase	7
Maneuvering	6 x 40 mph oval racetrack	Buddy-Lase	6
Total			22

Data collection included cockpit recording (both audio and video); range instrumentation including range cameras and time, space, position information; and target cameras, including laser energy detection capability mounted on the moving targets at which the weapons were aimed. Additionally, mission data sheets and surveys were completed by aircrew and maintenance personnel in order to provide the remaining data elements necessary for the full evaluation outlined in the DOT&E-approved OPTEVFOR Integrated Evaluation Framework.

Live Fire Testing

Warhead characterization testing was not conducted because Mk-82/BLU-111/BLU-126 500-pound warheads, which are used by DAMTC, have been previously characterized and are provided as Government Furnished Equipment to the LJDAM program. In the JMEM Weapon Engineering System (JWS 2.0.1), the lethality data are based on the warhead characterization. When guidance kits are added, as is the case with DAMTC, the JMEM uses the hit distribution for the designated warhead and combines it with the accuracy, reliability, impact conditions, etc., for the bomb with the kit installed. The output result is the Single Shot Probability of Damage

for the overall weapon system lethality. Four live weapons were employed and data from these integrated live fire tests validated the JMEMs estimate.

Test Limitations

The lack of weapon telemetry kits during the IOT&E limited the ability to analyze weapon behavior in terms of the frequency, magnitude, and direction of target updates based on received laser energy. In addition to information gathered by range cameras regarding laser energy and movement, telemetry data may have been able to reveal the reason for some of the large miss distances experienced during test.

Range size and weapon footprint restricted aircraft attack headings and engagement geometries for safety reasons. There was sufficient flexibility to achieve test objectives except for the racetrack pattern used during the buddy-lase drops. In this case, the results were confounded between the buddy-lase procedure and the engagement geometry.

There was no highly accelerated life testing conducted as there was insufficient test time to conclusively evaluate service and shelf lives of DAMTC components.⁵ However, UON weapons, which are essentially identical to the test weapons, with the exception of the new sapphire lens, provide some insight to the weapon reliability and shelf life.

Range safety limitations prevented operational testing of DAMTC with manned Joint Terminal Attack Controller (JTAC) designation. A JTAC is a forward deployed individual or team who direct the action of combat aircraft against a desired target. The risk to these personnel in peacetime or testing is too great for range operations. However, the Navy and Marine Corps consider JTAC designation of moving and maneuvering targets an unlikely concept of employment due to the high risk to personnel safety. Moreover, a stationary JTAC at ground level will have difficulty tracking a moving or receding target.

⁵ DAMTC-unique components are limited to the Precision Laser Guidance Set composed of the Laser Sensor Detector Assembly, an interface with the JDAM kit, and associated cabling and straps, plus the weapon and laser sensor software.

Section Three

Operational Effectiveness

DAMTC is operationally effective against moving (non-evasive) and maneuvering (evasive) targets when employed in the self-lasing mode (that is, when the aircraft delivering the weapon uses its own laser to designate the target). Against moving but non-maneuvering targets, DAMTC hit within a median miss distance of 5.8 meters from the laser spot (average spot position during the last 3.5 seconds of flight) and within a median miss distance of 6.4 meters from the target's geometric center. Against maneuvering targets, DAMTC demonstrated a median miss distance of 4.3 meters from the laser spot and 5.3 meters miss distance from the target center. These delivery accuracies are sufficient to assure lethal effects against the set of relatively soft targets, such as commercial vehicles, against which DAMTC will be employed.

DAMTC did not demonstrate operational effectiveness against moving and maneuvering targets when employed in the buddy-lasing mode.⁶ DAMTC median miss distance in this mode was 24.3 meters from the laser spot and 26.3 meters from the target center. However, due to test execution issues, these large miss distances may also be due in part to range restrictions on attack headings and engagement geometries during the three buddy-lasing trials. Therefore, the operational effectiveness of DAMTC using buddy-lasing deliveries is unknown.

Mission Accomplishment

Aircrew using the Laser JDAM accomplish the DAMTC mission when the weapon is successfully delivered within the lethal radius of its target, particularly a moving or maneuvering target. A successful mission requires preparing the aircraft by inventorying the installed weapon as a Laser JDAM and inputting the proper laser coding into the aircraft to match the laser coding of the weapon. These are routine steps required to enable laser guidance of the weapon in flight. Target engagement follows successful identification and tracking of the target, followed by continued tracking of the target after the weapon has been released. Laser designation during the terminal phase of the engagement is critical (particularly for a maneuvering target) to enable the weapon to guide to the correct target coordinates provided by the laser designation and destroy the target.

Failure of the weapon to receive laser energy results in a failure to update the expected target coordinates at time of impact and increases the miss distance of the weapon. Intermittent loss of energy degrades the quality of target coordinates, but if energy is regained with sufficient time before impact, the coordinate quality will improve.

⁶ Buddy-lasing is when one aircraft drops laser-guided weapons that are guided by the second aircraft's laser. This can be an effective tactic, where one aircraft can dedicate his efforts to accurate targeting and providing a stable lasing platform, while the second aircraft can focus solely on weapons delivery.

System Performance

Nearly all DAMTC effectiveness parameter thresholds were met. Maneuvering Target Accuracy failed to demonstrate the threshold Key Performance Parameter (KPP) of Circular Error Probable (CEP) less than 6 meters from the laser spot when employed using the buddy-lasing method, a sub-category that does not have its own threshold, most likely because of test execution issues. In addition, the single weapon employed as a demonstration in Inertial Navigation System (INS)-only mode against a stationary target exceeded its 15 meter threshold by 3.3 meters. However, previous test phases, starting with initial GBU-38 testing in 2002, demonstrated the ability of the weapon to meet its INS-only requirement on average when performance is measured over numerous attacks.⁷ Table 3-1 summarizes the IOT&E miss distances for the 19 valid weapon shots. Table 3-2 summarizes DAMTC required capabilities and the performance demonstrated during testing.

Table 3-1. IOT&E Miss Distance Results

OT Event	Target	Target Designation	Bomb Impact-to-Target (m)	Median Miss Distance to Target Center	Bomb Impact-to-Laser Spot Average ¹ (m)	Median Miss Distance from Laser Spot ⁶ (m)
STATIONARY						
Stationary GPS/INS						3.8
1 (Live)	Stationary	Coordinates	0.0		N/A	
2 (Live)	Stationary	Self-Generate	7.6		N/A	
Stationary INS²						18.3
18-2 (Live)	Stationary	Coordinates	18.3		N/A	
Stationary GPS/INS/LASER³						0.9
19-2	Stationary	Buddy-Lase	0.9		N/A	
MOVING BUT NOT MANEUVERING⁴				6.4		5.8
CONSTANT VELOCITY GPS/INS/Laser						
3	70 mph Steady	Self-Lase	27.5		29.2	
4	70 mph Steady	Self-Lase	3.2		3.7	
5	70 mph Steady	Self-Lase	7.1		6.3	
6	70 mph Steady	Self-Lase	17.3		18.0	
11	40 mph Steady ⁵	Self-Lase	5.6		5.3	

⁷ INS-only mode disables use of GPS to provide updates to the weapon's navigation, allowing its Inertial Measurement Unit to drift and become less accurate.

OT Event	Target	Target Designation	Bomb Impact-to-Target (m)	Median Miss Distance to Target Center	Bomb Impact-to-Laser Spot Average ¹ (m)	Median Miss Distance from Laser Spot ⁶ (m)
MANEUVERING – SELF-LASE ONLY (KPP=6m)				5.3		4.3
7	40 mph to 0 Decel	Self-Lase	5.3		4.3	
8	0 to 40 mph Accel	Self-Lase	4.0		3.3	
9	40 mph to 0 Decel	Self-Lase	7.1		7.1	
10	0 to 40 mph Accel	Self-Lase	6.0		3.7	
12	40 mph 30° turn	Self-Lase	2.3		2.3	
13	40 mph 60° turn	Self-Lase	4.2		5.8	
14	40 mph 60° turn	Self-Lase	7.6		5.5	
MANEUVERING – BUDDY-LASE ONLY				26.3		24.3
15-2	40 mph Race Track Pattern ⁷	Buddy-Lase	26.3		24.3	
16	40 mph Race Track Pattern ⁷	Buddy-Lase	12.2		12.4	
17	40 mph Race Track Pattern ⁷	Buddy-Lase	55.7		55.4	
NO SCORE						
15-1	40 mph Race Track Pattern ⁷	Buddy-Lase ⁸	83.7	9.2	79.4	
18-1	40 mph Race Track Pattern ⁷	Out of Launch Acceptability Region (LAR) ⁹	N/A	N/A	N/A	
19-1	40 mph Race Track Pattern ⁷	Buddy-Lase ¹⁰	55.7	N/A - No Laser	N/A - No Laser	
<p>Note 1: Laser Spot is average position during last 3.5 seconds of flight.</p> <p>Note 2: Coordinates in weapon to actual impact. Weapon guided but did not function.</p> <p>Note 3: Laser spot camera obscured by target. Scored from target.</p> <p>Note 4: Median results EXCLUDES 29 meter outlier.</p> <p>Note 5: Actual target maneuver occurred 5 seconds post weapon impact (Non-Maneuvering).</p> <p>Note 6: CEP is defined as the distance from the 3.5 second average of the laser spot inside which 50 percent of the impacts occurred.</p> <p>Note 7: Target prosecuted from forward quarter (worst case target maneuver).</p> <p>Note 8: Weapon page displayed 0000 at release. LJDAM seeker manually coded 1111.</p> <p>Note 9: Laser JDAM released past LAR min-range.</p> <p>Note 10: Aircraft masked target from laser.</p>						

Maneuvering and Moving Target Accuracy

Maneuvering target accuracy is the principal KPP for this system. During IOT&E, there were seven valid weapon drops using the self-lasing mode against maneuvering targets and three using the buddy-lasing mode. Three additional buddy-lasing drops were not scored. In addition, five weapons using the self-lasing mode against fast moving, but non-maneuvering, targets and four weapons against stationary targets were dropped.

DAMTC maneuvering target accuracy for the seven weapon releases using the self-lasing mode was 4.3 meter median from laser spot and 5.3 meter median from the center of the maneuvering target, meeting the KPP threshold of 6 meters CEP with a confidence of 88 percent. In fact, six of the seven valid weapon drops were less than 6 meters miss distance from the laser spot. The largest distance from the target center was 7.6 meters. The aircrew manually tracked all the targets throughout flight, and weapons received laser energy and made accurate updates through impact. All weapons were released from a rear aspect relative to the target.

Table 3-2. Effectiveness Parameters

Parameter	Threshold	Performance
Maneuvering Target Accuracy (Key Performance Parameter (KPP))	≤ 6 meters (m) CEP from the laser spot ^a	Exhibited 4.3 m median miss distance using self-lasing mode Exhibited 24.3 m median miss distance using buddy-lasing mode
Maneuvering Target Engagement Velocity (KPP)	Up to 40 mph	Maneuvering targets engaged at 40 mph
Maneuvering Target Acceleration (Post-Release Maneuvers) (KPP)	≤ 0.2 g-force (g)	Maneuvering targets achieved threshold g force via acceleration, deceleration, and 40 mph turns of 30 and 60 degrees
Moving Target Velocity	Up to 70 mph	Moving targets engaged at 70 mph
Moving Target Autonomous Lead Computation ^b	Required	Lead computation used as integral system function
Stationary Target Accuracy (INS Only)	≤ 15 m CEP	In IOT&E, one event achieved 18.3 m Previous testing met accuracy threshold
Stationary Target Accuracy (GPS/INS)	≤ 13 m CEP	Demonstrated during IOT&E with two weapons achieving a CEP of 3.8 m Previous testing met accuracy threshold
Stationary Target Accuracy (Laser)	≤ 5 m CEP	Demonstrated during IOT&E with one weapon hitting at 0.9 m Previous testing met accuracy threshold
Multi-mode Guidance Capability	Laser, GPS/INS, and INS-only	All modes demonstrated during IOT&E test phase
Weapon Maneuverability – Footprint for Stationary Targets Aircraft Release Conditions (20,000 feet (ft) Mean Sea Level (msl)/0.8 Mach)	2.5 to 8.5 nautical miles (nm) Down Range	Previous testing demonstrated full range of required weapon maneuverability IOT&E events ranged from 2.4 to 6.3 nm Down Range, and < 0.5 nm Cross Range
	± 2.0 nm Cross Range	

^a Circular Error Probable (CEP) is defined in the DAMTC Capabilities Production Document as the distance inside of which at least 50 percent of weapons impacted relative to the laser spot.

^b Moving Target Autonomous Lead Computation uses the movement of the laser spot to determine the target's velocity and direction and computes the predicted intercept point. This computation is performed by the weapon's software and it improves the weapon's performance against moving and maneuvering targets while maintaining the performance against stationary targets.

Three of the six weapons released against maneuvering targets using the buddy-lasing mode were not scored because of operational errors by aircrew and/or ground personnel, which prevented the weapon from performing as intended. In one case, the aircrew did not have the correct laser code, which prevented the weapon from seeing the laser spot resulting in an 80 meter miss. For the second miss, the pilot did not release the weapon until after exiting the Launch Acceptability Region (LAR), which prevented the weapon from having the ability to physically maneuver to the target. The third weapon was launched within the LAR and was guiding to the target when the lasing aircraft maneuvered into a position where the aircraft's own frame interfered with the laser energy reaching the target; the laser shuts off automatically to prevent laser energy reflecting into the cockpit. This resulted in no laser energy being received by the weapon for the last 6 seconds of flight and the result was a miss distance of 56 meters from the target.

The three buddy-lasing weapons that were scored resulted in a median miss distance of 24.3 meters from the laser spot and 26.3 meters from the maneuvering target center. The use of the repetitive race track pattern at China Lake on each of the buddy-lase events resulted in releases and engagements occurring with on-coming or crossing angles in relation to the target's direction and significant heading changes of the target. This attack profile is more challenging for the weapon than the tail chase engagements that were accomplished using the self-lasing mode. The extent to which the buddy-lasing method can be cited as the source of large miss distances is uncertain, especially when the one buddy-lasing event against a stationary target resulted in a 0.9 meter hit. Additional testing using self-lasing with these geometries and, if possible, using buddy-lasing from rear aspect geometries, should provide valuable information to distinguish between the effects of adverse target geometry and the effect of the buddy-lasing mode on DAMTC accuracy.

DAMTC was employed against five moving, but not maneuvering, targets, four of which were traveling at a constant speed of 70 miles per hour, while the fifth was traveling at a constant speed of 40 miles per hour. Four weapons were released from a rear aspect while the fifth was delivered from a direct head on aspect. All of these moving, non-maneuvering target engagements were accomplished using self-lasing mode. Of the five weapons employed, one impacted long and left of its target at a distance of 27.5 meters, nearly five times the CEP. The root cause of this failure is unknown. The weapon appeared to be initially guiding to the target, but at some point either did not receive laser energy or calculated an inaccurate target velocity and heading and impacted far from the target. It is standard practice to consider any drops that are 3.5 times the CEP to be "system failures," and not include the result in the calculated CEP.

Another weapon fell nearly 18 meters short of the target. This weapon appears to be an outlier as well, but was not considered as a system failure because it landed inside the range of 3.5 times the CEP distance. Considering the 27.5-meter miss as a system failure and thus removing it from CEP calculations, the moving target CEP is 5.8 meters from the laser spot and 6.4 meters from target center. Self-lasing accuracy for moving and maneuvering targets, including 11 weapons (excluding the 27.5-meter outlier), results in a median miss distance of 5.5 meters from the laser spot and 5.6 meters from the target center.

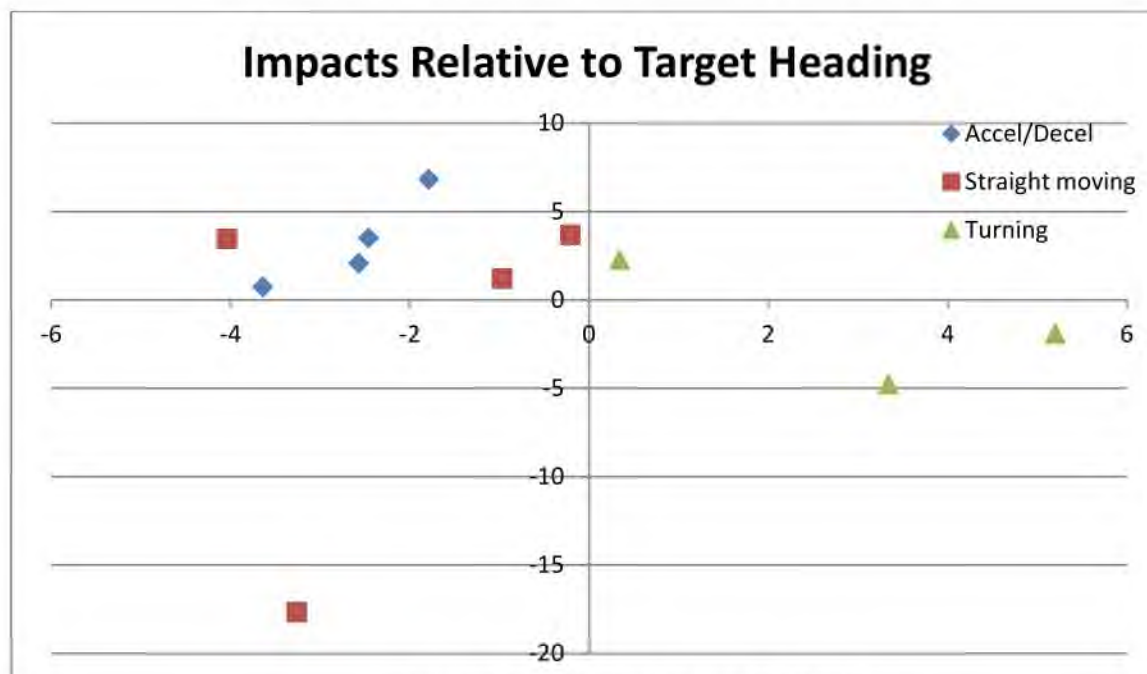


Figure 3-1. Self-Lasing Impact Distances

Figure 3-1 shows the impact distances in meters from the target relative to the target heading for the 11 valid weapon drops employed against moving or maneuvering targets using the self-lasing mode (red for moving, blue for maneuvering), assuming the target is at the vertex moving up the page. DAMTC hit dispersion for moving and maneuvering but not turning targets exhibited a modest bias averaging 2 meters left and 3.3 meters in front of the target.

For those weapons employed against the three turning targets, the hit dispersion is in a different direction and the bias is greater for the higher turning rate (60 degrees turns are the two far right points) than for the single 30-degree turn. The mean points of impact between the 60-degree and the 30-degree turning target groups are 6.9 meters apart. This is most likely a result of the Kalman filter software algorithm, used to estimate distance errors over time, lagging slightly in accepting the full change in direction and velocity observed by the laser sensor. Note that the CEPs for these two groups of weapons are not different from each other in a statistically significant manner but the mean points of impact are different.

The only factors observed to make a statistically significant difference in accuracy are the combination of self-lasing and rear aspect attack compared to the combination of buddy-lasing and racetrack pattern/forward or crossing aspect attack. As discussed above, test execution confounded the results for these two factors. Maneuver Initiation Timing, Aircraft Heading, and Maneuver did not show any statistically significant impact on miss distance.

Other Effectiveness Parameters

All maneuvering target events featured the target accelerating to 40 miles per hour, decelerating from 40 miles per hour, or turning at 40 miles per hour, thus meeting the requirements for up to a 40 miles per hour maneuvering target and for post-release maneuvers of

up to 0.2 g. Four of the five moving target events featured target speed of 70 miles per hour, meeting that requirement.

Moving Target Autonomous Lead Computation (MTALC) uses the movement of the laser spot to determine the target's velocity and direction and computes the predicted intercept point. This computation is performed by the weapon's software and it improves the weapon's performance against moving and maneuvering targets while maintaining the performance against stationary targets. The MTALC requirement is met because it is an inherent part of the Laser JDAM design. Previous testing confirmed MTALC capability; no performance degradations were noted during this IOT&E.

The test program addressed Stationary Target Accuracy as a demonstration only because of extensive previous history with standard JDAM delivery and previous Laser JDAM testing in these modes. The two weapons delivered using standard JDAM GPS-aided INS guidance impacted at 0.0 meters and 7.6 meters from the designated target coordinates. This is consistent with previous test results, a CEP of approximately 3 meters, all of which meet the threshold of 13 meters. The one weapon delivered using INS-only guidance impacted at 18.3 meters from the designated target coordinates. This is beyond the threshold of 15 meters, but the result is not well beyond the normal range of impact distances previously seen for this mode (CEP of 12 meters during Laser JDAM initial operational testing). Employment in this mode should not be expected unless both GPS and laser targeting are unavailable. The one weapon employed against a stationary target using laser targeting impacted 0.9 meters from the target center using the buddy-lasing mode. This met the threshold of 5 meters.

The demonstration of the three different stationary target guidance modes as well as employment of laser targeting of moving and maneuvering targets met the Multi-mode Guidance Capability requirement.

Previous testing confirmed the ability of the Laser JDAM weapon to meet the Weapon Maneuverability – Footprint for Stationary Targets Aircraft Release Conditions requirement of 2.5 nautical miles to 8.5 nautical miles release range coupled to a 2.5 nautical mile cross range capability. All IOT&E events were flown in an operationally realistic manner, without the specific intent of testing the known maneuverability envelope. A successful minimum range engagement took place during the IT phase with a 2.4 nautical mile release from the target, but during the IOT&E, a weapon delivered out of LAR at only 1.5 nautical miles was unable to maneuver sufficiently to engage the target.

This page intentionally left blank.

Section Four Operational Suitability

DAMTC is operationally suitable. During operational testing, the Laser JDAM weapon exceeded the threshold for material reliability and achieved a 100 percent pass rate in built-in test (BIT) function. Evaluations of DAMTC's logistics supportability, compatibility, training program, safety, and documentation revealed no deficiencies and consistently received satisfactory (or better) survey results. Aircraft and weapon bomb body compatibility requirements were also met. Testers discovered deficiencies related to interoperability with aircraft software (operational flight profile or OFPs) during initial weapon power-up on the ground. Also, placement of the wiring in the fuze-well physically hinders visual verification of fuze arming and function settings. Simple work-arounds such as accelerated ground checks and stronger flashlights currently exist to enable reliable mission completion until a more permanent solution is implemented. Human factors difficulties were reported by aircrew in maintaining precise laser designation on a moving target throughout weapon delivery; the manual tracking is necessary because the auto-track mode will easily break lock while tracking the moving target.

DAMTC demonstrated a material reliability, as measured by in-flight reliability, of 95.5 percent (21 of 22 weapons), exceeding its threshold value of 90 percent with a confidence level of 66 percent as indicated in Table 4-1.⁸ The in-flight reliability is measured from weapon release to impact. The single weapon failure was during one of the live weapon drops employed against a stationary target when the weapon did not detonate. No root cause for the failure was determined; range safety personnel destroyed the weapon and no other information is available than the observation cameras. Inclusion of Integrated Test (IT) weapons for reliability analysis resulted in a material reliability of 97.9 percent (46 of 47 weapons), exceeding the threshold value of 90 percent with a confidence level of 95 percent.

The Laser JDAM weapon since its post Urgent Operational Need (UON) fielding has reported only two observed failures out of 205 weapons employed.

Table 4-1. Reliability Parameter

Parameter	Threshold	Performance [confidence above threshold]
Key System Attribute (KSA) 9 Material Reliability	≥ 90% In-flight weapon reliability	95.5% for IOT&E weapons only [66% confident above threshold]
		97.9% for IOT&E and IT weapons [95% confident above threshold]

DAMTC maintainability, logistics supportability, training, safety, and documentation were all rated satisfactory and without deficiency. The maintainability measure of BIT function was demonstrated at 100 percent (26 of 26 BIT checks). All surveys of aircrew, maintenance

⁸ Material reliability is an in-flight reliability measure which is a Key System Attribute (KSA) for DAMTC.

personnel, and ordnance personnel showed high degrees of satisfaction with all areas. Safety and documentation surveys with 34 and 35 respondents surveyed, respectively, were 100 percent positive. Shipboard suitability, a DAMTC Key System Attribute (KSA), was evaluated as safe in the aircraft carrier operating environment.⁹

DAMTC met its compatibility Key Performance Parameter (KPP) of not requiring any modifications to aircraft hardware or software as indicated in Table 4-2 below. No aircraft hardware modifications were made in order to employ DAMTC and the weapon was employed with existing aircraft OFPs. Better weapon integration with future aircraft OFPs could improve weapon performance and should be incorporated as part of the regular OFP update.

DAMTC is compatible with legacy bomb bodies, Mk-82 and BLU-111 500-pound class bodies. During the OT phase, VX-9 employed 19 Mk-82 and 3 BLU-111s. There is a requirement for compatibility with the BLU-126 reduced collateral damage warhead, which is a “form/fit/function” of the BLU-111 with a different explosive fill to reduce collateral damage. A Laser JDAM with either bomb body would demonstrate the same accuracy against a moving target.

DAMTC is compatible with threshold aircraft models (F/A18C-F and AV-8B). VX-31 Squadron evaluated the F/A-18A+ model during the IT phase and found it to be compatible. This met the Aircraft Compatibility KPP.

Table 4-2. Compatibility Requirements

Parameter	Threshold	Performance
KPP 4 Aircraft Compatibility	No modifications to aircraft hardware or software	No modifications required.
KPP 5 Legacy Weapon Compatibility	BLU-111/BLU-126 /Mk-82	Compatible with BLU-111 and Mk-82 bomb bodies Not tested with BLU-126
KSA 8 Aircraft Compatibility	F/A-18A+/C/D/E/F and AV-8B	Compatible with all threshold aircraft

DAMTC adequately interfaced with threshold aircraft, mission planning systems, and BIT testing equipment. No deficiencies were noted when interfacing with the Joint Mission Planning System (JMPS) and with F-18 aircraft using the H6E OFP and AV-8B Harriers using H6.0 OFPs. Testers identified a deficiency on F/A-18 aircraft loaded with the newest aircraft software, 23X and H8E, on which a Laser JDAM was loaded and had the Common BIT Munitions Reprogramming Equipment (CMBRE) system perform a BIT check. Weapons initially powered up using the CMBRE would inventory on the F/A-18 Stores Management System (SMS) as a regular JDAM with the notation “J82” instead of as a Laser JDAM

⁹ The shipboard suitability assessment is based on a September 2008 analytical report completed by NAVAIR in support of the initial UON Laser JDAM fielding and the lack of any shipboard suitability deficiencies reported in more than three years of operational shipboard use.

and “LJ82.” Failure to notice the misnomer prior to aircraft launch results in loss of Laser JDAM functionality between the weapon and the aircraft. It is only possible to fix the problem while on the ground by either cycling SMS circuit breakers located on the right engine intake panel or cycling generator or battery power. The impact of this deficiency can be minimized by ensuring that check lists mandate verifying the weapon inventory early in the pre-launch procedures to prevent unnecessary launch delays. The next scheduled aircraft software modifications intend to eliminate the deficiency altogether.

Two deficiencies related to human factors were noted during testing. The first deficiency involved the dense wiring inside the tail-kit of live Laser JDAM weapons, which made verifying fuze arming and function settings extremely difficult, especially at night. The umbilical wire bundles result in a very crowded tail compartment making it difficult to read the settings or move the thick cable bundle. Using more powerful lighting is a work-around deemed acceptable by fleet squadrons until a better more permanent solution is identified.

For the second deficiency, testers noted that the various versions of the F/A-18 aircraft software automatically select a navigation mode, which is sub-optimal when the F/A-18 aircraft is employed in the Target of Opportunity mode (the principal mode for attacking moving and maneuvering targets). The default navigation mode does not enable the use of GPS data to eliminate JDAM inertial drift and correct aircraft position hand-off errors. The recommended Relative Navigation mode does enable the use of GPS data, thus reducing target location errors in flight. It is possible to switch to the better Relative Navigation mode after target designation, but if the aircrew is forced to designate a different target or re-designate the original target, the aircraft defaults again to the initial navigation mode. The need to switch navigation modes, and particularly the need to switch again on re-designation, exacerbates the high cockpit workload during target engagement under a compressed attack mission timeline. Correction of this deficiency is dependent on the Navy’s fielding schedule priorities within the aircraft routine software updates. This deficiency has been observed in the fielded weapons and during the IOT&E, and despite the increased workload, the aircrew have still been able to deliver weapons on targets within the required accuracy.

Continuous target tracking while lasing a target is normally a high workload event with any weapon, particularly when trying to maintain a consistent laser spot on a moving target. The targeting pods employed during the OT phase, the Advanced Targeting Forward-Looking Infrared (ATFLIR) and the LITENING pod, were not designed with moving laser targets in mind and, as a ‘non-developmental’ program, the DAMTC program could not make aircraft software changes to optimize performance against this target type. The ATFLIR in particular has deficiencies with its AUTOTRACK mode. Normally, the ATFLIR is unable to maintain this mode and reverts to manual tracking, which increases workload and reduces cockpit situational awareness and in one case prevented the aircrew from recognizing the aircraft exited the weapon’s Launch Acceptability Region (LAR) prior to weapon release. The aircraft flying that event used ATFLIR in manual track and released its weapon outside of the LAR, which resulted in weapon impact so far from the target that it was not scored. DAMTC weapons targeted using the LITENING pod do not appear to be more accurate than the ATFLIR targeted weapons when

each is properly employed, but the workload with the LITENING is much reduced and the likelihood of operator error consequently reduced as well.

Section Five Recommendations

The Navy should implement the following recommendations:

Operational Effectiveness

- Conduct additional testing using buddy-lasing from rear aspect geometries to distinguish between the effects of adverse target geometry and the use of the buddy-lasing on DAMTC accuracy.

Operational Suitability

- Incorporate changes to subsequent releases of future F/A-18 aircraft software to correct interoperability deficiencies with weapon identification and selection of aircraft navigation mode.
- Re-design the wiring bundle in the weapon's tail compartment to facilitate a visual pre-flight check of the weapon's fuze settings.

Filename: DRAFT DAMTC BLRIP 28 Jun 2012.docx
Directory: H:
Template: C:\Documents and Settings\BarretB\Application
Data\Microsoft\Templates\Normal.dotm
Title:
Subject:
Author: BADalton
Keywords:
Comments:
Creation Date: 6/28/2012 3:26:00 PM
Change Number: 6
Last Saved On: 6/29/2012 7:58:00 AM
Last Saved By: JacksonB
Total Editing Time: 18 Minutes
Last Printed On: 6/29/2012 8:00:00 AM
As of Last Complete Printing
Number of Pages: 29
Number of Words: 7,708 (approx.)
Number of Characters: 43,937 (approx.)



OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JUN 29 2012

OPERATIONAL TEST
AND EVALUATION

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

I have enclosed the Initial Operational Test and Evaluation (IOT&E) Report on the Direct Attack Moving Target Capability (DAMTC) as required by Sections 2399 and 2366, Title 10, United States Code. DAMTC uses a Laser Joint Direct Attack Munition (JDAM) (GBU-54/B) with the updated Block 8 Operational Flight Program software to prosecute moving and maneuvering, as well as stationary targets.

In the report I conclude:

- DAMTC is capable of providing effective, suitable, and lethal combat support in the prosecution of moving (non-evasive) and maneuvering (evasive) targets. DAMTC provides enhanced capability compared to baseline JDAM weapons (which are used to attack stationary targets) by enabling the successful engagement of both moving and maneuvering targets and eliminating Global Positioning System (GPS) Target Location Error when using precise laser designation.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.

J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Adam Smith
Ranking Member





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JUN 29 2012

The Honorable C. W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

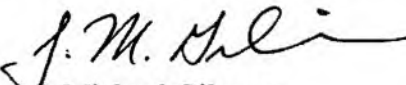
Dear Mr. Chairman:

I have enclosed the Initial Operational Test and Evaluation (IOT&E) Report on the Direct Attack Moving Target Capability (DAMTC) as required by Sections 2399 and 2366, Title 10, United States Code. DAMTC uses a Laser Joint Direct Attack Munition (JDAM) (GBU-54/B) with the updated Block 8 Operational Flight Program software to prosecute moving and maneuvering, as well as stationary targets.

In the report I conclude:

- DAMTC is capable of providing effective, suitable, and lethal combat support in the prosecution of moving (non-evasive) and maneuvering (evasive) targets. DAMTC provides enhanced capability compared to baseline JDAM weapons (which are used to attack stationary targets) by enabling the successful engagement of both moving and maneuvering targets and eliminating Global Positioning System (GPS) Target Location Error when using precise laser designation.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JUN 29 2012

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

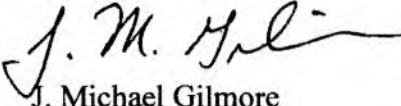
Dear Mr. Chairman:

I have enclosed the Initial Operational Test and Evaluation (IOT&E) Report on the Direct Attack Moving Target Capability (DAMTC) as required by Sections 2399 and 2366, Title 10, United States Code. DAMTC uses a Laser Joint Direct Attack Munition (JDAM) (GBU-54/B) with the updated Block 8 Operational Flight Program software to prosecute moving and maneuvering, as well as stationary targets.

In the report I conclude:

- DAMTC is capable of providing effective, suitable, and lethal combat support in the prosecution of moving (non-evasive) and maneuvering (evasive) targets. DAMTC provides enhanced capability compared to baseline JDAM weapons (which are used to attack stationary targets) by enabling the successful engagement of both moving and maneuvering targets and eliminating Global Positioning System (GPS) Target Location Error when using precise laser designation.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable John McCain
Ranking Member





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JUN 29 2012

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6025

Dear Mr. Chairman:

I have enclosed the Initial Operational Test and Evaluation (IOT&E) Report on the Direct Attack Moving Target Capability (DAMTC) as required by Sections 2399 and 2366, Title 10, United States Code. DAMTC uses a Laser Joint Direct Attack Munition (JDAM) (GBU-54/B) with the updated Block 8 Operational Flight Program software to prosecute moving and maneuvering, as well as stationary targets.

In the report I conclude:

- DAMTC is capable of providing effective, suitable, and lethal combat support in the prosecution of moving (non-evasive) and maneuvering (evasive) targets. DAMTC provides enhanced capability compared to baseline JDAM weapons (which are used to attack stationary targets) by enabling the successful engagement of both moving and maneuvering targets and eliminating Global Positioning System (GPS) Target Location Error when using precise laser designation.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.

J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Thad Cochran
Ranking Member



Director, Operational Test and Evaluation


EProcurement System

**Major Automated Information System (MAIS)
Initial Operational Test and Evaluation (IOT&E) Report**

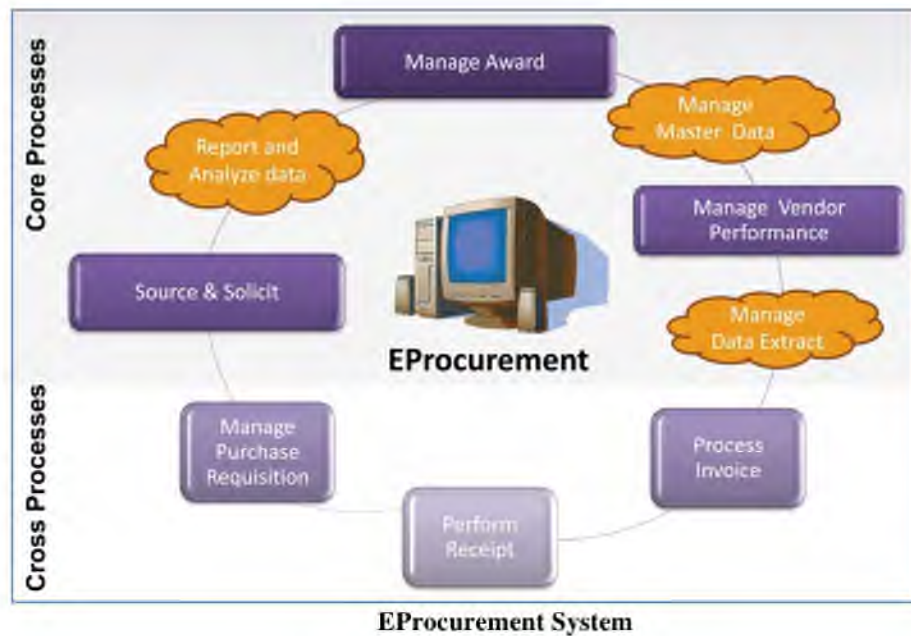


June 2012

This report assesses the adequacy of testing and the operational effectiveness, operational suitability, and survivability of the EProcurement System.


J. Michael Gilmore
Director

The marginal cost of producing this report is estimated to be approximately \$1.2K. The estimated acquisition cost of the program, which this report addresses, is \$0.37B.



Executive Summary

This document reports on the evaluation of test adequacy, operational effectiveness, suitability, and survivability of the EProcurement system. The evaluation is based primarily on data from the Initial Operational Test and Evaluation (IOT&E) that the Joint Interoperability Test Command (JITC) conducted from February through April 2012 at various Defense Logistics Agency (DLA) locations throughout the United States. EProcurement is operationally effective, operationally suitable with deficiencies, and survivable with limitations. This report also highlights the EProcurement program's highly effective procedures for deploying Defense Business System (DBS) software to new user groups

EProcurement is operationally effective. Users were able to accomplish all necessary job functions in 99 percent of the 1,363 tasks that were observed. The tasks addressed managing purchase requisitions, sourcing and soliciting goods and services, managing awards, processing receipts and invoices, creating reports, and maintaining system data. Minor errors were reported in 13 of the observed tasks. In addition, all 52 system interfaces (of 66 total interfaces) evaluated during the test processed all required inbound and outbound data without any recorded failures.

EProcurement is operationally suitable, but with deficiencies in the areas of training, usability, Help Desk operations, and supportability. During operational testing, EProcurement exceeded thresholds for reliability, availability, and maintainability. User surveys indicated that as a group both typical users and Business Process Analysts (BPAs) were not satisfied with the overall user-friendliness and usability of the system.¹ Typical users, but not the BPAs, were also critical of the quality of training and training aids provided. The time required to resolve EProcurement Help Desk tickets exceeded 8.5 days on average, and indicates that additional Help Desk training may be needed. Finally, DLA must continue to pursue test automation in order to effectively support future releases of EProcurement.

The EProcurement system is survivable against cyber threats but might be vulnerable to financial theft and fraud. The system is secure from an information assurance perspective. Only three security findings remain unresolved, with the operational impact of these issues considered as moderate to low by DOT&E.

No financial theft and fraud threat testing was conducted due to schedule constraints. DLA must ensure adequate protection of the Enterprise Business System (EBS), of which EProcurement is now a part, against financial theft and fraud threats. As part of this effort, DLA should establish a Theft and Fraud Prevention and Detection Red Team modeled after those used to probe for information assurance vulnerabilities.

DLA has developed a roadmap for deploying software to new users. The roadmap contains detailed tasks, dependencies, dates, and responsible persons for activities necessary to deploy EProcurement. The execution of these procedures has proven effective, and we recommend it for consideration by other DBS programs.

¹ BPAs are experienced EProcurement users whose job it is to provide first-level assistance to other users to resolve task issues and to determine when additional support is needed from the Help Desk.

System Description and Mission

EProcurement is to provide the DLA with a single, enterprise-wide capability that is more responsive to Services' requirements than the current legacy procurement systems.

EProcurement supports the following procurement functional areas: manage purchase requisitions, source and solicit goods and services, manage awards, manage vendor performance, and process receipts and invoices. EProcurement is developed based on a commercial product from SAP[®] and is a critical subsystem of the DLA EBS.

DLA employs EProcurement in an office setting with predominately Government civilian personnel as system users. Each user is assigned one or more roles to support the overall DLA mission of providing consumables, services, and depot-level repairables to the Army, Navy, Air Force, Marine Corps, other federal agencies, and combined and allied forces.²

Test Adequacy

The operational testing of EProcurement was adequate to support an evaluation of system operational effectiveness and operational suitability. An information assurance evaluation was adequate to determine the security posture of both EProcurement and its hosting site – the Defense Information Systems Agency (DISA) Defense Enterprise Computer Center (DECC) in Ogden, Utah.

Because the IOT&E was executed on the live system, there was limited ability for data collectors to observe specific tasks beyond those tasks required by the daily workloads at each site. Fourteen of the 66 interfaces between EProcurement and other systems were either not activated or did not have any activity during the test. These interfaces need to be evaluated in follow-on testing prior to a full deployment declaration.

No data were collected against 2 of 19 operational effectiveness evaluation areas. DLA indicates that these capabilities have a low execution rate in production, but we suggest that they be evaluated in future testing.

Operational Effectiveness

EProcurement is operationally effective. The effectiveness evaluation concentrated on the users' ability to use EProcurement in six areas: manage purchase requisitions, source and solicit goods and services, manage awards, process receipts and invoices, create reports, and maintain system data (data cleansing and conversions). JITC observed users performing day-to-day operations and recorded 1,363 observations of mission successes and failures. JITC recorded 13 failures during the test, resulting in a 99 percent success rate.

EProcurement is interoperable. JITC interoperability testers evaluated 52 inbound and outbound interfaces to assess the data exchanges between EProcurement and other Department of Defense (DoD) systems, with no failures reported in the more than 400 transactions evaluated.

² EProcurement uses role-based access control. Each user is assigned a role in the organization (Contracting Officer, BPA, Procurement Specialist, for example) and only the EProcurement capabilities needed to perform that role are available to the user.

DLA has done a very thorough job in preparing new sites to operate the EProcurement system. Other DoD business systems should leverage as best practices the DLA's work in the areas of change management and legacy data conversion.

Operational Suitability

EProcurement is operationally suitable, but with deficiencies in the areas of training, usability, Help Desk operations, and supportability.

DOT&E considers EProcurement reliable, available, and maintainable. The DECC in Ogden, Utah, where EProcurement is hosted, reported a 10-minute network outage. However, the operational impact to the EProcurement users was insignificant. DLA also reported one site-specific outage at Battle Creek, Michigan, lasting 1 hour and 55 minutes, but it appears to have been an isolated event.

EProcurement training, training aids, and system documentation need improvement. None of these areas met the 80 percent threshold of acceptability by the users surveyed. Typical users and BPAs report that EProcurement is not user friendly and is difficult to master.

Help Desk trouble tickets take a long time to resolve. Analysis of the closure rates for the tickets shows that the average time required to resolve trouble tickets was approximately 8.5 days, with resolution times ranging from less than 5 minutes to nearly 40 days.

Finally, the supportability of EProcurement needs improvement as DLA does not have an automated test capability to perform a thorough regression test on new software releases of EProcurement and its underlying commercial off-the-shelf software base.

Survivability

EProcurement is secure from an information assurance perspective. JITC information assurance testers, along with members of the Defense Information Systems Agency Field Security Office (DISA-FSO) and DLA Computer Emergency Response Team (CERT), conducted a series of Penetration and Exploitation (P&E) events primarily at the Ogden DECC.

As of the date of this report, only one moderate impact, and two low impact issues remain open, with minimal effect on system security and operations. DISA and DLA created a plan of action and milestones to address resolution of these issues.

We were unable to verify that DLA has a robust theft and fraud prevention and detection program. DLA asserts that by using role separations, at least two to three people would need to be involved in any theft and fraud activity and that while large-scale theft or fraud was not impossible, it would be difficult. DLA also indicated that bi-annual audits and other accounting controls are in place to further mitigate such activities. Additionally, DLA disclosed various pilot programs regarding theft and fraud protection and detection. While DOT&E acknowledged that some level of prevention and detection is available at DLA, the level is insufficient mostly due to the lack of a financial theft and fraud testing capability. DLA must demonstrate satisfactorily an adequate theft and fraud protection and detection capability prior to DLA declaring EProcurement as fully deployed. For example, a watch list is needed to prevent

debarred companies from easily receiving new Commercial and Government Entity (CAGE) codes.

Recommendations

- DLA should establish a Theft and Fraud Prevention and Detection Red Team modeled after those used to probe for information assurance vulnerabilities. The team would establish rules of engagement for theft and fraud testing, and the DLA process could become a model for the DoD to use for finance, logistic, and other business system acquisitions. DLA needs to demonstrate this capability through a follow-on operational assessment prior to DLA declaring EProcurement as fully deployed.
- DLA should continue their pilot program to utilize commercially available test automation software designed to functionally test the SAP[®] system. Based on the results of the recent pilot program, DLA should implement a more formal automated test program that again is expected to yield a model for other DoD entities to follow and become the standard within the DoD.
- DLA should improve the quality of training, training aids, and other system documentation for the users, and include role-specific training in the future when DLA transitions users at the remaining DLA sites to EProcurement.
- DLA should modify the method of managing trouble tickets in the Remedy system to better allow for data queries by program (EProcurement versus EBS, for example). DLA should also track the resolution times of system problems on a monthly or at least quarterly schedule to aid DLA management in identifying potential problem areas so that DLA can implement mitigation strategies before productivity is affected.
- JITC should administer the System Usability Scale survey periodically to a random sample of all EProcurement users through full deployment to see whether user satisfaction does improve with increased system use or whether a more inherent issue exists with system usability.
- In future testing, JITC and DLA should evaluate all untested interfaces that will be part of the full deployment.
- Although only minor issues remained after the last information assurance test event, the DISA-FSO and DLA CERT should periodically re-evaluate the security posture of the DECC and EProcurement as part of the overall defense-in-depth security strategy.


J. Michael Gilmore
Director

Contents

System Overview1

Test Adequacy7

Operational Effectiveness9

Operational Suitability17

Survivability23

Recommendations25

This page intentionally left blank.

Section One System Overview

This document reports on the evaluation of test adequacy, operational effectiveness, suitability, and survivability of the EProcurement system. This evaluation is based primarily on data from the Initial Operational Test and Evaluation (IOT&E) that the Joint Interoperability Test Command (JITC) conducted from February 27 through April 6, 2012, at various Defense Logistics Agency (DLA) locations throughout the United States.

Mission Description and Concept of Employment

EProcurement is to provide the DLA with a single, enterprise-wide procurement capability that is more responsive to Services' requirements than the current legacy procurement systems. EProcurement supports the following procurement functional areas: manage purchase requisitions, source and solicit goods and services, manage awards, manage vendor performance, and process receipts and invoices. EProcurement is developed based on a commercial product from SAP[®] and is a critical subsystem of the DLA Enterprise Business System (EBS).

DLA employs EProcurement in an office setting with predominately Government civilian personnel as system users. Each user is assigned one or more roles to perform to support the overall DLA mission of providing consumables, services, and depot-level repairables to the Army, Navy, Air Force, Marine Corps, other federal agencies, and combined and allied forces.

System Description

DLA employees use EProcurement to create and manage contracts for goods, services, and material; track delivery of items to DLA warehouses, and Service and Agency locations worldwide; and ensure that vendor invoices are paid correctly and within required timelines through the Defense Accounting and Finance Service.

The operational concept, which displays the major functionality of EProcurement is contained in Figure 1-1, and is discussed further in this section.

EProcurement Operational Concept

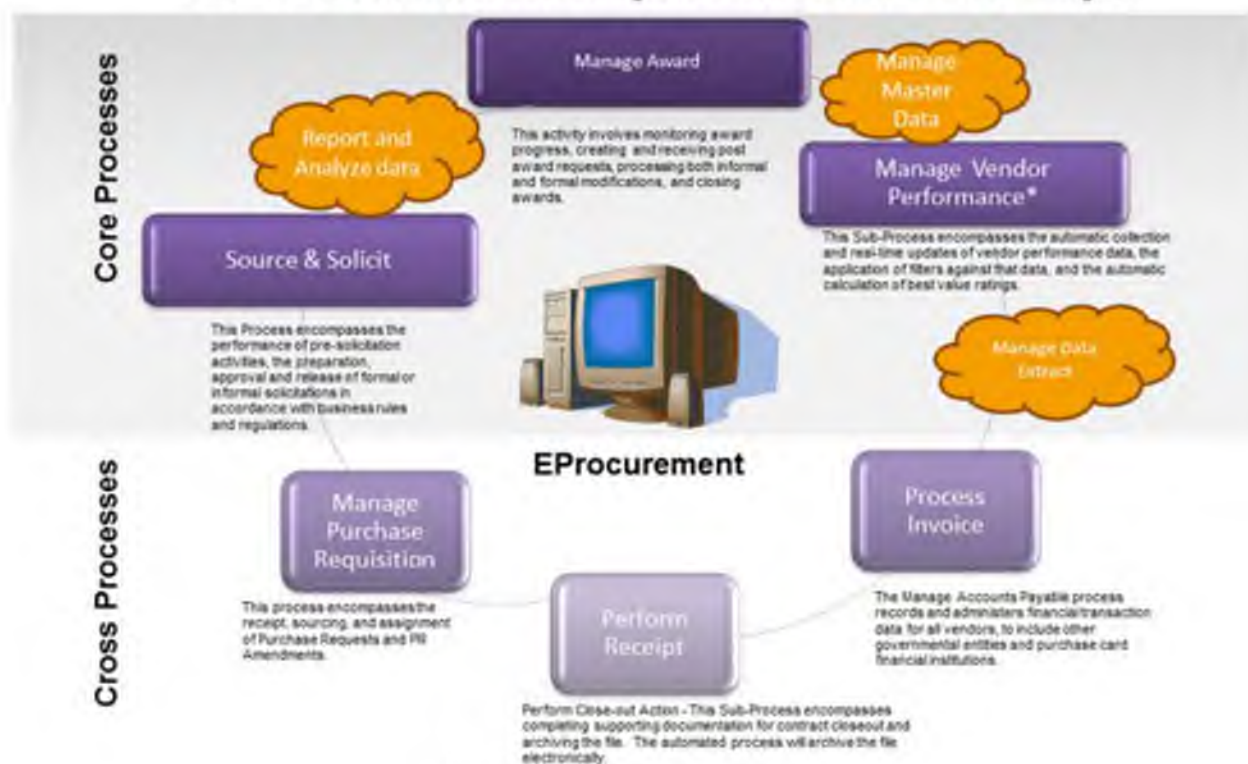


Figure 1-1. Operational Concept

A detailed description of the major functional areas is provided below:

- **Manage Purchase Requisition**
 - Supports the process by which DLA employees receive Purchase Requisitions and any required modifications.
 - Standard Purchase Requisition documents are developed from:
 - Customer Requisitions that cannot be satisfied by current stocked items or existing contract vehicles.
 - Delivery Orders that are requisitions for DLA stocked items.
 - Military Interdepartmental Purchase Requests that are agreements between Services and DLA to provide services/supplies.
- **Source and Solicit (Purchase Requisition fulfillment)**
 - Supports the formal review and validation process for the fulfillment of Purchase Requisitions.
 - Sourcing is the process by which validated Purchase Requisition documents are compared against existing inventory and existing contract vehicles. A

requisition that cannot be fulfilled by existing means is moved into the solicitation process.

- Solicitation issuing processes include pre-solicitation, preparation, approval, and release of solicitations.
 - Solicitation evaluation processes include offer receipt, offer review, negotiation of terms and conditions, and evaluation of price reasonableness and vendor responsibility.
 - Both automated and manual processes are supported during the Source and Solicit process.
- Manage Award
 - Assists DLA employees with the notification process for successful offers (awards pending) and unsuccessful offers.
 - Supports the ongoing contract and modification actions (i.e., monitoring the award progress; formal receipt of post award requests; storing post award actions in the electronic contract files for post-award request actions; processing modifications; and closing awards).
 - Provides data extracts from transactional data to support the compilation of reports.
 - Manage Vendor Performance
 - Supports the transmission of vendor performance data to the Past Performance Information Retrieval System to alert DLA employees of vendor performance issues.
 - Receipt and Invoice
 - Interfaces with the EBS for the execution of Receipt and Invoice functions.

DLA EProcurement Deployment Roadmap

Because EProcurement is replacing existing systems, DLA must populate the EProcurement database with copies of the data contained in legacy databases. In general, the legacy data are not of the same data structures as the new system, and so must be converted to the format of the new system. In addition, there may be some errors in the legacy data, or fields that the legacy system allowed to be blank, but must be filled-in in EProcurement.

To accomplish this data cleansing and conversion to support extension of the EProcurement effort, DLA has developed and instituted a four-step process that must be accomplished prior to porting the converted data into the operational database. The process includes cutover planning, mock conversion testing, data cleansing, and a site readiness assessment. Each of these areas will be detailed so that other Department of Defense (DoD) business systems can benefit from these best practices.

Cutover Planning

The process of bringing legacy data into EProcurement begins with DLA creating a roadmap that contains detailed tasks, dependencies, dates, and responsible persons for activities necessary to deploy EProcurement. The steps required for cutover planning are:

- Establish plans to conduct multiple, full-volume mock cutovers that are used to validate cutover processes and data conversion timeframes ahead of the production cutover, which include the following steps.
 - Data conversion and validation – the types of data to be converted, the amount of data to be converted for each type, estimated timeframes to convert the data, resources required for data validation, and the time to validate each data type.
 - Technical system setup (network, hardware, and software), transport management (in some cases new software code will be included in a cutover which will need to be transported to production), and verification (steps developers need to take to verify the code was migrated to production properly).
 - Manual data setup and manual configuration – these steps include identifying all of the tables that will need to be populated or updated during the cutover, and the software configurations that will need to be established or updated (an example of a configuration is a drop down box where a developer enters all of the options for that drop down box).
- Conduct regular meetings with all teams involved in cutover execution – multiple meetings are conducted well in advance of the cutover to review and refine the cutover plan.
- Conduct at least two meetings with all individuals with cutover execution responsibilities during which every line of the cutover plan is reviewed for the following items.
 - Ownership – resource responsible for a specific task.
 - Dependencies – a task that has a dependency with another task.
 - Execution duration – time to execute the task.
 - Clarity – an understanding of the specific task to be accomplished.
- Executive binders are used during cutover weekend and provide information on the following items.
 - Cutover schedule – a graphical depiction of the overall schedule.
 - System downtime – timeframe(s) when systems will be off-line and unavailable to the user community.
 - Data validation schedule – timeframes when resources will be required to validate the results of the data conversions.

- Executive Status call information – periodic calls (typically one per day) are established with the Executives to provide cutover and conversion status.

Mock Conversion Testing

After the appropriate DLA executives approve the cutover plans, the mock conversion test is scheduled and executed. Mock conversion testing confirms extract logic, data collection, and load process for converted data and ensures that data were converted in accordance with the design. This iterative process takes place ahead of each production rollout. Significant events and activities that occur during the mock conversions are:

- Multiple mock conversions are scheduled prior to each rollout. The number of mock testing cycles is determined based on several criteria to include the amount of new software code that is being deployed, and the volume and complexity of the types of data that will be migrated. Exit criteria or success factors are established for each of the mock conversions ahead of each test cycle.
- Testing includes iterative testing of full volume conversion routines, including data extraction (extracting data from the legacy system), data collection (formatting the extracted data for the new system), load (loading the data into the new system), and validation (validating the data loaded in the new system are correct).
- Dependencies between conversion data types and program run times are confirmed, which serve as inputs to cutover planning and performance tuning. In some cases, testing indicates that certain conversion programs run longer than expected and need to be tuned to run faster; in other cases, testing identifies a dependency between data types that must be factored into the overall cutover plan. For example, Purchase Request data must be converted into the new system prior to Purchase Order data.
- Records that fail during a mock conversion test are researched to determine the reason for failure and possible steps to resolve the failure.
- All mock conversion tests include technical validation by the conversion team where data records extracted and collected are compared to data loaded and validated to ensure there are no issues with the end-to-end process.
- Mock conversion tests also include business validation by the Business Process Analysts (BPAs) throughout the mock cycles. BPAs are functional resources who compare the data from the legacy system with the data converted into the new system to ensure the data are accurate and complete from a functional perspective.

Data Cleansing

The next step in the process, Data Cleansing, promotes high quality and integrity of data slated for conversion to EProcurement prior to going live. The process involves identifying discrepant data records subject to conversion to EProcurement and assigning subject matter experts to cleanse the data in the source system ahead of data conversion. Throughout the process, the data-cleansing progress is tracked closely and reported frequently prior to each rollout. To accomplish the data cleansing process, the following steps are executed:

- Functional resources identify areas of conversion data that require data cleanup prior to data conversion/migration. These personnel sample the data in the legacy system to identify specific data records that need to be updated or modified prior to cutover.
- The data cleanup effort is prioritized by the date when the data are slated for rollout.
- The cleanup effort is monitored and tracked to a specific schedule. Checkpoints are included within the overall cutover plan to track progress, and the frequency of checkpoints varies from monthly to weekly, depending on the time remaining before the rollout.

Site Readiness Assessment

The final step in preparation for importing the cleansed data into the production database is the assessment of site readiness. Site readiness planning involves preparing the sites and key stakeholders for go-live and post go-live activities, the standup of the go-live support structure and logistics, and the transition of teams into the deployment execution state. This site readiness assessment consists of the following activities:

- Developing a Site Rollout plan that includes detailed tasks required to complete ahead of the production rollout. Sample tasks include ensuring users have requested access to the new system, and user desktop software has been updated to accommodate the new system.
 - Weekly Site Readiness meetings are conducted where site deployment leads provide progress against the plan. The site deployment lead is also responsible for reporting status to their local Command.
- Developing the process for and conducting Executive checkpoints and flash calls. As mentioned earlier, checkpoint calls are conducted throughout the cutover on a daily basis to track progress of the cutover. Flash calls are then conducted for a few days after cutover to track the progress of the deployment, to track issue resolution, and to ensure users are productive and the system is stable.

Section Two

Test Adequacy

The operational testing of EProcurement was adequate to support an evaluation of system operational effectiveness and operational suitability. An information assurance evaluation was adequate to determine the security posture of both EProcurement and its hosting site — the Defense Information Systems Agency (DISA) Defense Enterprise Computer Center (DECC) in Ogden, Utah. However, no financial security testing was performed.

Operational Testing

The Initial Operational Test and Evaluation (IOT&E) involved approximately 300 Defense Logistics Agency (DLA) EProcurement users executing a wide range of system capabilities while performing their day-to-day missions. During the IOT&E, personnel from the Joint Interoperability Test Command (JITC) obtained data by direct observation of near 1,400 user actions that spanned the range of EProcurement capabilities. In addition, JITC personnel also collected user survey data to assess system usability and Help Desk data to evaluate supportability.

Test Limitations

Because the IOT&E was executed on the live system, there was limited ability for data collectors to observe specific tasks beyond those tasks required by the daily operations at each site. Fourteen of the 66 interfaces between EProcurement and other systems were either not activated or did not have any activity during the test period. These interfaces need to be evaluated in follow-on testing prior to full deployment. No data were collected against 2 (Defense Contract Management Agency Formal Modifications and Good Receipt/Invoice Processing via Wide Area Workflow) of 19 operational effectiveness evaluation areas. DLA indicates that these untested capabilities have a low execution rate in production, but we suggest that they be evaluated in future testing.

Looking forward, thorough regression testing will be needed for new EProcurement software releases. The current manual testing process involves hundreds of test scripts executed manually by dozens of testers and require months to complete. Automating this test process could increase the efficiency of the regression test process and better likelihood of identifying errors in the software.

This page intentionally left blank.

Section Three

Operational Effectiveness

EProcurement is operationally effective. Users were able to accomplish all necessary job functions with only minor errors reported in 13 of 1,363 observed mission performance related tasks.

The effectiveness evaluation concentrated on the users' ability to employ EProcurement to manage purchase requisitions, source and solicit goods and services, manage awards, process receipts and invoices, create reports, and maintain system data (data cleansing and conversions). In addition, Joint Interoperability Test Command (JITC) collected data to determine the degree of productivity change with EProcurement versus legacy systems, and theft and fraud protection and detection. Only limited data were available on these last two areas, and we recommend that the Defense Logistics Agency (DLA) further define processes and procedures to address these areas.

Tables in this section and throughout the report will be used to provide a graphical view of results with color-coding to indicate where an evaluation area met the user-stated threshold of performance (green), did not meet the required threshold (red), or either was not tested or insufficient data were collected to determine resolution (white). In addition, we identify any measures in the tables that are system Key Performance Parameters (KPP) as such.

Mission Accomplishment

DLA is the primary provider of goods, services, and material to support the armed Services and other DoD Agencies logistics needs including clothing and textiles; food and other consumables; petroleum and oil lubricants; and spare parts to ensure weapon system mission capability.

DLA employees uses EProcurement to create and manage contracts for goods, services, and material; track delivery of items to DLA warehouses and Service and Agency locations worldwide; and ensure that vendor invoices are paid correctly and within required timelines through the Defense Accounting and Finance Service.

Mission Performance

As stated earlier, JITC observed users performing these tasks during normal operations, and recorded 1,363 observations of mission successes and failures. JITC recorded 13 failures during the test, resulting in a 99 percent success rate. All task failures were attributable to minor system annoyances (added blank lines to some documents, for example), or had operational workarounds acceptable to the users.

JITC codified all failed tasks in incident reports and assigned a Priority (aka Severity) level by the Data Authentication Group (DAG), consisting of JITC testers and DLA user representatives as voting members, and DOT&E representatives as non-voting members. The DAG categorized all the incident reports in accordance with the Institute of Electrical and Electronics Engineers Standard 12207.2, *Software life cycle processes – Implementation*

considerations, dated April 1998. JITC generated 29 incident reports during the test. No Priority 1 or Priority 2 (major impact) incidents were reported, but seven Priority 3 (moderate impact), 20 Priority 4 (minor impact), and two informational incidents were reported. Five Priority 3 and seven Priority 4 incidents remain unresolved. All of the open Priority 3 incidents have operational workarounds acceptable to the DLA users. Table 3-1 contains the criteria and definitions that were used to determine the operational impact of each incident report.

Table 3-1. IEEE Standard 12207.2 Definitions

Severity Level	Applies if a problem could	Potential Operational Impact
1	a. Prevent the accomplishment of an essential capability b. Jeopardize safety, security, or other requirement designated "critical"	Major
2	a. Adversely affect the accomplishment of an essential capability and no workaround solution is known b. Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, and no workaround solution is known	
3	a. Adversely affect the accomplishment of an essential capability, but a workaround solution is known b. Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, but a workaround solution is known	Moderate
4	a. Result is user/operator inconvenience or annoyance, but does not affect a required operational or mission-essential capability b. Result in inconvenience or annoyance for development or maintenance personnel, but does not prevent the accomplishment of the responsibilities of those personnel	Minor
5	Any other effect	None

Manage Purchase Requisitions

EProcurement users correctly completed 179 out of 180 purchase requisitions (99.4 percent success rate). These requisitions were further categorized as either workload management (126 of 127 completed error-free for a 99.2 percent success rate) or manual purchase (53 of 53 deemed to be accurate, complete, and usable to accomplish required tasks for a 100 percent success rate). The lone failed workload management item was a cancelled purchase request still showing as active in the workload, which was resolved subsequently. Table 3-2 below contains these data along with their associated thresholds.

Table 3-2. Evaluation of Purchase Requisitions Management

Description	Total Samples	Total Success	Total Failures	Success Rate (%)	Required Threshold (%)
Workload Management	127	126	1	99.2	90
Manual Purchase Request Accuracy, Completeness and Usability (KPP)	53	53	0	100.0	80

Source and Solicitation

EProcurement users successfully completed 128 of 130 (98.5 percent success rate) manual and automatic actions involving sourcing and solicitation of goods and services. The solicitations were further examined using four sub-categories: manual sourcing and solicitation; accuracy, completeness, and usability of manual sourcing data; accuracy, completeness, and usability of automated sourcing data; and accuracy, completeness, and usability of data for automated evaluation processing.

Users successfully completed without error 57 of 59 (96.6 percent success rate) manual source and solicitation activities. One of the two failed observations, a Priority 4 incident with minimal operational impact, was caused by a known incompatibility between EProcurement and Microsoft Office Word® 2010 Service Pack 1 and required the user to uninstall the Service Pack. The other failed observation, a Priority 3 incident report, involved a user being unable to combine two purchase requests into one solicitation. A system change request to resolve the issue will be implemented in a future maintenance release.

Table 3-3 shows the results of the source and solicitation observations.

Table 3-3. Source and Solicit

Description	Total Samples	Total Success	Total Failures	Success Rate (%)	Required Threshold (%)
Manual Source and Solicitation	59	57	2	96.6	90
Manual Source and Solicitation Accuracy, Completeness, and Usability (KPP)	32	32	0	100.0	80
Automated Source and Solicitation Accuracy, Completeness, and Usability (KPP)	21	21	0	100.0	80
Automated Evaluation Processing Accuracy, Completeness, and Usability (KPP)	18	18	0	100.0	90

Manual Award Management

Users successfully completed without issues 823 out of 833 (98.8 percent success rate) manual award management processes. Manual award management is further examined using nine sub-categories: manual award management; accuracy, completeness, and usability for awards exceeding \$150,000; accuracy, completeness, and usability for awards less than \$150,000; accuracy, completeness, and usability for automated awards; formal contract modifications; accuracy, completeness, and usability of formal modifications; accuracy, completeness, and usability of Defense Contract Management Agency (DCMA) formal modifications; informal modifications; and electronic delivery order processing.

In the manual award sub-area, users successfully completed 343 of 348 actions (98.6 percent success rate). The five failed actions were documented in two Priority 3 and two Priority 4 incident reports, with one Priority 3 and one Priority 4 incident remaining unresolved. The unresolved Priority 3 issue is the presence of extra blank lines and poses minimal operational impact because these lines can be ignored. The unresolved Priority 4 incident involved a user getting an unexpected error message while preparing a purchase order that was subsequently completed with no operational impact.

For manual award management both above and below \$150,000 as well as automated award management, no issues were observed and all data were verified as being accurate, complete, and usable. Because DLA created very few manual awards above \$150,000 during the test period, only three assessments were recorded. For formal modifications, users successfully generated 266 out of 270 formal modifications (98.5 percent success rate) with all 58 records

evaluated for accuracy, completeness, and usability being deemed error-free.³ Three Priority 4 incident reports were generated for the failed formal modifications, with two incident reports remaining open. The impact to operations of the open reports is minimal.

No DCMA formal modifications were done during the six-week test period, so the ability of the system to support this capability is unresolved from an operational perspective. However, the impact to continuing operations should be minimal, as DLA identified these actions as occurring infrequently in production.

For information modification, users successfully complete all nine. Although statistical confidence is below the desired 80-percent level (61 percent confidence that the threshold of 90 percent will be met in the long term), the infrequency of this activity in operations does not create any serious concern that unanticipated problems in this area will occur in the future.

For electronic delivery, users successfully completed without issue 26 out of 27 attempts (96.3 percent success rate), with the lone failure caused by the DoD Activity Address Code not being populated in the electronically-processed delivery order. A Priority 4 incident report and a trouble ticket were opened for this issue and both were subsequently resolved.

Table 3-4 shows the results of the manual award management observations.

³ A formal modification is a change to a purchase order, delivery order, or contract that requires the use of a standard form (SF-30). It is typically used when changing something substantial on the original order or contract like a delivery date, quantity, or adding or deleting lines. An informal modification is a change to the order or contract that is not substantial and does not require the use of the SF-30.

Table 3-4. Manual Award Management

Description	Total Samples	Total Success	Total Failures	Success Rate (%)	Required Threshold (%)
Manual Award Management	348	343	5	98.6	90
Manual Award Management (in excess of \$150K) Accuracy, Completeness, and Usability (KPP)	3	3	0	100.0	90
Manual Award Management (less than \$150K) Accuracy, Completeness, and Usability (KPP)	97	97	0	100.0	90
Automated Award Management Accuracy, Completeness, and Usability (KPP)	21	21	0	100.0	90
Formal Modifications	270	266	4	98.5	90
Formal Modifications Accuracy, Completeness, and Usability (KPP)	58	58	0	100.0	90
DCMA Formal Modifications Accuracy, Completeness, and Usability (KPP)	0	0	0	No data collected	90
Informal Modifications	9	9	0	100.0	90
Electronic Delivery Order Processing Completeness	27	26	1	96.3	90

Invoice and Goods Receipts

JITC collected data on the ability of EProcurement users to process invoices and acknowledge the receipt of goods. Although the DOT&E-approved test plan called for both manual processing of goods receipt and invoices as well as processing via Wide Area Workflow, users did not execute any transactions involving the latter method during the test period.⁴ All 57 of the attempts to process invoices manually were successful. Table 3-5 displays the results of this assessment.

⁴ Wide Area Workflow is a secure web-based system for electronic invoicing, receipt, and goods acceptance. The Wide Area Workflow allows Government vendors to submit and track invoices and associated documents over the Internet, and allows government personnel to process those invoices in a real-time, paperless environment.

Table 3-5. Invoice and Goods Receipts

Description	Total Samples	Total Success	Total Failures	Success Rate (%)	Required Threshold (%)
Manually Process Goods Receipt and Invoice	57	57	0	100.0	90
Goods Receipt and Invoice Processing via Wide Area Workflow	0	0	0	No data collected	90

Reports

Users generated 35 reports successfully and without error. Report generation capability indicates no operational issues that could affect continuing DLA operations

Data Maintenance

All 128 observations of the user's ability to update and maintain data (master and transactional) critical to the mission accomplishment of procurement activities were successful. In this context, data maintenance encompasses the functions of records management processing, case management, records and case management conversion, clauses and form conversion, and master data maintenance.

Interoperability

DOT&E evaluates the interoperability of EProcurement with other DoD business systems favorably with no failures recorded in 440 transactions involving 30 operational outbound interfaces and 339 transactions involving 22 operational inbound interfaces. We did not assess seven additional outbound interfaces and seven inbound interfaces for various reasons, including deferment of interface activation by DLA, erroneous inclusion of legacy interfaces in the test plan, and lack of transaction activity. DOT&E recommends that in future testing JITC and DLA evaluate all untested interfaces that will be part of the full deployment.

This page intentionally left blank.

Section Four Operational Suitability

EProcurement is operationally suitable, but with deficiencies in the areas of training, usability, Help Desk operations, and system supportability. During operational testing, EProcurement exceeded reliability thresholds of 228 hours for mean time between critical failures (MTBCF) and system operational availability of 0.95.

User surveys indicated that as a group both typical users and Business Process Analysts (BPAs) were not satisfied with the overall user-friendliness and usability of the system. Typical users, but not the BPAs, were also critical of the quality of training and training aids the Defense Logistics Agency (DLA) provided.

The time required to resolve EProcurement Help Desk tickets exceeded 8.5 days on average, which indicates that additional Help Desk training may be needed.

Finally, DLA must continue to pursue test automation in order to support future releases of EProcurement and other business software to improve system supportability and reduce the potential for coding errors being introduced to future software releases.

Reliability, Availability, and Maintainability

The evaluation of this area was supported by four subareas: Reliability, Availability, Maintainability, and Incident Maintainability. The last item examined the time required to close trouble tickets against EProcurement based on Help Desk calls.

The Defense Enterprise Computer Center (DECC) in Ogden, Utah, reported a 10-minute network outage that affected all EProcurement users, and DLA reported one site-specific outage at Battle Creek, Michigan, which lasted 1 hour and 55 minutes. Neither issue significantly affected system availability, with the EProcurement enterprise as a whole meeting the operational availability requirement of 95 percent uptime (99.98 percent for the enterprise and 99.8 percent for Battle Creek). In addition, the system met the maintainability requirement to reestablish system operations within 12 hours of an event.

Because the DECC outage did not last more than 12 hours, there were no chargeable critical system failures.⁵ The required MTBCF of 228 hours was met.

The specific cause and corrective action for the Battle Creek outage were as follows (extracted from an email sent to the Joint Interoperability Test Command (JITC) Test Director from the DLA Test Lead):

"While testing the fire alarm system, DLA Installation Support contractor personnel tripped the main breaker that powers the network and server equipment racks in our computer facility. As a result, all equipment in the room went down hard. Once the breaker was reset, all equipment came back on line except for the Enterprise Telecommunications Network (ETN) Core 3 router. We contacted the Network Operations Security Center (NOSC) for troubleshooting. The Small Form-factor Pluggable (i.e. fiber module) interface on ETN equipment was down.

⁵ A critical system failure is defined by DLA as a system-wide outage that prevents processing of Priority Group 1 orders for 12 hours or more. Priority groups are defined in internal DLA policies.

The NOSC had the wrong information on their diagram as to the correct port that Battle Creek was plugged into on their router. Team Battle Creek called the NOSC after seeing the interface not working and had the NOSC activate the correct port. The NOSC then provided the correct port information for the NOSC to update their drawings.

After Action task (completed): The NOSC has fixed their diagram and has provided the Telecom team instructions on what to look for after a power outage.”

While this may be an isolated incident, it is prudent for DLA to examine the remaining network drawings at each NOSC to verify the completeness and correctness of those drawings.

JITC obtained copies of Help Desk logs to attempt to determine the closure rates of trouble tickets opened against the EProcurement system. Help Desk trouble ticket resolution is slow. During the IOT&E, 286 trouble ticket tickets considered as “Medium” priority or above were opened against the EProcurement system, of which 18 remain unresolved as of May 9, 2012. The Help Desk considers a trouble ticket as resolved if a fix action was implemented that they believe resolves the problem, but often they keep the ticket open (resolved, but not closed) for another week or so to verify that the problem does not recur. The Help Desk prioritized all of these tickets medium priority. Difficulty separating EProcurement issues from Enterprise Business System (EBS) problems prevented collection of reliable data on the number of low-priority tickets. Our analysis of the closure rates for the tickets shows that the time required to resolve trouble tickets was approximately 8.5 days, with resolution times ranging from less than 5 minutes to nearly 40 days.

While a reason for the large spread in resolution rates has not yet been determined, one possible cause could be the lack of familiarity of the Help Desk with identifying and solving EProcurement issues. In addition, the methodologies JITC used to query the database, with DLA assistance, cannot be effectively used with the historical data in the Remedy[®] system for trend analysis with respect to system problems, nor for workload analysis to determine if more Help Desk support is needed. This information could be especially useful to DLA when new sites or user groups are added to the EProcurement workflow.

DOT&E believes that the wealth of information contained in the trouble ticket database could be a useful tool for DLA to more effectively manage problem resolution and conduct trend analysis. To this end, DLA should modify the method of identifying trouble tickets in the Remedy system to better allow for data queries by program (EProcurement versus EBS, for example). DLA should also track at least the average and maximum resolution times of system problems on a monthly or at least quarterly schedule to aid DLA management in identifying potential problem areas so that they can implement strategies before productivity is affected.

Usability

The usability assessment is based primarily on the user responses to survey questions administered in person by a member of the JITC test team. Two sets of respondents were included in the surveys. The first set comprised typical EProcurement users with anywhere from a few months to more than a year of experience with the system, while the second set comprised

experienced BPAs whose job it is to provide first-level assistance to users to resolve task issues and who determine when additional support through the DLA Help Desk is needed.

Four subareas supported the evaluation of overall usability (training, documentation, and user satisfaction with system operation); user logon and screen refresh time; Help Desk adequacy; and ability to perform the critical tasks required to support the mission.

Table 4-1 shows the user responses for survey questions addressing overall usability. The usability survey used a four-point Likert scale. The desired positive response rate was set at 80 percent, per the DOT&E-approved test plan. Analysis of the user responses shows that while the general user responses did not meet the 80 percent threshold, the BPA responses did, leading one to conclude that the added proficiency of the BPAs using EProcurement might have contributed to increased satisfaction with system training and documentation. In any case, DLA should re-evaluate the adequacy of training quality for the average user, and include role-specific training in the future when DLA transitions users at the remaining DLA sites to EProcurement.

Table 4-1. Usability Survey Results

Question	Users		BPAs	
	Total	Percent Positive	Total	Percent Positive
How adequate was training in assisting you to use the system and perform your job?	91	63	13	100
Rate the adequacy of the user training materials to provide you with the information you require to perform your job.	83	60	12	100
Rate the adequacy of the job aids (online help) to enable you to use EProcurement in accomplishment of your job.	71	61	13	92

In addition to the survey results shown in Table 4-1, JITC also assessed system ease of use and the degree to which users and BPAs felt they could easily use the system to perform their tasks. The survey was set up using a System Usability Scale (SUS) that queried users with both positive and negative statements about the system and computed an overall SUS score using a prescribed algorithm.

Table 4-2 contains the aggregated results of the EProcurement usability surveys for 91 typical users and 13 BPAs. The top set of responses for each survey question shows responses from the typical users, while the bottom set is the BPA responses.

Table 4-2. SUS Results

Question	Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Strongly Agree
	1	2	3	4	5
I like to use the EProcurement system to complete my job	30	17	25	13	6
	0	1	5	5	2
I find the EProcurement system unnecessarily complex	4	13	15	20	39
	0	2	3	5	3
I think the EProcurement system is easy to use	30	29	16	12	4
	4	3	3	2	1
I frequently need technical support to be able to use the EProcurement system for my job	6	27	23	21	14
	1	4	5	2	1
I find various functions in the EProcurement system are well integrated	22	20	28	15	6
	2	1	4	6	0
I think there is too much inconsistency between various functions in the EProcurement system	4	15	22	26	24
	1	5	1	5	1
I think that most people learn to use the EProcurement system very quickly	37	28	13	8	5
	5	4	3	0	1
Most people find the EProcurement system very cumbersome to learn and use	2	8	18	29	34
	1	2	0	6	4
I feel confident using the EProcurement system	9	17	28	29	8
	0	2	0	8	3
I need to learn a lot of things before I can proficiently use the EProcurement system	4	20	23	32	12
	2	3	2	3	3

Applying the SUS algorithm and averaging gives an aggregate score for each group as

Users: 36.7

BPAs: 46.7.

Using the criteria established in the literature for SUS evaluations, the desired threshold for satisfaction was that 67.5 percent of respondents rate a SUS of 75 or higher.⁶ While the BPAs rated the EProcurement system more highly than the average user, significant difficulty exists in all groups with regard to system navigation and ease of use. It is interesting to note that 7 of the 91 users did rate EProcurement with a SUS score of 75 or greater, while none of the BPAs did. We believe that much of the dissatisfaction might be a result of having to learn a new system, and the level of difficulty experienced by the users with EProcurement is similar to that experienced by other Enterprise Resource Planning users of DoD systems.

DOT&E recommends that JITC administer the survey periodically after IOT&E to all EProcurement users through full deployment, and the SUS scores for users subdivided by length

⁶ Details of the SUS method can be found in "A Comparison of Questionnaires for Assessing Website Usability," Thomas S. Tullis and Jacqueline N. Stetson, Human Interface Design Department, Fidelity Center for Applied Technology, 82 Devonshire St., V4A, Boston, Massachusetts 02109.

of time using EProcurement to perform user operations, to see whether user satisfaction does improve with increased system use or whether a more inherent issue exists with system usability.

User Logon and Screen Refresh Time

Data collected for system logon time using system logs show in each case that users were able to log onto the system in 10 seconds or less, which is adequate for continued mission operations. The average and median connect times to log onto the SAP system were 2.96 seconds and 2.26 seconds, respectively, based on 732 hours of log data.

Automated data logging of user activities to support performance monitoring of system responses from the user perspective were non-existent. Although the desire was to see as much of this screen refresh data as possible collected automatically, the available logs and other tools did not provide enough traceability back to user actions, so human observations of the tasks performed, combined with stopwatch measurements, were used to obtain the statistics on screen refresh. This level of manual activity will not support monitoring of these performance metrics by DLA. DOT&E recommends continuous monitoring capabilities for performance metrics: automated data capturing should be built into the system early for all performance requirements, and testing those requirements at IOT&E should simply be a matter of displaying the status of automated reports.

Even without automated data collection for screen refresh, 2,727 separate timed events encompassing all aspects of EProcurement activities at the IOT&E test locations were observed and refresh times recorded. Average time to refresh was 12.6 seconds (versus a threshold of 15 seconds) with a median refresh time of 6.0 seconds. Seventy-four percent of all measured responses were below the 15-second threshold. Many refreshes were nearly instantaneous, while those requiring significant input or output activities to the database (data save, for example) took significantly longer, with the maximum recorded time being longer than 4 minutes (257 seconds).

Help Desk

The BPAs' job is to provide primary support to the users, and, if the BPA cannot resolve the problem, to call the Help Desk on the user's behalf. For this reason, JITC surveyed only BPAs regarding Help Desk adequacy. Ten BPAs responded to the survey question, with all BPAs rating Help Desk support as adequate.

Critical Tasks Performance

Typical users indicated difficulty in using EProcurement to accomplish their assigned tasks. JITC surveyed both typical users and BPAs regarding the degree to which EProcurement is effective in supporting critical mission tasks. Table 4-3 contains the response data for the 91 users and 13 BPAs surveyed. Color-coding corresponds to 80 percent user agreement that the task was effective or better (green), between 75 and 80 percent agreement (yellow), or below 75 percent agreement (red). As before, the top set of responses for each survey question shows responses from the typical users, while the bottom set is the BPA responses.

Table 4-3. User Rating of System to Support Mission Tasks

Question	N/A	Very Ineffective	Ineffective	Effective	Very Effective	Percent Positive
Manage Purchase Requisitions	20	8	21	36	6	59
	3	0	2	3	5	80
Support Solicitations	22	10	22	34	3	54
	3	0	1	6	3	90
Support Evaluations	55	4	14	15	3	50
	9	0	1	3	0	75
Support Delivery Order Processing	31	5	15	35	5	67
	4	0	0	6	3	100
Support Award Processing	17	5	23	42	4	62
	3	0	1	6	3	90
Support Post-Award Processing	33	9	16	29	4	59
	3	0	1	9	0	90
Goods Receipts	70	6	6	7	2	43
	9	0	1	0	3	75
Invoices	72	7	4	8	0	42
	9	0	1	0	3	75

As shown in the table, BPAs generally agreed that the system supports mission elements, although the sample size was quite small. In addition, the typical users rated the system less positively than the BPAs, with significant differences in how the two groups view evaluation support and delivery order processing. Goods Receipts and Invoices also showed a marked difference, but the small sample sizes make definitive conclusions difficult. Finally, note that the responses denoted as “N/A” (not applicable) reflect the DLA stratification of users’ roles and that not all EProcurement users perform the same set of tasks.

Finally, DOT&E is concerned that DLA does not have a robust automated test capability to perform a thorough regression test on new EProcurement software releases. Observations show that DLA uses a manual process to perform regression testing, with hundreds of test scripts executed manually by dozens of testers and require months to perform. Our view is that this level of human activity has the potential to fail to identify latent errors in the updated software, and could conceivably lead to severe mission impacts if not automated.

To this end, DLA instituted a pilot program with JITC to demonstrate that they can automate one or more current test scripts and execute it using commercially available software designed to functionally test the EProcurement and EBS systems. Based on the success of the pilot program, DLA should now implement a more formal automated test program that again is expected to yield a model for other DoD entities to follow and become the standard within the DoD.

Section Five Survivability

The EProcurement system is survivable against cyber threats but might be vulnerable to financial theft and fraud threats. The system is secure from an information assurance perspective. Only three security findings remain unresolved, with the operational impact of these issues considered as moderate to low by DOT&E.

No financial theft and fraud threat testing was conducted. The Defense Logistics Agency (DLA) must ensure the protection of the Enterprise Business Systems (EBS), of which EProcurement is now a part, against financial theft and fraud threats. As part of this effort, DLA should establish a Theft and Fraud Prevention and Detection Red Team modeled after those used to probe for information assurance vulnerabilities.

Information Assurance

The EProcurement system as tested is secure from an information assurance perspective. The information assurance evaluation examined the security posture of the Defense Enterprise Computer Center (DECC) hosting the EProcurement using four criteria: the ability to protect against unauthorized penetration of the DECC and EProcurement; the ability to detect when such exploits are made; the existence of adequate and appropriate system and personnel reaction to intrusion attempts; and the ability to restore normal system operations after a disruption.

JITC information assurance testers, along with members of the Defense Information Systems Agency Field Security Office (DISA-FSO) and DLA Computer Emergency Response Team (CERT), conducted a series of three Penetration and Exploitation (P&E) events at the DECC located in Ogden, Utah.

The information assurance team executed the first P&E event in August 2011 on EProcurement Release 1.1 and identified 16 information assurance issues, of which the team rated 9 as posing high risk to system security. The team executed the second P&E event in February 2012 on EProcurement Release 1.2, and identified 17 issues, of which 6 were still open from the earlier P&E event. The team rated five issues as posing high security risk after this event.

The team executed the final P&E event in March 2012 during the IOT&E. While no high risk information assurance issues were discovered, 11 issues from the previous P&E testing remain open with five posing moderate risk, three posing low risk, and three considered as informational (that is, suggestions for security improvement versus actual security deficiencies). DISA and DLA created a plan of action and milestones to address resolution of these issues. As of the date of this report, one moderate risk issue and two low risk issues remain open.

The open information assurance issues were assessed for their effect on the ability of the DECC to protect against intrusion, to detect when intrusions are attempted, to react to such attempts, and to restore system operations after an intrusion event. The areas of protect, detect,

and react all had findings against them, albeit minor ones, while the restore area was determined to have no known issues.

Although few of the vulnerabilities identified by the information assurance team remain unresolved, the DISA-FSO and DLA CERT should periodically re-evaluate the security posture of the DECC and the EProcurement as part of the overall defense-in-depth security strategy.

Theft and Fraud Protection and Detection

To assess DLA's ability to protect against fraudulent activities, to detect when suspect activities occur (including detection of counterfeit procurement items), to react to detected activities, and to restore the system if needed to a state prior to the theft or fraud occurrence, DOT&E directed that measures designed to test theft and fraud protection and detection at DLA be added to the test plan and scenarios developed and executed to provide data to perform the assessment.

DOT&E was unable to verify that DLA has a robust theft and fraud prevention and detection program. DLA asserts that by using role separations, at least two to three people would need to be involved in any theft or fraud activity and that while large-scale theft or fraud was not impossible, it would be difficult. DLA also indicated that bi-annual audits and other accounting controls are in place to further mitigate such activities. Finally, DLA disclosed various pilot programs, including a Decision Support Capability (DSC), regarding theft and fraud protection and detection. If DLA decides to pursue the DSC, then one outcome will be a Commercial and Government Entity (CAGE) Code Watch List that will be utilized to deter new CAGE code assignments to bad actors or to entities with which the bad actors may be affiliated. (In the past, this was loosely referred to as "cage hopping"). Although any or all of the technologies of the DSC may or may not prove to be cost-effective for DLA (those are DLA business decisions), a CAGE Code Watch List is an urgent operational need.

While DOT&E acknowledged that some level of theft and fraud prevention and detection are available at DLA, the level may be insufficient. DOT&E directed that DLA provide an update to the EProcurement Test and Evaluation Master Plan (TEMP), prior to a full deployment decision review, detailing the steps that will be implemented to ensure adequate theft and fraud protection and detection mechanisms. This TEMP update is an ongoing activity that should be complete in the near future, and DOT&E recommends that other DoD business systems adopt similar theft and fraud prevention and detection mechanisms, using the DLA output as a model.

DOT&E recommends that DLA establish a Theft and Fraud Prevention and Detection Red Team modeled after those used to probe for information assurance vulnerabilities. The team would establish rules of engagement for theft and fraud testing, and as before, the DLA process could become a model for the DoD to use for finance, logistics, and other business system acquisitions.

Section Six Recommendations

DOT&E offers the following recommendations that should be instituted prior to the Defense Logistics Agency (DLA) declaring EProcurement as fully deployed or should be considered as DoD best practices and promulgated to other DoD business acquisition program offices.

- DLA should establish a Theft and Fraud Prevention and Detection Red Team modeled after those used to probe for information assurance vulnerabilities. The team would establish rules of engagement for theft and fraud testing, and the DLA process could become a model for the DoD to use for finance, logistic, and other business system acquisitions. DLA needs to demonstrate this capability through a follow-on operational assessment prior to DLA declaring EProcurement as fully deployed.
- DLA should continue their pilot program to utilize commercially available test automation software designed to functionally test the SAP[®] system. Based on the results of the recent pilot program, DLA should implement a more formal automated test program that again is expected to yield a model for other DoD entities to follow and become the standard within the DoD.
- DLA should improve the quality of training, training aids, and other system documentation for the users, and include role-specific training in the future when DLA transitions users at the remaining DLA sites to EProcurement.
- DLA should modify the method of managing trouble tickets in the Remedy system to better allow for data queries by program (EProcurement versus Enterprise Business System (EBS), for example). DLA should also track the resolution times of system problems on a monthly or at least quarterly schedule to aid DLA management in identifying potential problem areas so that DLA can implement mitigation strategies before productivity is affected.
- JITC should administer the System Usability Scale (SUS) survey periodically to a random sample of all EProcurement users through full deployment to see whether user satisfaction does improve with increased system use or whether a more inherent issue exists with system usability.
- In future testing, JITC and DLA should evaluate all untested interfaces that will be part of the full deployment.
- Although only minor issues remained after the last information assurance test event, the Defense Information Systems Agency Field Security Office (DISA-FSO) and DLA Computer Emergency Response Team (CERT) should periodically re-evaluate the security posture of the DECC and EProcurement as part of the overall defense-in-depth security strategy.



OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JUN 13 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

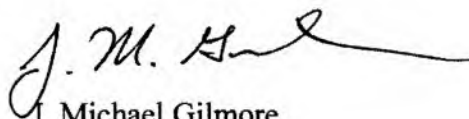
I have attached my IOT&E report on the EProcurement Release 1.2. The report assesses EProcurement, which Defense Logistics Agency (DLA) employees use to create and manage contracts for goods, services, and material; track delivery of items to DLA warehouses and Service and Agency locations worldwide; and ensure that vendor invoices are paid correctly and within required timelines through the Defense Accounting and Finance Service. In the report, I conclude the following:

- The IOT&E of EProcurement was adequate to support an evaluation of the system's operational effectiveness, suitability, and survivability and was conducted in accordance with the test plan I approved.
- EProcurement is operationally effective. Users were able to accomplish all necessary job functions in 99 percent of the 1,363 tasks that were observed. The tasks addressed managing purchase requisitions, sourcing and soliciting goods and services, managing awards, processing receipts and invoices, creating reports, and maintaining system data. Minor errors were reported in 13 of the observed tasks. The 52 system interfaces (of a total of 66 interfaces) evaluated during the test processed all required inbound and outbound data without any recorded failures.
- EProcurement is operationally suitable, but with deficiencies in the areas of training, usability, Help Desk operations, and supportability. During operational testing, EProcurement satisfied the requirements for reliability, availability, and maintainability. However, surveys indicated that users were not satisfied with the training and training material provided, or with the overall user-friendliness and usability of the system. The average time required to resolve EProcurement Help Desk tickets exceeded 8.5 days, which needs improvement. Finally, the lack of an automated capability for regression testing of future releases of EProcurement should be rectified.
- EProcurement is survivable against cyber threats but its ability to detect and prevent financial theft and fraud has not been tested. The system is secure from an information assurance perspective. Only three security findings remain



unresolved at the end of the test, with the operational impact of these issues considered as moderate to low. However, schedule constraints prevented financial theft and fraud threat testing from being conducted during IOT&E. Testing using a financial red team will be conducted subsequently to verify the effectiveness of EProcurement for theft and fraud detection and prevention.

Section 2399, Title 10, United States Code provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have also provided copies to the Under Secretary of Defense for Acquisition, Technology and Logistics; the Director of the Defense Logistics Agency; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Adam Smith
Ranking Member



OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JUN 13 2012

The Honorable C. W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

Dear Mr. Chairman:

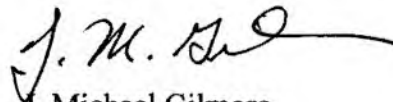
I have attached my IOT&E report on the EProcurement Release 1.2. The report assesses EProcurement, which Defense Logistics Agency (DLA) employees use to create and manage contracts for goods, services, and material; track delivery of items to DLA warehouses and Service and Agency locations worldwide; and ensure that vendor invoices are paid correctly and within required timelines through the Defense Accounting and Finance Service. In the report, I conclude the following:

- The IOT&E of EProcurement was adequate to support an evaluation of the system's operational effectiveness, suitability, and survivability and was conducted in accordance with the test plan I approved.
- EProcurement is operationally effective. Users were able to accomplish all necessary job functions in 99 percent of the 1,363 tasks that were observed. The tasks addressed managing purchase requisitions, sourcing and soliciting goods and services, managing awards, processing receipts and invoices, creating reports, and maintaining system data. Minor errors were reported in 13 of the observed tasks. The 52 system interfaces (of a total of 66 interfaces) evaluated during the test processed all required inbound and outbound data without any recorded failures.
- EProcurement is operationally suitable, but with deficiencies in the areas of training, usability, Help Desk operations, and supportability. During operational testing, EProcurement satisfied the requirements for reliability, availability, and maintainability. However, surveys indicated that users were not satisfied with the training and training material provided, or with the overall user-friendliness and usability of the system. The average time required to resolve EProcurement Help Desk tickets exceeded 8.5 days, which needs improvement. Finally, the lack of an automated capability for regression testing of future releases of EProcurement should be rectified.
- EProcurement is survivable against cyber threats but its ability to detect and prevent financial theft and fraud has not been tested. The system is secure from an information assurance perspective. Only three security findings remain



unresolved at the end of the test, with the operational impact of these issues considered as moderate to low. However, schedule constraints prevented financial theft and fraud threat testing from being conducted during IOT&E. Testing using a financial red team will be conducted subsequently to verify the effectiveness of EProcurement for theft and fraud detection and prevention.

Section 2399, Title 10, United States Code provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have also provided copies to the Under Secretary of Defense for Acquisition, Technology and Logistics; the Director of the Defense Logistics Agency; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JUN 13 2012

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

Dear Mr. Chairman:

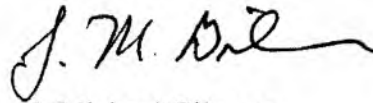
I have attached my IOT&E report on the EProcurement Release 1.2. The report assesses EProcurement, which Defense Logistics Agency (DLA) employees use to create and manage contracts for goods, services, and material; track delivery of items to DLA warehouses and Service and Agency locations worldwide; and ensure that vendor invoices are paid correctly and within required timelines through the Defense Accounting and Finance Service. In the report, I conclude the following:

- The IOT&E of EProcurement was adequate to support an evaluation of the system's operational effectiveness, suitability, and survivability and was conducted in accordance with the test plan I approved.
- EProcurement is operationally effective. Users were able to accomplish all necessary job functions in 99 percent of the 1,363 tasks that were observed. The tasks addressed managing purchase requisitions, sourcing and soliciting goods and services, managing awards, processing receipts and invoices, creating reports, and maintaining system data. Minor errors were reported in 13 of the observed tasks. The 52 system interfaces (of a total of 66 interfaces) evaluated during the test processed all required inbound and outbound data without any recorded failures.
- EProcurement is operationally suitable, but with deficiencies in the areas of training, usability, Help Desk operations, and supportability. During operational testing, EProcurement satisfied the requirements for reliability, availability, and maintainability. However, surveys indicated that users were not satisfied with the training and training material provided, or with the overall user-friendliness and usability of the system. The average time required to resolve EProcurement Help Desk tickets exceeded 8.5 days, which needs improvement. Finally, the lack of an automated capability for regression testing of future releases of EProcurement should be rectified.
- EProcurement is survivable against cyber threats but its ability to detect and prevent financial theft and fraud has not been tested. The system is secure from an information assurance perspective. Only three security findings remain



unresolved at the end of the test, with the operational impact of these issues considered as moderate to low. However, schedule constraints prevented financial theft and fraud threat testing from being conducted during IOT&E. Testing using a financial red team will be conducted subsequently to verify the effectiveness of EProcurement for theft and fraud detection and prevention.

Section 2399, Title 10, United States Code provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have also provided copies to the Under Secretary of Defense for Acquisition, Technology and Logistics; the Director of the Defense Logistics Agency; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.

A handwritten signature in black ink, appearing to read "J. M. Gilmore", with a long horizontal flourish extending to the right.

J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable John McCain
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JUN 13 2012

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6025

Dear Mr. Chairman:

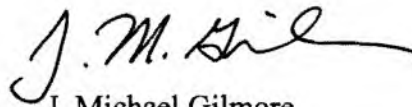
I have attached my IOT&E report on the EProcurement Release 1.2. The report assesses EProcurement, which Defense Logistics Agency (DLA) employees use to create and manage contracts for goods, services, and material; track delivery of items to DLA warehouses and Service and Agency locations worldwide; and ensure that vendor invoices are paid correctly and within required timelines through the Defense Accounting and Finance Service. In the report, I conclude the following:

- The IOT&E of EProcurement was adequate to support an evaluation of the system's operational effectiveness, suitability, and survivability and was conducted in accordance with the test plan I approved.
- EProcurement is operationally effective. Users were able to accomplish all necessary job functions in 99 percent of the 1,363 tasks that were observed. The tasks addressed managing purchase requisitions, sourcing and soliciting goods and services, managing awards, processing receipts and invoices, creating reports, and maintaining system data. Minor errors were reported in 13 of the observed tasks. The 52 system interfaces (of a total of 66 interfaces) evaluated during the test processed all required inbound and outbound data without any recorded failures.
- EProcurement is operationally suitable, but with deficiencies in the areas of training, usability, Help Desk operations, and supportability. During operational testing, EProcurement satisfied the requirements for reliability, availability, and maintainability. However, surveys indicated that users were not satisfied with the training and training material provided, or with the overall user-friendliness and usability of the system. The average time required to resolve EProcurement Help Desk tickets exceeded 8.5 days, which needs improvement. Finally, the lack of an automated capability for regression testing of future releases of EProcurement should be rectified.
- EProcurement is survivable against cyber threats but its ability to detect and prevent financial theft and fraud has not been tested. The system is secure from an information assurance perspective. Only three security findings remain



unresolved at the end of the test, with the operational impact of these issues considered as moderate to low. However, schedule constraints prevented financial theft and fraud threat testing from being conducted during IOT&E. Testing using a financial red team will be conducted subsequently to verify the effectiveness of EProcurement for theft and fraud detection and prevention.

Section 2399, Title 10, United States Code provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have also provided copies to the Under Secretary of Defense for Acquisition, Technology and Logistics; the Director of the Defense Logistics Agency; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.

A handwritten signature in black ink, appearing to read "J. M. Gilmore", with a stylized, flowing script.

J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Thad Cochran
Ranking Member

Global Combat Support System – Army (GCSS-Army), Release 1.1

Initial Operational Test and Evaluation Report



June 2012

This report evaluates the adequacy of testing and the operational effectiveness, operational suitability, and survivability of the GCSS-Army, Release 1.1.

J. Michael Gilmore
Director

The marginal cost of producing this report is estimated to be approximately \$49K. The estimated acquisition cost of the program which this report addresses is \$2.09B.



Global Combat Support System – Army (GCSS-Army)

Executive Summary

This document reports on the evaluation of test adequacy, operational effectiveness, operational suitability, and survivability of the Global Combat Support System – Army (GCSS-Army) Release 1.1. The Initial Operational Test and Evaluation (IOT&E) was adequate to evaluate GCSS-Army. The evaluation is based on data from:

- GCSS-Army IOT&E conducted by the U.S. Army Test and Evaluation Command (ATEC) from August 29 to October 21, 2011
- GCSS-Army Cyber Threat Test conducted by the U.S. Army Threat System Management Office (TSMO) from September 19-29, 2011, and the Program Management Office's (PMO) corrective actions up through March 16, 2012.
- GCSS-Army Continuity of Operations (COOP) Demonstration conducted by the GCSS-Army PMO from November 7-10, 2011

Mission and System Description

GCSS-Army is a Major Automated Information System (MAIS) intended to support force commanders in garrison and when deployed in all theaters of operation and environmental conditions. It provides capabilities for the users to perform materiel management, maintenance management, and property accountability. It also integrates tactical financials into logistics and financial processes, providing an audit trail.

GCSS-Army replaces the legacy logistics Standard Army Management Information System (STAMIS) with a single, web-based system available to users worldwide. GCSS-Army uses a commercial off-the-shelf enterprise resource planning (ERP) system produced by Systems, Applications, and Products in Data Processing (SAPTM) to provide business processes for end-to-end logistics. The SAPTM ERP system was adapted by Northrop Grumman Information Technology to meet Army requirements.

The primary GCSS-Army server center is located at Redstone Arsenal, Alabama, with a backup server center located at Radford, Virginia, that provides a COOP capability. Users access GCSS-Army via Army Knowledge Online (AKO) using their common access cards over the Nonsecure Internet Protocol Router Network (NIPRNet). At full operational capability, GCSS-Army will support 168,000 licensed users across all components of the Army.

Test Adequacy

The GCSS-Army initial operational test, cyber threat test, and COOP demonstration were adequate to evaluate the GCSS-Army critical operational issues and additional test parameters found in the GCSS-Army Test and Evaluation Master Plan (TEMP). However, the system was not stressed with enough users during the IOT&E, and did not reflect scaling (needed server and storage capacity, help desk support, etc.) for the projected number of users. During the test, there were 545 GCSS-Army users, compared to the total expected user population of 168,000 when fully operational. The deployment process is expected to take about three years. The

PMO should continue monitoring the system scaling as more units are fielded. Additionally, the IOT&E did not include Army Reserve or National Guard units. The PMO should conduct testing and evaluation to ensure the system satisfies the unique requirements for the Army Reserve and National Guard units before fielding to these units. The scope of the test should follow the DOT&E guidelines for Operational Test and Evaluation of Information and Business Systems, as documented in the TEMP.

Operational Effectiveness

GCSS-Army is operationally effective as indicated by an overall critical mission function success rate of 99 percent, but needs to comply with the requirements of the Federal Financial Management Improvement Act (FFMIA) of 1996. GCSS-Army demonstrated that it can support Army users in garrison and when deployed. It provided near real time information to all levels of command by integrating the Army's tactical financial system into the property accountability, maintenance, and retail supply systems. Commanders were able to use GCSS-Army to see a unit's equipment readiness, track the status of work order and property book requisitions necessary to improve a unit's readiness status, and verify funds availability at any time. The system logs from the IOT&E period from August 29 to October 21, 2011, revealed no interoperability shortfalls with the Army and Joint trading partners. The GCSS-Army will need to satisfy the National Defense Authorization Act (NDAA) 2010 requirement to be ready for audit by 2017. In order to do so, the GCSS-Army PMO, Assistant Secretary of the Army for Financial Management and Comptroller (ASA FMC), and the Army Audit Agency (AAA) are working to comply with the FFMIA requirements.

Operational Suitability

GCSS-Army is operationally suitable. The GCSS-Army had no system aborts in 1,296 hours of operation, giving 84 percent confidence that the system can satisfy the required 716 hours of operation without a system abort. The system was available 99.4 percent of time compared to the requirement of 95 percent. Training, help desk, and change management were adequate for successful operation and sustainment. However, the IOT&E was conducted with 545 users, including 345 users from the test unit and 200 existing users from Fort Irwin. The Capability Production Document (CPD) predicts the Army will have 168,000 users when fully fielded. Although support was adequate for the 545 users during IOT&E, a study initiated by the PMO indicated that there may be difficulty scaling the system to an increased user base. As the user base will increase by a factor of 300 over the next three years, the PMO needs to continue monitoring and observing the effects additional users have on the system, and should conduct modeling of these impacts, both computational (i.e., server capacity, storage, and bandwidth) and human factors (i.e., help desk support, overhead labor and communications costs, and data noise), so as to project any breakdown in the system.

Survivability

GCSS-Army is survivable against cyber threats. The penetration test conducted by TSMO revealed significant shortfalls for protecting against cyber threats, especially on the Army

Enterprise Systems Integration Program (AESIP). The PMO made fixes since the IOT&E, and the significant issues are now resolved.

Survivability against financial threats remains an open issue.

Recommendations

The PMO should consider the following recommendations in order to ensure operational effectiveness, operational suitability, and survivability throughout deployment:

- Collect data for computational (server capacity, storage, and bandwidth) and human factors (help desk responsiveness, overhead labor and communication costs, and data noise) impacts of an increased user base. Use such data to establish a pattern of demand on the system, so that future demand can be adequately anticipated and resourced as more users come online.
- Test and evaluate future improvements, including deployments to the Army Reserve and National Guard units, in accordance with the September 2010 DOT&E guidelines for Operational Test.
- Develop and implement automated regression testing to continue monitoring software effectiveness for future updates.
- Continue the cooperation with the Army Audit Agency (AAA) to achieve financial auditability as mandated by the 2010 NDAA.
- Work with ATEC to establish a financial red team to conduct tests of the system's ability to prevent and detect theft and fraud.
- Continue with the current plan of updating the DoD Information Assurance Certification and Accreditation Process (DIACAP), including conduct of COOP demonstrations.



J. Michael Gilmore
Director

This page intentionally left blank.

Contents

System Overview 1

Test Adequacy 5

Operational Effectiveness 7

Operational Suitability 11

Survivability..... 15

Recommendations 19

This page intentionally left blank.

Section One System Overview

This document reports on the evaluation of test adequacy, operational effectiveness, operational suitability, and survivability of the Global Combat Support System–Army (GCSS-Army) Release 1.1. The evaluation is based on data from:

- GCSS-Army Initial Operational Test and Evaluation (IOT&E) conducted by the U.S. Army Test and Evaluation Command (ATEC) from August 29 to October 21, 2011
- GCSS-Army Cyber Threat Test conducted by the U.S. Army Threat System Management Office (TSMO) from September 19-29, 2011 and the Program Management Office's (PMO) corrective actions up through March 16, 2012.
- GCSS-Army Continuity of Operations (COOP) Demonstration conducted by the GCSS-Army PMO from November 7-10, 2011

Mission Description and Concept of Employment

The GCSS-Army, a Major Automated Information System (MAIS), provides essential operational sustainment capabilities such as materiel management, maintenance management, and property accountability operations. GCSS-Army integrates tactical logistics financial information into logistics and financial processes, providing an audit trail from the originating logistics event to financial transaction and general ledger account balances. GCSS-Army makes information visible, accessible, and understandable to users and provides Soldiers and sustaining base elements with a responsive and efficient ability to anticipate, allocate, and synchronize the flow of resources, services, and information among sustaining base elements and supported units at the strategic, operational, and tactical force levels.

GCSS-Army will be available at all levels and components of the Army, including the Army Reserves and the Army National Guard. When GCSS-Army reaches its full operational capability, it will be supporting up to 168,000 licensed users across all components of the Army.

GCSS-Army shares data with appropriate Joint information systems to allow for the mobilization, deployment, sustainment, and redeployment of Army Forces and Joint Forces, and provides logisticians with situational awareness from the tactical to national levels by providing in-transit visibility of supplies and services.

System Description

GCSS-Army replaces the legacy, stove-piped logistics Standard Army Management Information System (STAMIS) with a single, web-based, service-oriented system available to users worldwide. GCSS-Army uses a commercial off-the-shelf enterprise resource planning (ERP) system produced by Systems, Applications, and Products in Data Processing (SAPTM) to provide business processes for end-to-end logistics. Northrop Grumman Information Technology is the primary integrator charged with the responsibility to adapt the SAPTM ERP system to meet Army requirements.

GCSS-Army combines five main logistical functions into a single software application: finance/accounting, supply, property accountability, maintenance, and logistics management. GCSS-Army facilitates the flow of information among all internal business processes and also manages the connections and information flows to and from external trading partners such as the Logistics Management Program (LMP) and General Fund Enterprise Business System (GFEBS).

The primary GCSS-Army server center is located at Redstone Arsenal, Alabama, with a backup server center located at Radford, Virginia, that provides a COOP capability. Users access GCSS-Army via Army Knowledge Online (AKO) using their common access cards over the Nonsecure Internet Protocol Router Network (NIPRNet). GCSS-Army is to be used in garrison and when deployed, and connectivity to the NIPRNet will be via either the Defense Information Systems Network (DISN) land line or the Combat Service Support Automated Information Systems Interface (CAISI) very small aperture terminal (VSAT) satellite link. (See Figure 1-1.)

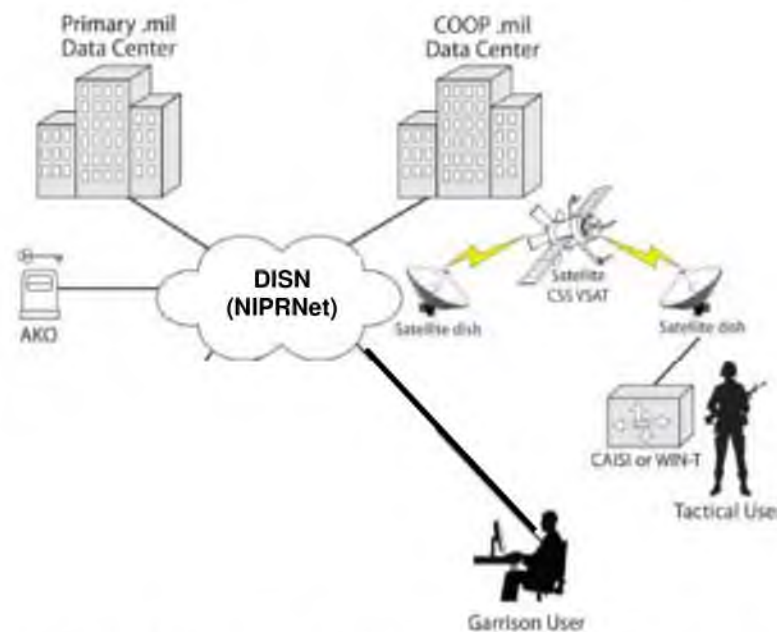


Figure 1-1. High-level Diagram of GCSS-Army System Configuration

The Army Enterprise Systems Integration Program (AESIP) is part of the GCSS-Army program, but it is separate from the GCSS-Army field tactical application used directly by Army logisticians. AESIP is a data brokering hub that operates in the background without user notice. AESIP has three functions. First, it translates different message data formats between GCSS-Army field tactical application and external trading partners such as LMP and GFEBS. Second, it provides a single source of authoritative data, pushing any changes in authoritative data to users who subscribe to those data. Finally, AESIP supports cross-functional business intelligence by providing access to multiple data sources. (See Figure 1-2.)

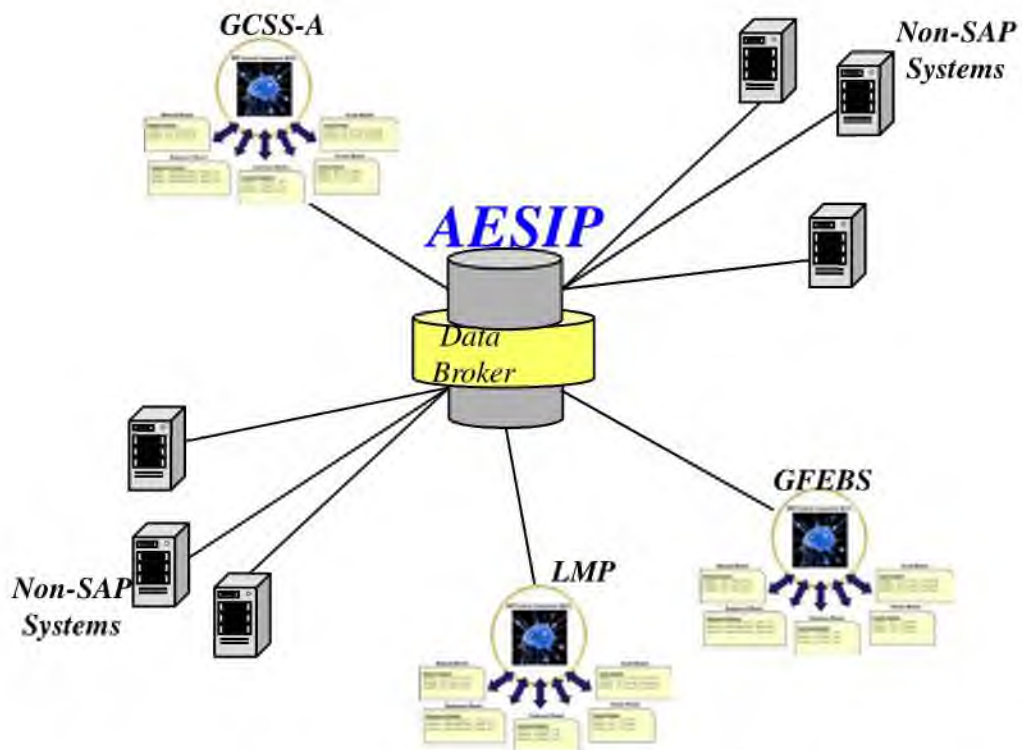


Figure 1-2. AESIP is a Data Brokering Hub between GCSS-Army and External Trading Partners

This page intentionally left blank.

Section Two Test Adequacy

The operational testing of the GCSS-Army Release 1.1 was adequate to support the evaluation of GCSS-Army operational effectiveness, suitability, and survivability for a limited user base. The IOTE did not include Army National Guard or Army Reserve units, and was not stressed to replicate the entire Army usage. Future independent or program-conducted testing and evaluation should be scheduled based on risk assessment by the Operational Test Agency in accordance with the approved Test and Evaluation Master Plan (TEMP). The ATEC conducted the IOT&E in accordance with the DOT&E-approved TEMP and the Army Test and Evaluation Command (ATEC) Test Plan.

Initial Operational Test and Evaluation (IOT&E)

ATEC conducted the GCSS-Army Initial Operational Test from August 29 through October 21, 2011, at Fort Bliss, Texas, with the 2d Brigade Combat Team, 1st Armored Division. The unit was both in garrison at Fort Bliss, Texas, and deployed to White Sands Missile Range (WSMR), New Mexico. Additional GCSS-Army users from the 15th Sustainment Brigade and the 1st Division G-8 at Fort Bliss, Texas, and from the Defense Finance and Accounting Office at Rome, New York, participated in the IOT&E.

The unit exercised property accountability actions, maintenance actions, and supply actions for its assigned equipment using GCSS-Army. Resource managers in Rome, New York, and the unit at Fort Bliss and WSMR exercised financial management to ensure unit spending did not exceed the unit's budget as funds were obligated and disbursed. GCSS-Army accurately reported the funds' status.

ATEC collected and delivered Test Incident Reports (TIR), help desk logs, and user surveys. The PMO collected and delivered audit logs from the server sites and the audit logs generated by SAPTM. The user representatives worked with the PMO and ATEC personnel to reduce the log data and compare with the manual data collection forms.

The use of system-knowledgeable and test-trained auditors is a recommended practice. Many test team members understood both the system and the data collection as they had participated in the GCSS-Army Limited User Test conducted in September 2010. The data collection team was augmented by soldiers with logistics and finance experience to act as subject matter experts. Although most GCSS-Army users submitted task performance forms themselves, there were ten data collectors designated as auditors who randomly shadowed users and submitted task performance forms and test incident reports as needed. In examining the differences between the data collected by shadowing auditors and the data collected by the users they shadowed, it became clear that the users were less accurate than the auditors as the users were often too busy to enter data as events occurred. The data collection tasks given to users (if any) should be very simple. More complex data collection should be done by system-knowledgeable and test-trained auditors.

Threat Test

The Threat System Management Office – Threat Computer Network Operation Team performed a threat assessment from September 19-29, 2011. Threat portrayal included outsider, near-sider, and insider threat, and was executed in accordance with the DOT&E memorandum of January 21, 2009, *Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs*.¹

Continuity of Operations (COOP) Demonstration

The GCSS-Army product manager and the Army Enterprise Systems Integration Program (AESIP) product manager conducted a continuity of operations (COOP) demonstration from November 7-10, 2011, to evaluate the system's ability to restore operations in the event of a declared disaster at the Redstone Arsenal, Alabama, production server hub. The test was adequate to evaluate the COOP requirements for data loss and time to resume operations, and to verify the COOP procedures.

Test Limitations

The system server capacity was not stressed during the IOT&E. During the test, there were 545 GCSS-Army users, compared to the total expected user population of 168,000 when fully operational. The number of test users did not accurately reflect the operational environment for the projected number of operational users. As discussed in Section Four, the computational environment requirements (needed server, storage capacity, and bandwidth) and/or the human factors environment (help desk support, overhead labor and communications costs, and data noise effects) could become untenable as the user base increases.

The IOT&E did not include Army Reserve or National Guard units. Before deploying to these units, the PMO should ensure that the unique requirements from these units are satisfied.

¹ A near-sider is defined as an attacker who is authorized physical access but does not have an authorized user account (such as maintenance staff).

Section Three

Operational Effectiveness

GCSS-Army is operationally effective as indicated by an overall critical mission function success rate of 99 percent, but needs to comply with the requirements of the Federal Financial Management Improvement Act (FFMIA) of 1996. GCSS-Army users can execute logistics tasks both in garrison and when deployed. GCSS-Army provided near real time enhanced situational awareness to all levels of command by integrating the Army's tactical financial system into the property accountability, maintenance, and retail supply systems. Commanders were able to see a unit's equipment readiness, track the status of work order and property book requisitions necessary to improve a unit's readiness status, and verify funds availability at any time using GCSS-Army.

System Performance

GCSS-Army users identified 20 Critical Mission Functions (CMFs) needed to successfully accomplish five Mission Critical Functions (MCF). Table 3-1 lists the MCFs and CMFs and shows details of the GCSS-Army performance during IOT&E. The user requirement was to successfully execute each CMF more than 90 percent of the time (threshold), with 80 percent confidence. Success is defined as a transaction that was processed accurately within the time allowed. The GCSS-Army successfully executed all 20 CMFs for 7,447 of 7,511 attempts (99.15 percent), thereby exceeding the threshold requirement. The failures were attributed to satellite connectivity, errors related to role and permissions, and crew errors. The results in Table 3-1 include operations over satellite communication as well as a local area network, and operations performed by trained and untrained users. Neither the network nor the training levels made statistically significant difference (at 90 percent confidence level).

GCSS-Army will undergo many iterations of software updates. The PMO should invest in an automated tool to conduct regression tests so that future updates can be tested and evaluated efficiently.

**Table 3-1. Critical Mission Functions Performance
FOR OFFICIAL USE ONLY**

MCF	CMF	Point Est	80%LCL (one-sided)	Pass	Success	Attempt
Property Book/Unit Supply	Asset Management	99%	98%	PASS	675	683
	Property Book Inventory Validation	96%	91%	PASS	46	48
	Property Book Reports	99%	97%	PASS	132	134
Retail Supply	Issue Supplies	96%	94%	PASS	126	131
	Process Turn-ins	100%	99%	PASS	195	195
	Request and Receive General Supplies	99%	97%	PASS	162	164
	Store General Supplies	100%	99%	PASS	309	310
Maintenance	Configuration & Maint Management	95%	92%	PASS	110	116
	Maint Supply	100%	99%	PASS	213	214
	Manage Platform Configuration	100%	96%	PASS	36	36
	Manage Scheduled Maint/AOAP	99%	99%	PASS	741	745
	Update Equipment Record	99%	98%	PASS	394	398
	Work Order Management	100%	100%	PASS	1,599	1,603
Logistics Management	Generate Logistics Report	98%	97%	PASS	305	310
	Manage Equipment Operators	99%	99%	PASS	1,474	1,483
	Manage Equipment Utilization	99%	98%	PASS	671	678
Finance	Financial Reporting	97%	95%	PASS	112	115
	Manage Execution Funds Account	100%	94%	PASS	26	26
	Manage Liabilities (Budget Execution)	100%	97%	PASS	51	51
	Post to General Ledger	99%	96%	PASS	70	71
	Total	99%			7,447	7,511

FOR OFFICIAL USE ONLY

Financial Audit Readiness

The 2010 National Defense Authorization Act (NDAA) requires “financial statements of the Department of Defense are validated as ready for audit by not later than September 30, 2017.” One of the conditions to achieve this requirement is for the system to be compliant with the requirements documented in the Federal Financial Management Improvement Act (FFMIA). GCSS-Army is not yet compliant with the FFMIA. The PMO is working with the Assistant Secretary of the Army for Financial Management and Comptroller (ASA FMC) and the Army Audit Agency (AAA) to coordinate the necessary actions. The PMO, with help from the ASA

FMC, mapped the FFMIA requirements to the test cases. The PMO will need to run the test scripts and demonstrate compliance with the FFMIA. The Army Audit Agency (AAA) will observe the test and review the test results. AAA will document the results as an independent party in an official attestation of compliance upon satisfactory demonstration of the FFMIA requirements. As the PMO, ASA FMC, and AAA continue to work toward the FFMIA compliance, the Army Audit Readiness team is working with each of the Army financial system program offices on the overall readiness for audit by 2017.

Once GCSS-Army is ready for audit, the PMO and ATEC should arrange for evaluation of auditability. Audit reviews will/should include multiple levels of review. Any and all reviews should be observed as part of early tests of auditability.

An important part of the FFMIA compliance involves the controls on user roles and the permissions associated with user roles. Automated regression testing should be used to help maintain system auditability by validating roles and permissions across future software releases. An audit is a snapshot of a software system, but software systems usually change quite frequently. When changes are needed in any component software, the PMO should use automated test tools to conduct “positive” and “negative” regression testing of new releases to ensure that roles and permissions are still functional. Positive regression tests should demonstrate that authorized users are able to access everything within their authorization. Negative regression tests should demonstrate that users are unable to access anything outside their authorization levels.

Interoperability

The Joint Interoperability Test Command (JITC) released an updated GCSS-Army Increment 1, Release 1.1 Quick Look Report on February 7, 2012. The report is not final, as the update to the System View (SV)-6 from the certified requirement that documents the System Data Exchanges (SDE) is still in draft.

JITC compared logs from the IOT&E period of August 29 to October 21, 2011, with the SV-6 requirements. The logs showed that each of the demonstrated information exchanges was successful. Some SDEs did not execute during the IOT&E period (3 of the 22 Joint Critical SDEs and 6 of 30 Army Critical SDEs). However, other SDEs between the same systems and using similar protocol suites were successful. The majority of interface problems would either be caused by functionality issues or system or protocol mismatch. While functionality issues cannot be ruled out, the high success of other system functionality and the high success of similar protocol exchanges between the same systems suggests that the SDEs that were not executed during IOT&E will have few to no issues.

This page intentionally left blank.

Section Four Operational Suitability

GCSS-Army is operationally suitable. Table 4-1 summarizes key findings from the IOT&E.

**Table 4-1. Suitability Critical Operational Issues and Criteria (COIC)
FOR OFFICIAL USE ONLY**

COIC	Requirement	Data Source	Findings
Reliability	MTBSA \geq 716 Hours	Equipment Downtime Logs	MTBSA \geq 1296 Hours (length of test - no system aborts per CPD.) (MTBSA = Mean Time Between System Abort.)
Availability	$A_o \geq 95\%$	Equipment Downtime Logs	$A_o = 100\%$ per CPD (excludes scheduled maintenance time.) or 99.4% including the maintenance down times.
Maintainability	MCMT \leq 4 Hours for 90% of events	Equipment Downtime Logs	COIC (downtime events of critical IT components): 30 Minutes Maximum Corrective Maintenance Time.
Manpower & Personnel Requirements Integration (MANPRINT)		User Surveys	User had perception that Automatic Identification Technology (AIT) Hand Held Bar Code Scanner was slow over the satellite. Users entered data manually.
		User Surveys, Help Desk Tickets	When fully fielded, GCSS-Army will have 168,000 users who could generate up to 46,000 help desk tickets per month. The help desk was adequate during the IOT&E but the PM should monitor the adequacy of the help desk as the user population increases.
		User Surveys, Test Incident Reports	Very few system problems were attributed to training shortfall or to crew.
Change Management	85% positive responses is good indicator	User Surveys	Overall good. About 70% favorable responses. Initial issues with roles and permissions.
Integrated Logistics Support		User Surveys	Over 80% favorable responses for job aids
		User Surveys, Help Desk Tickets	Over 80% favorable responses for questions relating to help desk support
Data Cleansing (Not a COIC)		Test Incident Reports	Satisfactory: Nine failure events out of 68 were related to data. All were non-essential function failures, and they were result of data that failed to migrate properly from the legacy databases into GCSS-Army.

FOR OFFICIAL USE ONLY

Operational Availability

The system was available 99.4 percent of the time, compared to the requirement of 95 percent. There were no system aborts in 1,296 hours of testing, indicating with 84 percent confidence that the system can satisfy the mean time between system abort requirements of 716 hours.

Training and Help Desk Support

Training was adequate for the users. During the IOT&E, the operators who received New Equipment Training (NET) successfully performed 99 percent of tasks (6,515 of 6,573). Users who did not receive formal training also successfully performed 99 percent of tasks (932 of 938). The high success rate of both formally trained crew as well as untrained crew indicates that support structure is very sound, so that even an untrained user will have high probability of success. Part of the infrastructure success came from the help desk; 81 percent of the 165 respondents gave favorable ratings for the help desk.

Of the NET trained users, 79 percent of 170 respondents felt NET prepared them to execute GCSS-Army transactions effectively and 92 percent of 168 respondents agreed that they were adequately trained to know where to look, or whom to contact, if they had trouble.

The testers turned in 68 test incident reports during the IOT&E; two incidents were charged to training shortfalls and 27 events were charged to crew errors, indicating that 43 percent of test incidents were chargeable to either crew or training. An incident was charged to training if the operator was not trained in the particular task, whereas the incident was charged to crew if the user was trained in the task. None of the 29 crew or training incidents resulted in a system abort. Even though 99 percent success indicates both trained and untrained users can successfully employ GCSS-Army to execute their missions, the high percentage of training and crew error indicates that the PMO should consider further improvement in GCSS-Army training as a candidate for further improvement.

Usability

Informal interviews with the operators indicated perception that hand-held scanners are slow when used over the satellite link. As a result, warehouse personnel chose to manually type in incoming shipments rather than using the hand-held scanner. This process was not considered to be a major limitation to the warehouse users.

Even though some users expressed perception of slow services over satellite links, GCSS-Army transactions over the satellite link were successful 5,395 times out of 5,437 (99 percent success). This result is comparable to the 2,052 successful transactions out of 2,074 attempts (99 percent success) when connected over the local area network. Since the success criteria include timeliness requirements, the performance indicates that satellite delays might be frustrating to the users, but are not going to cause mission failures. The PMO is working on improving the satellite responsiveness, but that problem should not significantly reduce the value of GCSS-Army to the users.

Scalability

The number of users during the IOT&E was a small subset of expected users at full deployment. As with other Army ERP solutions, both the computing capacity and the administrative support will need to expand with the growth of the user population. These expansions may give rise to scalability issues in computing and/or in human factors to support and manage the user population at full deployment. Computing factors include the need for

enough servers, storage, and communications bandwidth. Human factors include the need for sufficient help desk support, scalable processes and procedures, and adequate data management (that is not overwhelmed by natural variability and errors in the data provided by a full user population).

A study sponsored by the PMO uncovered the possibility of future scalability problems. The study found that the depth of finance configuration and its alignment with organization structure is too complex. The study also found that the algorithm locks together the organization structure, cost center, fund center, and work breakdown structure and unnecessarily restricts business processes. These two key shortfalls could cause significant scaling problems for supporting the objective 168,000 users. The PMO and the prime contractor formed a team to find solutions for this issue, and proposed to truncate the organization structure to company level and to “un-lock” the design so that organization structure, cost center, fund center, and work breakdown structure can be configured independently. These fixes might be sufficient to address the scalability problems, but the test community will need to test the solutions before fully implementing them. The test should include regression tests of previously demonstrated functionality to ensure that these changes do not cause shortfalls in those functions.

The PMO also needs to “develop models” (which can simply mean creating relevant spreadsheets) to understand how the human factors will scale. A model of help desk support should be able to predict how the number of incoming help desk tickets rises over time following a roll-out of GCSS-Army software to a new unit. A business process model will reveal communications nodes in the system, like the help desk, that have communications demands that increase with the number of users. All such processes pose a scalability risk. Finally, several lightweight (spreadsheet) models of data noise effects are recommended in order to track data management scalability. Through simple empirical data collected in the early deployment phase, we can be sure full deployment will be possible and/or modulate the rate of deployment to account for observed transient effects.

The PMO needs to monitor the adequacy of the help desk support as the user population increases. It may be most useful to divide the help desk tickets into categories. For example, the Institute for Defense Analyses modeled the tickets related to roles and permissions and found linear growth with the number of users. Over the two-month period during the IOT&E with 545 users, 299 help desk tickets were generated regarding roles and permissions. If this number is taken to be an indicator of the number of help desk tickets, it equates to 0.274 tickets per user per month. Extrapolating this number to the expected 168,000 users, this would mean 46,000 help desk tickets per month. This simple indicator is alarming, and also, hopefully, not accurate. A more rigorous analysis of the demand model should also track the rate at which tickets decline over the months following software deployment. The appropriate projected total help desk tickets per month should be calculated from the steady state number of tickets, and the software deployment rate should be such that the help desk capacity is at all times sufficient for the accumulated steady state load plus the transient increase in tickets from each deployment. Naturally, these very simple models can and should be improved by observations during the course of software deployments.

The PMO should have a business process model of human communications flows within GCCS-Army. Any node (such as the help desk) that can receive communications from all users is a potential point of failure. The PMO should identify other such nodes. The PMO also needs to model the support labor costs of new users. For example, each new user added to the user population carries a turnover cost, usually determined by the probability that the user will leave (quit, retire, etc.) and the number of hours of labor needed to train a new user, establish new accounts, remove the old accounts, etc. Those costs can be modeled early from low-cost, straightforward observations and can provide additional insight into system scalability. Finally, the PMO should model the data noise effects as new users are added. For example, a database used by a large user population will presumably have duplicate data entries. The GCCS-Army software will protect against duplicates and decrease the rate at which duplicate data entries are added to the database, but that is really the only protection. The PMO should use current rates of duplicate data and data cleansing costs to project costs at full deployment. If this projection of steady state costs of cleansing duplicates at full deployment number is high, that indicates a scalability problem. As another example, a data field may sometimes have the wrong kind of data in it (a phone number instead of a street address, for example). The software is the only protection, but it cannot catch everything. Again, the full deployment costs of the required data cleansing can be calculated from currently observable data. There is also data noise whenever users can make choices – how to categorize, what directory to file in, what file name to use, etc. If each user's choices ultimately impacts the user interface of an unlimited number of other users (for example in a pull-down menu with all the categories entered by all the users since the system first booted up), then that is a scalability problem that the PMO can fix before it becomes a usability problem.

Section Five Survivability

GCSS-Army is survivable against cyber threats. The penetration test conducted by the U.S. Army Threat System Management Office (TSMO) revealed significant shortfalls for protecting against cyber threats, especially on the Army Enterprise Systems Integration Program (AESIP). However, the PMO made fixes since the IOT&E, and the significant issues are now resolved.

Survivability against financial threats remains an open issue. The PMO should start preparing for financial red team tests immediately for near-term evaluation the system's ability to prevent and detect fraud or theft (because the deployed system is already subject to the equivalent of such tests from unfriendly forces). In addition to reviews of system accounting and financial security controls, an operational test of financial security will include financial red teams conducting ongoing tests of system vulnerability to theft and fraud.

Penetration Test

The TSMO Threat Computer Network Operation Team performed a threat assessment supporting the GCSS-Army and AESIP Initial Operational Test from September 19-29, 2011, and discovered seven major vulnerabilities to a cyber attack. Threat portrayal for both systems was representative of an outsider, near-sider, and insider threat. A near-sider is defined as an attacker who is authorized physical access but does not have an authorized user account (such as maintenance staff). The TSMO final report includes major findings against both the GCSS-Army System and the AESIP program.

Table 5-1 summarizes the Information Assurance (IA) evaluation. The greatest risk to the system came from computer network attacks against AESIP. Using only basic AKO access permissions, the threat team was able to acquire programmatic budget data, system architecture data, network diagrams, and security information such as usernames and passwords. The information was primarily on the AESIP program itself, but also contained information about GCSS-Army and other SAP™ systems. The threat team downloaded nearly 400 megabytes of data from the AKO repository with no indication of detection. Within a day of the initial out-brief on September 29, 2011, corrective action had been taken, and the main repository on AKO was no longer available or had been removed.

**Table 5-1. Survivability measures
FOR OFFICIAL USE ONLY**

Measure	Requirement	Data Source	Findings
Protect		Threat Test	Shortfalls were identified and corrected per the Plan of Action and Milestones (POA&M)
Detect		Threat Test	Shortfalls were identified and corrected per the POA&M
React	Notify RCERT within 5 min of high alert; Coordinate attack response within 30 min	Threat Test	Satisfactory: Detections resulted in help desk ticket and corrective actions to enhance protection such as better control of portals. The final report does not indicate that a "high alert" occurred.
Restore	Operational within 24 hrs of declaration of emergency; < 4 hrs data loss (T), < 2 hrs data loss (O)	COOP Test	Satisfactory: AESIP operational in ~7 hrs 20 min. GCSS-Army operational in ~3 hrs 15 min. Lost up to 50 minutes of data. PM plans to conduct DIACAP and COOP Stand-up quarterly.

FOR OFFICIAL USE ONLY

The PMO fixed most serious problems as of March 16, 2012, and the remaining on-going fixes relate to the shortfalls from the SAPTM. The PMO is continuing to pursue fixes to these as well as implementing defenses against new threats via internal quarterly DoD Information Assurance Certification and Accreditation Process (DIACAP) updates. .

Continuity of Operation (COOP) Demonstration.

The GCSS-Army PMO conducted a COOP demonstration from November 7-10, 2011, verifying the system's ability to execute its disaster recovery plan. The PMO shut down the data transfer that synchronizes the production site at Redstone Arsenal, Alabama, and the COOP site in Radford, Virginia, in order simulate the loss of the primary site. Once the data synchronization was stopped, the PMO executed a modified disaster recovery plan whereby the primary production servers at Redstone Arsenal continued to support normal activity.

GCSS-Army restored operational capability 3 hours and 15 minutes, and AESIP restored operational capability 7 hours and 20 minutes, after declaration of emergency. The system logs validated that no more than 50 minutes of data would have been lost. The threshold requirement for COOP and disaster recovery is to restore operations within 24 hours with no more than 4 hours of data loss, and the objective is to restore operations within 24 hours with no more than 2 hours of data loss. The COOP demonstration satisfied the objective requirement.

Once both GCSS-Army and AESIP were deemed online at the COOP site, functional tests were completed to verify that GCSS-Army was operational. A test team composed of National Guard and Army Reserve soldiers executed 10 test cases that executed a wide variety of the GCSS-Army functions, including transactions that required information exchanges via AESIP. Nine of 10 test cases passed. The one failed case was attributed to a problem with the production software and not a problem caused by the COOP standup.

The PMO incorporated lessons learned from the COOP demonstration into the disaster recovery plan, which has grown to be a 563-page document with detailed screen shots for AESIP

and a 15-page check list for GCSS-Army. The GCSS-Army PMO plans to conduct a COOP standup demonstration quarterly to keep the data recovery plan up to date and COOP site personnel proficient in its procedures.

This page intentionally left blank.

Section Six Recommendations

The PMO should consider the following recommendations in order to ensure operational effectiveness, operational suitability, and survivability throughout deployment:

- Collect data for computational (server capacity, storage, bandwidth) and human (help desk responsiveness, overhead labor and communication costs, and data noise) impacts of increases in the size of the user base. Use such data to establish a pattern of demand on the system, so that future demand can be adequately anticipated and resourced as more users come online.
- Test and evaluate future improvements, including deployments to the Army Reserve and National Guard units, in accordance with the September 2010 DOT&E guidelines for Operational Test.
- Develop and implement automated regression testing to continue monitoring software effectiveness for future updates.
- Continue the cooperation with the Army Audit Agency (AAA) to achieve financial auditability as mandated by the 2010 National Defense Authorization Act (NDAA).
- Work with ATEC to establish a financial red team to conduct tests of the system's ability to prevent and detect theft and fraud.
- Continue with the current plan of updating the DoD Information Assurance Certification and Accreditation Process (DIACAP), including conduct of Continuity of Operations (COOP) demonstrations.



OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JUN 12 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035


Dear Mr. Chairman:

I have enclosed my Initial Operational Test and Evaluation (IOT&E) report on the Global Combat Support System – Army (GCSS-Army), Release 1.1. In the report I conclude the following:

- The IOT&E was adequate to evaluate the operational effectiveness, suitability, and survivability of the system.
- GCSS-Army, Release 1.1 is operationally effective, operationally suitable, and survivable.

My report includes recommendations for the Program Management Office to address system scalability, validate the system functionality for Reserve and National Guard units, achieve the readiness for financial audit, implement automated regression testing, establish a financial red team to test against theft and fraud, and to continue with the planned updates for Information Assurance.

Section 2399, Title 10, United States Code provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have also provided copies to the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Secretary of the Army; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable Adam Smith
Ranking Member





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JUN 12 2012

The Honorable C. W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

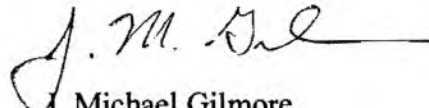
Dear Mr. Chairman:

I have enclosed my Initial Operational Test and Evaluation (IOT&E) report on the Global Combat Support System – Army (GCSS-Army), Release 1.1. In the report I conclude the following:

- The IOT&E was adequate to evaluate the operational effectiveness, suitability, and survivability of the system.
- GCSS-Army, Release 1.1 is operationally effective, operationally suitable, and survivable.

My report includes recommendations for the Program Management Office to address system scalability, validate the system functionality for Reserve and National Guard units, achieve the readiness for financial audit, implement automated regression testing, establish a financial red team to test against theft and fraud, and to continue with the planned updates for Information Assurance.

Section 2399, Title 10, United States Code provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have also provided copies to the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Secretary of the Army; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable Norman D. Dicks
Ranking Member





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JUN 12 2012

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

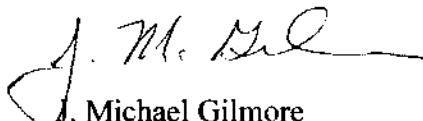
Dear Mr. Chairman:

I have enclosed my Initial Operational Test and Evaluation (IOT&E) report on the Global Combat Support System – Army (GCSS-Army), Release 1.1. In the report I conclude the following:

- The IOT&E was adequate to evaluate the operational effectiveness, suitability, and survivability of the system.
- GCSS-Army, Release 1.1 is operationally effective, operationally suitable, and survivable.

My report includes recommendations for the Program Management Office to address system scalability, validate the system functionality for Reserve and National Guard units, achieve the readiness for financial audit, implement automated regression testing, establish a financial red team to test against theft and fraud, and to continue with the planned updates for Information Assurance.

Section 2399, Title 10, United States Code provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have also provided copies to the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Secretary of the Army; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable John McCain
Ranking Member





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JUN 12 2012

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6025

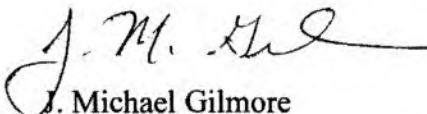
Dear Mr. Chairman:

I have enclosed my Initial Operational Test and Evaluation (IOT&E) report on the Global Combat Support System – Army (GCSS-Army), Release 1.1. In the report I conclude the following:

- The IOT&E was adequate to evaluate the operational effectiveness, suitability, and survivability of the system.
- GCSS-Army, Release 1.1 is operationally effective, operationally suitable, and survivable.

My report includes recommendations for the Program Management Office to address system scalability, validate the system functionality for Reserve and National Guard units, achieve the readiness for financial audit, implement automated regression testing, establish a financial red team to test against theft and fraud, and to continue with the planned updates for Information Assurance.

Section 2399, Title 10, United States Code provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have also provided copies to the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Secretary of the Army; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable Thad Cochran
Ranking Member



Combined Follow-on Operational Test and Evaluation (FOT&E) Report on the MH-60R Multi-Mission Helicopter and the MH-60S Multi-Mission Combat Support Helicopter Preplanned Product Improvement (P3I) Program

This report assesses the operational effectiveness and operational suitability of selected systems of the MH-60R Multi-Mission Helicopter and MH-60S Multi-Mission Combat Support Helicopter Preplanned Product Improvement (P3I) Program. These systems are designed to improve flight safety, enhance and facilitate maintainability, improve airframe longevity, and reduce aircrew fatigue. The Navy conducted Follow-on Operational Test and Evaluation (FOT&E) on all three systems from February 23 to September 30, 2011. The tested systems were the:

- Active Vibration Control System (AVCS)
- Ground Proximity Warning System (GPWS)
- Integrated Mechanical Diagnostic System (IMDS).

The AVCS is designed to reduce aircraft vibration and facilitate aircraft maintenance. The system consistently reduced vibration throughout the entire flight regime as well as or better than the legacy system. In addition, it reduced maintenance man-hours and the number of necessary maintenance check flights. The GPWS is designed to alert the pilots to an impending crash situation. The system met all requirements for providing accurate and timely warnings to the pilots in order to avert a potentially catastrophic situation. The IMDS is an embedded system designed to provide data on component health, performance, and impending failure alerts. The system met all threshold requirements and facilitated maintenance by providing improved maintenance diagnostics, reducing maintenance man-hours, reducing the number of necessary maintenance check flights, streamlining maintenance management record keeping, and improving component lifecycle tracking. All three P3I systems are assessed to be operationally effective and suitable for all missions. The test results did not affect any prior findings on the overall operational effectiveness or operational suitability for either airframe in any mission area.

The Navy did not conduct any dedicated live fire test and evaluation events in support of this phase of MH-60 P3I testing. The Navy's engineering analysis indicated that the incorporation of P3I systems in MH-60 aircraft did not alter the survivability of either aircraft from that reported in prior operational testing (OT); DOT&E concurs with that assessment.

Although all three systems are installed on fleet aircraft, only AVCS and IMDS are operational; the Navy has withheld the authorization for fleet use of GPWS until FOT&E is completed. These three P3I systems do not provide any additional operational capability or mission essential functionality to the aircraft; however, the GPWS and the IMDS both provide information to the aircrew to aid in real-time decision-making.

System Description

The MH-60R Multi-Mission Helicopter and MH-60S Multi-Mission Combat Support Helicopter are ship-based, medium lift, tactical rotary-wing aircraft. Built by Sikorsky Aircraft

The marginal cost of producing this report is estimated to be approximately \$18.6K. The estimated acquisition cost of the MH-60R program is \$14.3B and the estimated acquisition cost of the MH-60S program is \$7.9B.

Corporation of Stratford, Connecticut, both aircraft are designed and built for all-weather, day and night operations, from large and small deck combatant and auxiliary ships. The P3I Program fields systems, sensors, and advanced subcomponents designed to improve both MH-60R and MH-60S readiness, flight performance, and operational capabilities.

Background

The MH-60R and MH-60S are both derivatives of the Army UH-60L Blackhawk. The MH-60R is the Navy's primary helicopter for Undersea Warfare and Surface Warfare. The MH-60S is the Navy's primary helicopter for airborne logistics, Combat Search and Rescue, and Carrier Plane Guard/Search and Rescue. The MH-60S reached its initial operating capability in 2002 and the MH-60R in 2006.

The P3I Program is an overarching administrative construct used by the Navy to manage 16 disparate acquisition programs that are designed to improve MH-60 performance and/or capabilities. These programs either field new technology or provide upgrades or improvements to current aircraft systems. Most of the P3I systems function independently, and are often fielded as such. The Navy conducts OT of these systems as they reach developmental maturity; ten MH-60 P3I systems completed OT prior to this FOT&E.

By design, the MH-60R and MH-60S have an extremely high degree of commonality. The primary differences between the two aircraft are structural, and relate to the internal design of the airframe. These differences have little to no effect on operational performance. The aircraft share a common cockpit and the same logical and physical data architecture. For this reason, a single common P3I system can be installed on either the MH-60R or the MH-60S without customized modification. All three of these tested P3I systems now come installed on all new production MH-60R/S aircraft. The Navy is in the process of retrofitting these systems on aircraft already in the fleet.

System Under Test

Active Vibration Control System (AVCS)

The AVCS is designed to replace the current passive vibration absorbers on the MH-60R and MH-60S aircraft. The Navy intended the system to actively reduce airframe vibration caused by the main rotor system, thereby reducing vibration-induced fatigue and increasing component life.

The system consists of a computer, 10 feedback accelerometer sensors, and a Vibration Control Actuation System (VCAS). The VCAS comprises an electronics unit and five force generators and imparts forces on the airframe to counteract the vibrations produced by the rotor system. The system is completely autonomous and requires no input from the pilots; the only cockpit control is an "ON/OFF" switch.

In contrast, the current passive system does not dynamically respond to changes in vibratory load. The passive absorbers used by the legacy system are tuned to a fixed vibration frequency. During aggressive aircraft maneuvering situations where main rotor loading and

resultant main rotor vibrations change quickly, the aircraft will be subjected to increased, potentially damaging and rapidly varying vibratory loads. Additionally, a battle-damaged aircraft could generate a unique vibratory load that the passive system cannot properly dampen. The passive system could exacerbate the effects of the battle damage-induced vibratory load because it is tuned to a fixed vibratory frequency.

In addition to being able to respond to fluctuating vibration frequencies, the actuators in the active system work together to achieve a more uniform vibration reduction over the entire airframe. This is in contrast to the passive absorbers, which act independently and in a single vibratory plane.

The AVCS eliminates the maintenance requirement of the legacy system to periodically tune the system to the appropriate vibration frequency, resulting in the elimination of maintenance man-hours and the test flight hours currently required for vibration analysis and reduction. The lower vibration levels also reduce crew fatigue, making a positive contribution to safety of flight.

Ground Proximity Warning System (GPWS)

Controlled Flight into Terrain (CFIT) is the unintentional flight into the ground of a properly functioning aircraft, usually caused by a distracted or preoccupied pilot. For the military pilot, this situation is most often encountered when the pilot at the controls is distracted by the immediate operational scenario, employment of weapons or sensors, or is dealing with an in-flight aircraft emergency. The GPWS is a software algorithm designed to provide timely and appropriate warnings to the pilot so that effective action can be taken to avoid crashing over land or over water. GPWS software uses existing aircraft flight systems and requires no additional hardware. The system is designed to provide protection against flight into terrain or water surface, dynamic rollover, altitude loss after takeoff, and hard landings (landings with an excessive and potentially hazardous rate of descent). The algorithm discerns between the pilot's intent to land and CFIT.

GPWS performs dynamic calculations to continuously assess the potential for CFIT. When the algorithm identifies an impending CFIT condition, it generates an aural warning to the pilots over the aircraft's Internal Communication System. This warning specifies the best initial recovery action that the pilot can take to execute a safe recovery. These aural cues consist of one of four voice warnings: "Power," "Pull-Up," "Roll Left," or "Roll Right." All warnings are repeated at 2-second intervals until a recovery has been safely executed at an altitude that provides 20 feet above ground level clearance.

The GPWS software is embedded in the aircraft's computer operating systems. It receives data from a number of sensors, primarily the AN/APN-194 radar altimeter. The algorithm constantly checks the validity of the sensor inputs to ensure the system is processing accurate data. Even if the aircrews decide to disable the audio cues for tactical or other reasons, the GPWS software will continue to function.

Integrated Mechanical Diagnostic System (IMDS)

The IMDS is an embedded aircraft system designed to improve fleet readiness and safety through the early identification of degraded components. It also facilitates maintenance by streamlining maintenance practices and reducing the number of post-maintenance test flights required. The system provides monitoring and diagnostic capabilities for rotor track and balance, engine health, gearbox and drive train health, and fatigue life tracking. IMDS includes both the On-Board System and the Ground Station. The On-Board System includes a network of 35 permanently installed sensors located throughout the aircraft drive train. The system is designed to collect, analyze, and record numerous measures on propulsion, drive train, and rotor system components; these data are then downloaded to the Ground Station for further analysis. The aircraft system includes a Flight Data Recorder that records various aircraft state parameters and selected vibration data that can be used to assist in aircraft mishap investigations.

The Navy designed the system to sense and record conditions that jeopardize flight safety, notify the aircrew of a serious degradation or imminent failure of the monitored components, and provide diagnostic information to the aircrew for real-time decision-making in these situations. The IMDS integrates with the Naval Aviation Logistics Command Management Information System (NALCOMIS) Optimized for Organizational Maintenance Activities (OOMA) to provide a complete equipment management solution. NALCOMIS OOMA is the basis for maintenance management and record keeping, aircraft configuration and parts-life tracking, flight record keeping, and aircraft maintenance quality assurance. IMDS reduces operation and support costs by rapidly and seamlessly transferring comprehensive aircraft performance data directly into the electronic records of the NALCOMIS OOMA, eliminating the need for manual data entry.

The Navy also designed IMDS to provide a significantly improved method for adjusting rotor blade track and balance. A track and balance is required any time a component is changed or adjusted on the rotor head. The helicopter main rotor produces vibration in both the vertical and lateral planes. To reduce these rotor-induced vibrations, helicopter rotors must be both statically and aerodynamically balanced. An out of balance rotor system generates excessive vibration that adversely affects rotor blade structural integrity, airframe and component life, and aircrew fatigue. Aerodynamic balancing corrects imbalances in the entire rotating system.

Aircraft maintenance personnel accomplish the rotor track and balance process by increasing or decreasing the amount of lift generated by each blade so that they all perform equally, each generating the same amount of lift. This is done by adjusting the individual blade pitch (adjusting a pitch link), bending trim tabs on the blades, adding or removing specifically designed balancing weights to each blade, or most likely, a combination of all three; this is an iterative and time-consuming process that typically requires multiple adjustments. An adjustment to one blade will often adversely affect the performance of another. Furthermore, the blades must maintain track and balance throughout the entire flight envelope. It is not uncommon for a rotor system to be well balanced in a hover or at a particular airspeed, and then be out of balance at another airspeed.

The legacy system for rotor track and balance is the Automatic Track and Balance Set (ATABS). Aircraft maintenance personnel use this system to gather data for the legacy vibration analysis process. Conducting a track and balance with the legacy system required the installation of both tracking tabs on the rotor blades and an ATABS computer in the aircraft. The track was measured using a handheld optical tracking device (camera) to sight the rotating tracking tabs. Blade track readings are taken on the ground with no pitch (zero aerodynamic load), in a hover, at 120 and 140 knots indicated airspeed (KIAS), and at V_{\max} (i.e., the maximum airspeed the airframe is capable of achieving within its operating limits). The system indicates the margin by which individual blades are out of track at each of these intervals. This legacy system did not provide any suggested corrective actions. In contrast, IMDS is permanently embedded in the aircraft, takes no installation time, automatically takes track and balance readings, and is designed to provide suggested corrective adjustments that will provide a properly balanced rotor system throughout the entire flight envelope.

Test Adequacy

The Air Test and Evaluation Squadron ONE (VX-1), based at Naval Air Station (NAS) Patuxent River, Maryland, conducted all OT. The evaluation incorporated selected data from developmental testing (DT) conducted by Air Test and Evaluation Squadron TWO ONE (HX-21), also based at NAS Patuxent River, Maryland. The FOT&E was adequate and executed in accordance with DOT&E-approved test plans on January 31, 2011.

The Navy conducted testing from February 23, 2011 to September 30, 2011 at NAS, Patuxent River, Maryland, where the VX-1 squadron operated four MH-60R helicopters and two MH-60S helicopters. VX-1 flew 433.0 flight hours in support of the test, which was conducted in accordance with DOT&E-approved test plans. The FOT&E was adequate to assess the operational effectiveness and operational suitability of the P3I systems.

Operational Effectiveness

All three P3I systems are operationally effective for all missions. There were no significant operational effectiveness deficiencies identified during testing. This result does not affect any prior findings on the overall operational effectiveness for either airframe in the conduct of any mission area.

Active Vibration Control System (AVCS)

The AVCS is operationally effective on the MH-60R and MH-60S aircraft. The Navy tested the AVCS on MH-60S for 198.1 hours total flight time during this FOT&E, and tested the system on MH-60R for 8.7 hours total flight time during the previous FOT&E. The system was responsive and adaptive to changes in vibratory load throughout all flight regimes and changes to aircraft gross weight airspeed, rotor speed, and other dynamic flight conditions, as well as mission configurations. Pilots were able to activate and deactivate the system at will to qualitatively assess the differences in aircraft vibration over a range of flight conditions with and without the benefit of AVCS. Qualitative assessments by all OT pilots consistently assessed the system as equal or superior to the legacy system in reducing cockpit vibration.

During P3I OT, the test aircraft were not instrumented; hence, there was no way to quantitatively measure changes in aircraft vibration levels throughout the flight regime or in various mission configurations. However, during contractor testing (CT), Sikorsky Aircraft Corporation instrumented both the MH-60R and the MH-60S test aircraft. The contractor's test data indicated that the AVCS demonstrated improved performance over the legacy passive system. AVCS consistently achieved lower vibration levels than the passive absorber suite and was less sensitive to changes in rotor speed. The Navy purchased, installed, and operated the AVCS based on these results. Although not ideal, this approach was considered adequate to evaluate the AVCS.

A major advantage of the AVCS is that it eliminates the need to conduct the vibration analysis and vibration absorber tuning that the legacy system required. Since AVCS automatically and dynamically responds to aircraft vibrations, no tuning is required. Prior to AVCS, aircraft maintenance personnel conducted vibration analysis flights at periodic maintenance intervals and required for many drive train component changes, and tail and main rotor adjustments. Installation of the ATABS equipment was required to record pre-adjustment vibration readings gathered from the aircraft operating in-flight, and to record post-adjustment vibration readings gathered during a second flight, to confirm the effectiveness of the applied tuning adjustments. Since there is no passive system to tune, there is no longer a requirement for flights to identify and confirm tuning adjustments. In addition, the installation and removal of the ATABS equipment, which alone accounts for 2.3 maintenance man-hours, is no longer required.

Ground Proximity Warning System (GPWS)

The GPWS is operationally effective on the MH-60R and MH-60S aircraft. The Navy flew 392.4 flight hours in support of this test. Test results for the operational effectiveness for GPWS are summarized below in Table 1.

Table 1. GPWS Operational Effectiveness Test Results

Requirement	Threshold	Objective	Test Result	80% Confidence Interval
Probability of a Successful Warning (P_{SW})	$\geq 40\%$	$\geq 60\%$	84.6% (77/91)	78.6 - 89.4%
Probability of a Nuisance Warning (P_{NW})	$< 5\%$	$< 2\%$	0.6% (3/503)	0.02 - 1.3%

A successful warning is defined as a GPWS warning generated in time for the pilot to execute a safe recovery. A nuisance warning is a false warning provided to the pilot that a CFIT condition exists when it does not. The DOT&E-approved test plan authorized Commander, Operational Test and Evaluation Force to use data collected during DT, only to calculate Probability of Successful Warnings (P_{SW}). This nuance of the test plan was approved because only HX-21 test pilots are authorized to execute the complex aircraft maneuvers necessary to conduct CFIT testing and collect P_{SW} data.

The GPWS should have generated a CFIT warning for 91 DT events. Out of the 91 events, a warning was generated 77 times. The P_{SW} rate was 84.6 percent; this exceeded the objective requirement of at least 60 percent. The 80 percent confidence interval for the probability of receiving a successful warning when a potential CFIT condition exists is 78.6 to 89.4 percent.

During OT, aircraft pilots enacted an aggressive maneuver in 503 events during which there was the potential for a nuisance warning to occur. Of these events, the pilots performed 399 Combat Search and Rescue maneuvers at high speed, in close proximity to the ground at steep angles of bank with extreme nose attitudes. Overall, only 3 warnings were classified as nuisance warnings during the 503 events; this yields a demonstrated Pnw of 0.6 percent, which is significantly less than the objective requirement of 2 percent. Based on this sample proportion of 0.6 percent, the 80 percent confidence interval for the probability of the GPWS generating a nuisance warning when no CFIT condition exists is 0.02 to 1.3 percent. Given this performance, the GPWS is assessed to make a positive contribution to averting crashes due to CFIT while minimizing unnecessary warnings to the pilots.

Integrated Mechanical Diagnostics System (IMDS)

The IMDS is operationally effective on the MH-60R and MH-60S aircraft. The Navy flew 230.0 flight hours in support of this test. The test plan authorized OPTEVFOR to use DT and OT data to assess IMDS Rotor Track and Balance Correction/Adjustment. Testers observed fleet maintenance personnel induce 25 correction opportunities to assess IMDS Rotor Track and Balance Correction/Adjustment. The system enabled maintainers to achieve a proper track and balance with one set of adjustments in 16 of 25 attempts for a success rate of 64 percent; this did not meet the objective criterion of 70 percent. However, the system was successful in enabling maintainers to achieve a proper track and balance with two sets of adjustments in 25 of 25 attempts for a success rate of 100 percent; this exceeded the threshold criterion of 95 percent. The 80 percent lower confidence bound for probability of achieving a proper track and balance within two sets of corrections is 91.2 percent. Although this is a small sample size, qualitative feedback from fleet users is universally positive. MH-60 fleet squadrons report success rates equal to or greater than those observed in the test. Test results for the operational effectiveness for IMDS are summarized below in Table 2.

Table 2. IMDS Operational Effectiveness Test Results

Requirement	Test Result	80% Confidence Interval
Threshold: Perform rotor track and balance with no more than two sets of adjustments 95% of the time.	100% (25/25)	91.2% - undefined*
Objective: Perform rotor track and balance with no more than one set of adjustments 70% of the time.	64% (16/25)	49.2 - 77%
*With zero failed attempts at achieving the threshold, the upper bound of the confidence interval cannot be calculated and therefore is undefined.		

Additionally, use of IMDS also eliminates the 2.3 maintenance man-hours necessary to install and uninstall the portable ATABS equipment required for each track and balance evolution. The legacy system usually required multiple attempts to achieve a proper track and balance. Additionally, the legacy system required the rotor system to be engaged and disengaged multiple times to take readings and make adjustments on the ground or flight deck. Following this, the process begins again in a hover. The time required is not a concern for shore-based operations; however, on an aircraft carrier, this is a major problem. The amount of flight deck space required to conduct a track and balance is significant. Usually, aircraft maintainers cannot conduct a track and balance during fixed-wing (jet aircraft) flight operations because the operating helicopter is simply in the way. As a result, the opportunities to perform an end-to-end track and balance are extremely limited. The inability to conduct a track and balance due to flight deck considerations has a corresponding negative impact on aircraft availability. With IMDS, once the track is found to be within basic limits in a hover, the aircraft can transition to forward flight, take all the necessary readings, and, based on the results demonstrated here, complete the track and balance within two evolutions. Furthermore, DOT&E believes this system will make a significant positive contribution to fleet readiness.

The Ground Station Interface is the means to transfer recorded IMDS data from the On-Board System to the Ground Station. This enables the electronic input of the data directly into NALCOMIS OOMA. The transfer medium is a Personal Computer Memory Card International Association (PCMCIA) memory card. The PCMCIA card is installed during the flight to record data, and then the card is removed from the aircraft and inserted in the Ground Station to transfer the data post-flight.

The term used to describe a successful download and transfer of the data from the On-Board System to the Ground Station is an “acquisition.” Percentage Successful Acquisitions (P_{SA}) is a measure of IMDS Ground Station Interface effectiveness. This is determined by dividing the total number of IMDS “acquisition” attempts conducted by the total number of “successful acquisitions” achieved, and is expressed as a percentage. During this test, VX-1 testers observed fleet maintenance personnel use IMDS to facilitate the conduct of 66 total “acquisition” attempts that resulted in 61 total “successful acquisitions” achieved. Test results for the operational effectiveness of the Ground Station Interface are summarized below in Table 3.

Table 3. Ground Station Interface Operational Effectiveness Test Results

Requirement	Test Result	80% Confidence Interval
Threshold: $P_{SA} \geq 90\%$ Objective: $P_{SA} \geq 95\%$	92.4% (61/66)	86.4 - 96.2%

Operational Suitability

All three P3I systems are operationally suitable for all missions. There were no significant operational suitability deficiencies identified during testing. This result does not

affect any prior findings on the overall operational suitability for either airframe in the conduct of any mission area.

The MH-60R and MH-60S each have different suitability requirements due to the different missions they are required to perform. Individual P3I systems installed in these aircraft do not have specified suitability requirements; however, since these P3I systems are embedded in each aircraft, their suitability must support the required suitability of those aircraft.

During testing, the Mean Time Between Operational Mission Failure (MTBOMF) was measured for the MH-60R and MH-60S. The threshold MTBOMF for MH-60R is 14.8 hours and for MH-60S is 20.3 hours. While there were no system hardware failures or software faults associated with any of the three tested P3I systems in either aircraft, it is important to note that the complete failure of any of these systems would not result in an operational mission failure for either aircraft. Test results for P3I Systems MTBOMF are summarized below in Table 4.

Table 4. P3I Systems MTBOMF Test Results

P3I System	Operating Time (Hours)	Mission Failures	MTBOMF (Hours) (at 80 Percent Confidence*)
AVCS	198.1	0	123.09
GPWS	392.4	0	243.8
IMDS	230.0	0	142.9
*All lower confidence bounds exceed the reliability requirements for both host aircraft.			

Training, human factors, safety, and documentation for each P3I system is assessed to be satisfactory in their support of the overall suitability the aircraft.



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

APR 08 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

I have enclosed my Combined Follow-on Operational Test and Evaluation (FOT&E) Report on the MH-60R Multi-Mission Helicopter and MH-60S Multi-Mission Combat Support Helicopter, required by Sections 2399 and 2366, Title 10, United States Code.

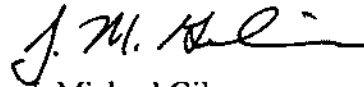
The report assesses Preplanned Product Improvements (P3I) implemented on the MH-60R and the MH-60S. The P3I systems are designed to improve flight safety, enhance and facilitate maintainability, improve airframe longevity, and reduce aircrew fatigue. They include the Active Vibration Control System (AVCS), Ground Proximity Warning System (GPWS), and Integrated Mechanical Diagnostic System (IMDS). In the report, I conclude the following:

- The AVCS is operationally effective and suitable on the MH-60R and MH-60S aircraft. The system was responsive and adaptive to changes in vibratory load throughout all flight regimes and changes to aircraft gross weight, airspeed, rotor speed, and other dynamic flight conditions, as well as mission configurations. All operational test pilots consistently assessed the system as equal or superior to the legacy system in reducing cockpit vibration. The AVCS eliminates the maintenance requirement of the legacy system to periodically tune the rotor system to the appropriate vibration frequency, resulting in the elimination of maintenance man-hours and the test flight hours currently required for vibration analysis and reduction. The lower vibration levels also reduce crew fatigue, making a positive contribution to safety of flight.
- The GPWS is operationally effective and suitable on the MH-60R and MH-60S aircraft. The GPWS is a software algorithm designed to provide timely and appropriate warnings to the pilot so that effective action can be taken to avoid controlled flight into terrain (CFIT). The GPWS met requirements for generating timely warnings (that is, a warning providing enough time for a pilot to take action to avoid CFIT), as well as for not generating false warnings.
- The IMDS is operationally effective and suitable on and for use with the MH-60R and MH-60S aircraft. The IMDS is an embedded aircraft system designed to improve fleet readiness and safety through the early identification of degraded components. It also facilitates maintenance by streamlining maintenance



practices and reducing the number of post-maintenance test flights required. Test results demonstrated the system significantly reduced the time and effort associated with performing several complex maintenance activities.

Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairman and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Adam Smith
Ranking Member



OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

APR 06 2012

The Honorable C. W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

Dear Mr. Chairman:

I have enclosed my Combined Follow-on Operational Test and Evaluation (FOT&E) Report on the MH-60R Multi-Mission Helicopter and MH-60S Multi-Mission Combat Support Helicopter, required by Sections 2399 and 2366, Title 10, United States Code.

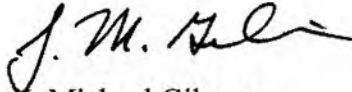
The report assesses Preplanned Product Improvements (P3I) implemented on the MH-60R and the MH-60S. The P3I systems are designed to improve flight safety, enhance and facilitate maintainability, improve airframe longevity, and reduce aircrew fatigue. They include the Active Vibration Control System (AVCS), Ground Proximity Warning System (GPWS), and Integrated Mechanical Diagnostic System (IMDS). In the report, I conclude the following:

- The AVCS is operationally effective and suitable on the MH-60R and MH-60S aircraft. The system was responsive and adaptive to changes in vibratory load throughout all flight regimes and changes to aircraft gross weight, airspeed, rotor speed, and other dynamic flight conditions, as well as mission configurations. All operational test pilots consistently assessed the system as equal or superior to the legacy system in reducing cockpit vibration. The AVCS eliminates the maintenance requirement of the legacy system to periodically tune the rotor system to the appropriate vibration frequency, resulting in the elimination of maintenance man-hours and the test flight hours currently required for vibration analysis and reduction. The lower vibration levels also reduce crew fatigue, making a positive contribution to safety of flight.
- The GPWS is operationally effective and suitable on the MH-60R and MH-60S aircraft. The GPWS is a software algorithm designed to provide timely and appropriate warnings to the pilot so that effective action can be taken to avoid controlled flight into terrain (CFIT). The GPWS met requirements for generating timely warnings (that is, a warning providing enough time for a pilot to take action to avoid CFIT), as well as for not generating false warnings.
- The IMDS is operationally effective and suitable on and for use with the MH-60R and MH-60S aircraft. The IMDS is an embedded aircraft system designed to improve fleet readiness and safety through the early identification of degraded components. It also facilitates maintenance by streamlining maintenance



practices and reducing the number of post-maintenance test flights required. Test results demonstrated the system significantly reduced the time and effort associated with performing several complex maintenance activities.

Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairman and Ranking Members of the Congressional defense committees.

A handwritten signature in black ink, appearing to read "J. M. Gilmore", with a stylized flourish at the end.

J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

APR 06 2012

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

Dear Mr. Chairman:

I have enclosed my Combined Follow-on Operational Test and Evaluation (FOT&E) Report on the MH-60R Multi-Mission Helicopter and MH-60S Multi-Mission Combat Support Helicopter, required by Sections 2399 and 2366, Title 10, United States Code.

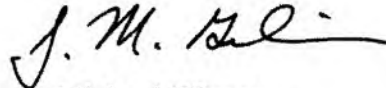
The report assesses Preplanned Product Improvements (P3I) implemented on the MH-60R and the MH-60S. The P3I systems are designed to improve flight safety, enhance and facilitate maintainability, improve airframe longevity, and reduce aircrew fatigue. They include the Active Vibration Control System (AVCS), Ground Proximity Warning System (GPWS), and Integrated Mechanical Diagnostic System (IMDS). In the report, I conclude the following:

- The AVCS is operationally effective and suitable on the MH-60R and MH-60S aircraft. The system was responsive and adaptive to changes in vibratory load throughout all flight regimes and changes to aircraft gross weight, airspeed, rotor speed, and other dynamic flight conditions, as well as mission configurations. All operational test pilots consistently assessed the system as equal or superior to the legacy system in reducing cockpit vibration. The AVCS eliminates the maintenance requirement of the legacy system to periodically tune the rotor system to the appropriate vibration frequency, resulting in the elimination of maintenance man-hours and the test flight hours currently required for vibration analysis and reduction. The lower vibration levels also reduce crew fatigue, making a positive contribution to safety of flight.
- The GPWS is operationally effective and suitable on the MH-60R and MH-60S aircraft. The GPWS is a software algorithm designed to provide timely and appropriate warnings to the pilot so that effective action can be taken to avoid controlled flight into terrain (CFIT). The GPWS met requirements for generating timely warnings (that is, a warning providing enough time for a pilot to take action to avoid CFIT), as well as for not generating false warnings.
- The IMDS is operationally effective and suitable on and for use with the MH-60R and MH-60S aircraft. The IMDS is an embedded aircraft system designed to improve fleet readiness and safety through the early identification of degraded components. It also facilitates maintenance by streamlining maintenance



practices and reducing the number of post-maintenance test flights required. Test results demonstrated the system significantly reduced the time and effort associated with performing several complex maintenance activities.

Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff and the Chairmen and Ranking Members of the Congressional defense committees.

A handwritten signature in black ink, appearing to read "J. M. Gilmore", with a stylized flourish at the end.

J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable John McCain
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

APR 06 2012

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6025

Dear Mr. Chairman:

I have enclosed my Combined Follow-on Operational Test and Evaluation (FOT&E) Report on the MH-60R Multi-Mission Helicopter and MH-60S Multi-Mission Combat Support Helicopter, required by Sections 2399 and 2366, Title 10, United States Code.

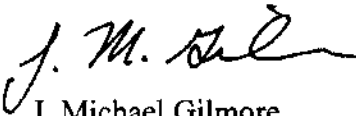
The report assesses Preplanned Product Improvements (P3I) implemented on the MH-60R and the MH-60S. The P3I systems are designed to improve flight safety, enhance and facilitate maintainability, improve airframe longevity, and reduce aircrew fatigue. They include the Active Vibration Control System (AVCS), Ground Proximity Warning System (GPWS), and Integrated Mechanical Diagnostic System (IMDS). In the report, I conclude the following:

- The AVCS is operationally effective and suitable on the MH-60R and MH-60S aircraft. The system was responsive and adaptive to changes in vibratory load throughout all flight regimes and changes to aircraft gross weight, airspeed, rotor speed, and other dynamic flight conditions, as well as mission configurations. All operational test pilots consistently assessed the system as equal or superior to the legacy system in reducing cockpit vibration. The AVCS eliminates the maintenance requirement of the legacy system to periodically tune the rotor system to the appropriate vibration frequency, resulting in the elimination of maintenance man-hours and the test flight hours currently required for vibration analysis and reduction. The lower vibration levels also reduce crew fatigue, making a positive contribution to safety of flight.
- The GPWS is operationally effective and suitable on the MH-60R and MH-60S aircraft. The GPWS is a software algorithm designed to provide timely and appropriate warnings to the pilot so that effective action can be taken to avoid controlled flight into terrain (CFIT). The GPWS met requirements for generating timely warnings (that is, a warning providing enough time for a pilot to take action to avoid CFIT), as well as for not generating false warnings.
- The IMDS is operationally effective and suitable on and for use with the MH-60R and MH-60S aircraft. The IMDS is an embedded aircraft system designed to improve fleet readiness and safety through the early identification of degraded components. It also facilitates maintenance by streamlining maintenance



practices and reducing the number of post-maintenance test flights required. Test results demonstrated the system significantly reduced the time and effort associated with performing several complex maintenance activities.

Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Thad Cochran
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

MAR 29 2012

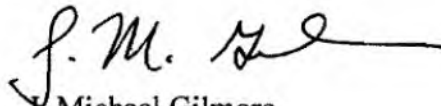
The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6025

Dear Mr. Chairman:

(U) I have enclosed the Follow-on Operational Test and Evaluation (FOT&E) Report on the EA-18G Airborne Electronic Attack (AEA) aircraft with Software Configuration Set (SCS) H6E, as required by Section 2399, Title 10, United States Code. The EA-18G is a derivative of the F/A-18F Super Hornet and serves as the Navy's replacement for the aging fleet of EA-6Bs, providing the capability to detect, identify, locate and suppress hostile emitters. In the report, I conclude the following:

- (U) Testing was adequate to determine the EA-18G AEA system operational effectiveness and suitability within the usual limitations related to testing Electronic Warfare systems.
- (U) The FOT&E results confirm the EA-18G with SCS H6E continues to be operationally effective as an AEA weapon system capable of adequately supporting all mission areas.
- (U) The EA-18G with SCS H6E is now operationally suitable. In particular, FOT&E results show improvements in ALQ-99 pod integration and maintenance documentation relative to Initial Operational Test and Evaluation. Test results demonstrated adequate AEA system availability and reliability; however, maintenance repair time still suffers from poor built-in-test performance.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable Thad Cochran
Ranking Member





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

MAR 29 2012

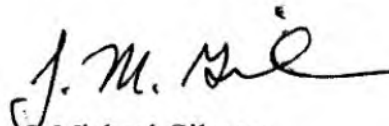
The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

Dear Mr. Chairman:

(U) I have enclosed the Follow-on Operational Test and Evaluation (FOT&E) Report on the EA-18G Airborne Electronic Attack (AEA) aircraft with Software Configuration Set (SCS) H6E, as required by Section 2399, Title 10, United States Code. The EA-18G is a derivative of the F/A-18F Super Hornet and serves as the Navy's replacement for the aging fleet of EA-6Bs, providing the capability to detect, identify, locate and suppress hostile emitters. In the report, I conclude the following:

- (U) Testing was adequate to determine the EA-18G AEA system operational effectiveness and suitability within the usual limitations related to testing Electronic Warfare systems.
- (U) The FOT&E results confirm the EA-18G with SCS H6E continues to be operationally effective as an AEA weapon system capable of adequately supporting all mission areas.
- (U) The EA-18G with SCS H6E is now operationally suitable. In particular, FOT&E results show improvements in ALQ-99 pod integration and maintenance documentation relative to Initial Operational Test and Evaluation. Test results demonstrated adequate AEA system availability and reliability; however, maintenance repair time still suffers from poor built-in-test performance.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable John McCain
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

MAR 29 2012

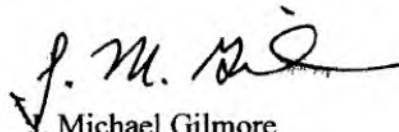
The Honorable C.W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

Dear Mr. Chairman:

(U) I have enclosed the Follow-on Operational Test and Evaluation (FOT&E) Report on the EA-18G Airborne Electronic Attack (AEA) aircraft with Software Configuration Set (SCS) H6E, as required by Section 2399, Title 10, United States Code. The EA-18G is a derivative of the F/A-18F Super Hornet and serves as the Navy's replacement for the aging fleet of EA-6Bs, providing the capability to detect, identify, locate and suppress hostile emitters. In the report, I conclude the following:

- (U) Testing was adequate to determine the EA-18G AEA system operational effectiveness and suitability within the usual limitations related to testing Electronic Warfare systems.
- (U) The FOT&E results confirm the EA-18G with SCS H6E continues to be operationally effective as an AEA weapon system capable of adequately supporting all mission areas.
- (U) The EA-18G with SCS H6E is now operationally suitable. In particular, FOT&E results show improvements in ALQ-99 pod integration and maintenance documentation relative to Initial Operational Test and Evaluation. Test results demonstrated adequate AEA system availability and reliability; however, maintenance repair time still suffers from poor built-in-test performance.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable Norman D. Dicks
Ranking Member





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

MAR 29 2012

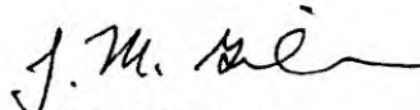
The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

(U) I have enclosed the Follow-on Operational Test and Evaluation (FOT&E) Report on the EA-18G Airborne Electronic Attack (AEA) aircraft with Software Configuration Set (SCS) H6E, as required by Section 2399, Title 10, United States Code. The EA-18G is a derivative of the F/A-18F Super Hornet and serves as the Navy's replacement for the aging fleet of EA-6Bs, providing the capability to detect, identify, locate and suppress hostile emitters. In the report, I conclude the following:

- (U) Testing was adequate to determine the EA-18G AEA system operational effectiveness and suitability within the usual limitations related to testing Electronic Warfare systems.
- (U) The FOT&E results confirm the EA-18G with SCS H6E continues to be operationally effective as an AEA weapon system capable of adequately supporting all mission areas.
- (U) The EA-18G with SCS H6E is now operationally suitable. In particular, FOT&E results show improvements in ALQ-99 pod integration and maintenance documentation relative to Initial Operational Test and Evaluation. Test results demonstrated adequate AEA system availability and reliability; however, maintenance repair time still suffers from poor built-in-test performance.

(U) Section 2399 provides that the Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Navy; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable Adam Smith
Ranking Member

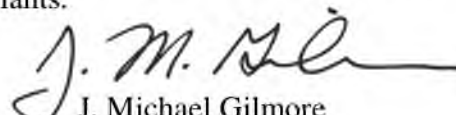


Director, Operational Test and Evaluation
Mine Resistant Ambush Protected (MRAP)
Family of Vehicles:
Dash with Independent Suspension System (ISS)
MRAP Recovery Vehicle (MRV)
Marine Corps Cougar Ambulance
Combined Operational and Live Fire Test and Evaluation Report



March 2012

This report on the three Mine Resistant Ambush Protected (MRAP) Family of Vehicle variants fulfills the provisions of Title 10, United States Code, Sections 2399 and 2366. It assesses the adequacy of testing and the operational effectiveness, operational suitability, and survivability of the Dash with ISS, MRV, and Cougar Ambulance variants.


J. Michael Gilmore
Director

The marginal cost of producing this report is estimated to be approximately \$34,280. The estimated acquisition cost of the program with which this report deals is \$3.5 Billion.



**Navistar Dash Independent
Suspension System (ISS)**



**Navistar MRAP Recovery
Vehicle (MRV)**



**Force Protection Industries (FPI)
Cougar Ambulance**

Executive Summary

This report is an evaluation of the operational effectiveness, suitability, and survivability of three variants of the Mine Resistant Ambush Protected (MRAP) Family of Vehicles: Navistar MRAP Dash with an Independent Suspension System (ISS), Navistar MRAP Recovery Vehicle (MRV), and the Force Protection Industries (FPI) Cougar Ambulance.

The Navistar Dash ISS is operationally effective and suitable for use in Afghanistan. Live Fire Test and Evaluation (LFT&E) of the Dash is ongoing; once this testing and evaluation are complete, the results will be provided in a classified Live Fire vulnerability assessment. Our preliminary assessment of the available LFT&E data indicates the Dash is survivable. The off-road mobility and maneuver capability of the Dash with ISS enabled units to be less predictable in their movement than would be possible without the ISS, continue operations under armor protection, and conduct mounted maneuver to approach and secure an objective.

The Navistar MRV is neither operationally effective nor suitable for recovery operations. LFT&E results indicate the MRV is survivable. The MRV does not possess the capability to traverse most cross-country terrain, rough trails, or steep hills with or without a vehicle in tow. This lack of mobility precludes its effectiveness for use in Afghanistan. The Navistar MRV can, however, perform combat tow and recover damaged MRAPs on flat improved roads and trails.

The FPI Cougar Ambulance is operationally effective and survivable. A unit equipped with the Ambulance can provide protected transport and emergency medical care for casualties in close proximity to enemy forces. In 2010, DOT&E assessed the FPI Cougar Category II A2 with ISS as survivable. Based on Live Fire testing, the integration of an ambulance kit did not affect the survivability of the vehicle. The FPI Cougar Ambulance provides sufficient all-terrain mobility for medical teams to support combat operations. However, the Ambulance is not operationally suitable due to its poor reliability, which contributed to its low availability and high need for maintenance.

The Limited User Test (LUT) was adequate to support an assessment of the operational effectiveness and suitability of the Navistar Dash ISS, Navistar MRV, and the FPI Cougar Ambulance. The Army Test and Evaluation Command (ATEC) conducted the LUT in accordance with the DOT&E-approved test plans. The LFT&E programs were adequate to assess the vulnerability and survivability of the Navistar MRV and Dash ISS, and FPI Cougar Ambulance.

Navistar Dash with ISS

The Navistar Dash ISS vehicle is a lighter, smaller, and more maneuverable version of the Navistar MaxxPro MRAP vehicle. The MRAP program procured 1,696 Navistar MRAP Dash with ISS to support combat operations in Afghanistan.

The Dash-equipped Infantry unit successfully completed 10 of 12 missions during the two 96-hour scenarios of the LUT. The unit employed the Dash ISS to provide security and observation, to maneuver and engage the enemy, and to provide fire support for dismounted

troops. One of the two unsuccessful missions was attributed to two Navistar Dash vehicles that could not negotiate the Afghanistan-like terrain. The other unsuccessful mission was due to lack of fuel---the Dash used far more fuel than anticipated.

During the LUT, the Dash met or exceeded requirements for reliability, maintainability, and availability. The Navistar Dash ISS demonstrated improved reliability relative to the non-ISS version of the vehicle evaluated in the 2009 operational test. The Dash with ISS did not experience the terrain-induced failures that the non-ISS Dash encountered when traversing rough terrain.

Navistar MRAP Recovery Vehicle (MRV)

The Navistar MRV is a two-person Navistar Dash cab built on a commercial platform. The two-person cab is designed to provide MRAP-level protection against underbody and under-wheel blast threats.

During the LUT, the Army and Marine Corps Recovery crews equipped with the Navistar MRV successfully completed seven of 15 missions. Eight unsuccessful missions were attributed to the vehicle's inability to operate in soft soil and on hilly terrain.

There are many different variants of MRAPs in use in Afghanistan. These vehicles have weights that exceed the capability of current wheeled Army recovery vehicles. During the LUT, the Recovery element equipped with the Navistar MRV demonstrated the ability to lift and recover vehicles weighing up to 52,000 pounds on improved flat roads.

The Navistar MRV has poor reliability. During the LUT, the MRV demonstrated 271 Mean Miles Between Operational Mission Failure (MMBOMF) versus its required 600 miles. Human factor and safety problems detracted from the ability of the Recovery element to accomplish missions. Since the Navistar MRV does not have a powered cable payout system for unwinding the winch cable or a tensioner for rewinding slack cable, recovery operations physically exhausted the crews during the LUT. Without a powered payout system, operators must manually pull on the cable to turn the winch drum to unwind the cable.

FPI Cougar Ambulance

The FPI Cougar Ambulance is a Cougar Category II ISS vehicle modified with an ambulance kit that includes medical equipment, special seating, and brackets for two litters. A driver, vehicle commander, and one or two Navy Corpsmen crew the vehicle. The Ambulance can carry two litter patients, four ambulatory patients, or a combination of one litter and two ambulatory patients.

During the LUT, the Ambulance successfully maneuvered over all terrain and demonstrated mobility comparable to the FPI Cougar Category II ISS Troop Carrier tested in November 2009. The Corpsmen successfully executed all treatment tasks. The FPI Cougar Ambulance element successfully treated and evacuated patients in 12 of 17 missions. Four of the five unsuccessful missions were due to ambulance reliability failures. One of the unsuccessful missions was due to a mission execution decision not related to the ambulance.

The FPI Cougar Ambulance has poor reliability. During the LUT, the Ambulance experienced two suspension system mounting bracket failures, which degraded its Maintenance Ratio, Mean Time to Repair, and Operational Availability. This failure mode was not observed in the 2009 operational testing of the FPI Cougar Category II ISS Troop Carrier.

Recommendations

The MRAP Joint Program Manager should consider the following recommendations to improve the operational effectiveness and operational suitability of the MRAP variants:

Navistar MRAP Dash ISS


- Improve the vehicle commander's access to communication system controls and displays.
- Provide tie-down/storage points for ammunition; provide tie-down netting for the rear cargo area; and provide better external storage points for mission equipment (such as a tow bar).

Navistar MRAP Recovery Vehicle

- Improve cross-country mobility.
- Improve system reliability.
- Provide more power for combat towing and climbing hills.
- Install a powered cable payout and tensioner system to reduce operator's physical fatigue from manually winding and unwinding cable.

FPI Cougar Ambulance

- Conduct a failure analysis of the suspension system mounting bracket failures.
- Add a protective shield around the automatic fire extinguishing system valves and piping that are near the head of the driver-side litter patient.
- Reposition communications and navigation system switches located directly adjacent to the forward Corpsman position.
- Provide overhead handholds in the rear of the vehicle.
- Add rifle storage racks in the rear of the vehicle for the Corpsmen.
- Redesign/reposition the handles on the insides of the rear doors.
- Investigate removing the rear tow pintle from Cougar Category II ISS vehicles that are converted to ambulances.


J. Michael Gilmore
Director

This page intentionally left blank.

Contents

System Overview 1

Test Adequacy 5

Navistar Dash Independent Suspension System (ISS)..... 7

Navistar MRAP Recovery Vehicle (MRV) 13

FPI Cougar Ambulance..... 21

Recommendations 27

This page intentionally left blank.

Section One

System Overview

System Description

The Mine Resistant Ambush Protected (MRAP) variants are a family of vehicles (FoV) with a blast resistant body designed to protect their crew from fragmentary blasts, mines, and direct fire weapons. These vehicles are intended to provide greater crew and passenger protection against battlefield threats, such as Improvised Explosive Devices (IEDs), mines, and small arms fire than the current tactical wheeled vehicles such as the High Mobility Multi-purpose Wheeled Vehicles (HMMWVs) with Fragmentation Kit 5. Some vehicles can be configured with additional kits that improve protection against rocket-propelled grenades (RPGs) and explosively-formed projectiles.

The Department of Defense has procured the MRAP FoV to satisfy an urgent need for increased mobility and survivability for ground forces engaging in a wide variety of missions. This report covers three variants from the MRAP FoV:

- The Navistar Dash, modified with an Independent Suspension System (ISS) for improved mobility in the Operation Enduring Freedom (OEF) Theater of Operations, can transport six passengers plus a gunner.
- The Navistar MRAP Recovery Vehicle (MRV) is designed to recover MRAP FoV and other catastrophically damaged vehicles and possess the same survivability characteristics of the MRAP FoV. The program intends the Navistar MRV to provide mobility comparable to the Heavy Expanded Mobility Tactical Truck (HEMTT) wrecker in the OEF Theater of Operations.
- The Force Protection Industries (FPI) Cougar Category II Ambulance with ISS (Cougar Ambulance) is designed to transport two litters or four ambulatory patients, or a combination of one litter and two ambulatory patients.

Figures 1-1 through 1-3 show the Navistar Dash ISS, FPI Cougar Ambulance, and the Navistar MRV.

Navistar Dash with ISS

The Navistar Dash ISS vehicle is a lighter, smaller, and more maneuverable version of the Navistar MaxxPro MRAP vehicle. The MRAP program procured 1,696 Navistar Dash MRAP with ISS to support combat operations in Afghanistan. The Army Test and Evaluation Command (ATEC) conducted the ISS Limited User Test using two ISS-configured Dash vehicles each with a roof-mounted Objective Gunner's Protection Kit, Driver's Vision Enhancer, the "Rhino" infrared counter-IED trigger, and the "Duke" counter-IED jammer. One Dash was equipped with an anti-RPG net system. ATEC tested the non-ISS Dash in 2009 and DOT&E assessed it as not operationally effective or suitable for use in Afghanistan due to mobility and reliability problems related to the solid axle suspension.



Figure 1-1. Navistar Dash ISS with Anti-RPG Net System

Navistar MRAP Recovery Vehicle (MRV)

The Navistar MRV is a two-person Navistar Dash cab built on a commercial platform. The two-person cab is designed to provide MRAP-level protection against underbody and under-wheel blast threats. The recovery and towing systems include a 30-ton boom that can traverse 360 degrees, a 50,000-pound main drag winch, two 25,000-pound boom winches, and a 35,000-pound underlift for towing. Deployable outriggers and a rear spade system stabilize the MRV during recovery operations. The MRV does not have a vehicle-mounted weapon system. The MRAP program procured 390 MRVs.



Figure 1-2. Navistar MRV Conducts Recovery

FPI Cougar Ambulance

The FPI Cougar Ambulance is a Cougar Category II ISS vehicle modified with an ambulance kit that includes medical equipment, special seating, and brackets for two litters. A driver, vehicle commander, and one or two Navy Corpsmen crew the vehicle. The ambulance can carry two litter patients, four ambulatory patients, or a combination of one litter and two ambulatory patients. It is equipped with the Objective Gunner's Protective Kit. The vehicle

does not have a gunner's stand. The Cougar Category II ISS Troop Carrier (non-ambulance) was tested in 2009 and found to be operationally effective and suitable. The MRAP program procured 30 ambulance kits to retrofit production FPI Cougar Category II ISS vehicles for Marine Corps use in Afghanistan.



Figure 1-3. FPI Cougar Ambulance (left) and Interior of Cougar Ambulance (right)

Mission

Units equipped with MRAP vehicles conduct small unit combat operations such as mounted patrols, medical treatment, security, route clearance, and battlefield recovery. Army units employ the Navistar Dash ISS to conduct reconnaissance, patrols, and convoy security missions. The Marine Corps units employ the FPI Cougar Ambulance to transport and provide emergency care for battlefield casualties. The Army and Marine Corps units equipped with Navistar MRV intend to recover and tow disabled vehicles over small roadways, mountainous areas, and rugged terrain conditions in Afghanistan.

Operational Concept

The Navistar Dash ISS variant is primarily a transport vehicle. Threat conditions might require employment as a combat vehicle in close combat engagements to support dismounted infantry. The Army intends for Navistar Dash ISS-equipped units to operate with minimal external support for up to 96 hours. Forces use specialized MRAP variants for support functions such as medical evacuation and recovery operations. A Marine Corps medical element will employ the FPI Cougar Ambulance to move casualties and provide enroute care to maneuvering troops with matched mobility and survivability as the unit they support. The Army and Marine Corps units will use the Navistar MRV to recover MRAPs and other damaged vehicles on the small roads and rugged terrain of Afghanistan. The Navistar MRV will provide the same level of IED protection as the MRAPs being recovered.

Maintenance Concept

Consistent with practice in Afghanistan, Soldier maintainers perform unit-level maintenance for the Dash ISS. Contractor Field Service Representatives perform unit-level

maintenance for the Navistar MRV and Cougar Ambulance. Dash ISS Field Service Representatives will assist the Soldier maintainers if there is a maintenance action above their level of experience or training.

Section Two

Test Adequacy

The Limited User Test (LUT) was adequate to support an assessment of the operational effectiveness and suitability of the Navistar Dash ISS, Navistar MRV, and the FPI Cougar Ambulance. The Army Test and Evaluation Command (ATEC) conducted the operational testing in accordance with the DOT&E-approved test plans. The Live Fire Test and Evaluation program was adequate to assess the vulnerability and survivability of the Navistar MRV and Dash ISS, and FPI Cougar Ambulance.

ATEC executed the LUT at Yuma Proving Ground, Arizona, from June 12-25, 2011. The test unit consisted of an Infantry Company composed of two platoons with 15 Marine Corps personnel and four Navy Corpsmen attached to these platoons. The Infantry Company employed three Dash ISSs augmented with three MRAP All Terrain Vehicles (M-ATVs). A joint Army-Marine Corps recovery element employed two Navistar MRVs. Infantry Soldiers with eight High Mobility Multi-purpose Wheeled Vehicles (HMMWVs) provided security for the Navistar MRV element. A Marine Corps ambulance element employed two FPI Cougar Ambulances and two M-ATVs. The two M-ATVs provided security for the Cougar Ambulance Element. The test unit conducted testing on terrain that matched Afghanistan. A Heavy Expanded Mobility Tactical Truck (HEMTT) wrecker and one Marine Corps Mk 48 Logistics Vehicle System (LVS) wrecker provided administrative recovery support for the test.

The Infantry Company conducted four Operation Enduring Freedom (OEF) presence patrol/show-of-force missions, four convoy security missions, and four route reconnaissance missions. Of these 12 operational missions, the company conducted eight daytime and four nighttime missions.

The Navistar MRV element conducted 15 missions, including five recovery missions, five towing missions, and five combined recovery and towing missions. The Navistar MRV element was in direct support of the infantry unit or was tasked independently by a simulated battalion operations cell. Two of the five recovery missions were conducted as Special Test Events. Approximately one-half of the Navistar MRV missions were conducted at night.

The Cougar Ambulance element conducted 17 medical evacuation missions. The operational missions were conducted in direct support of the Infantry Company or independently tasked by a simulated battalion operations cell. One-third of the missions were conducted at night.

The Infantry Unit conducted seven special test events: urban mobility, vehicle towing, Navistar MRV Lift-tow and Flat-tow, Flat-tow Dash ISS, night driving, Casualty Evacuation (CASEVAC), ingress/egress, Navistar MRV recovery of mired MRAP vehicles, and Navistar MRV self-recovery in mud.

Table 2-1. Test Scope

Unit	Vehicles and Planned Miles	Missions
Army Infantry Company	3 Dash ISSs 3 M-ATVs 6 HMMWVs	4 Presence Patrol/Show-of-Force 4 Convoy Security 4 Route Reconnaissance 12 Total Missions
Army and Marine Corps Recovery Element	1 Navistar MRV (Army) 1 Navistar MRV (Marine Corps) 2 HMMWVs (security element)	1 Recovery of MRAP mired in mud (Special Test Event (STE)) 1 Self-recovery of Navistar MRV mired in mud (STE) 3 Recovery (45-degree and 90-degree) 5 Combat tow 5 Recovery and combat tow (45-degree and 90-degree) 15 Total Missions
Marine Corps Ambulance Element	2 Cougar Ambulances 2 M-ATVs (security element)	17 Medical Evacuations

Opposing Force

An enemy force consisting of light infantry with assault rifles and rocket-propelled grenades (RPGs) attacked the unit during test missions. In addition to blank ammunition, the enemy used RPG simulators that included a noise and smoke replicator to add realism. Small explosive charges along the routes simulated Improvised Explosive Devices (IEDs). The enemy force used hit-and-run tactics to engage the units.

Test Limitations

During developmental testing, the Navistar MRV demonstrated poor off-road mobility and could not safely negotiate Yuma terrain during the LUT. Consequently, the test unit assigned the Navistar MRV to less demanding routes and controlled events.

Live Fire Test and Evaluation

As outlined in the 2011 DOT&E Annual Report, Live Fire testing of the Navistar MRV and Cougar Ambulance indicates both vehicles are survivable. In 2010, DOT&E assessed the FPI Cougar Category II A2 with ISS as survivable. Based on Army Live Fire testing of the FPI Cougar Ambulance, the integration of an ambulance kit did not affect the survivability of the vehicle. The Navistar MRV is survivable based on assessment of Army LFT&E results. LFT&E of the Navistar Dash ISS is ongoing and the results will be reported separately in a classified Live Fire vulnerability assessment. Our preliminary assessment of the live fire test data indicates that the Navistar Dash ISS is survivable.

Section Three

Navistar Dash Independent Suspension System (ISS)



Figure 3-1. Navistar Dash ISS

Operational Effectiveness

The Navistar Dash ISS is operationally effective for use in Afghanistan. The off-road mobility and maneuver capability of the Dash with ISS enabled units to be less predictable in their movement relative to non-ISS vehicles, continue operations under armor protection, and conduct a greater variety of mounted maneuvers to approach and secure an objective.

In urban environments with narrow streets, multi-story buildings, and alleys, the Dash is less maneuverable than an up-armored High Mobility Multi-purpose Wheeled Vehicle (HMMWV) due to the Dash's large size and turning radius. Small windows limit crew visibility. The unit operating the Dash on unimproved trails and roads through mountainous terrain will have sufficient power, rate of climb, and acceleration to maintain speed and maneuver comparable to the up-armored HMMWV.

The Dash-equipped Infantry unit successfully completed 10 of 12 missions during the two 96-hour scenarios of the LUT. The unit employed the Dash ISS to provide security and observation, to maneuver and engage the enemy, and to provide fire support for dismounted troops. One of the two unsuccessful missions was attributed to two vehicles that could not negotiate the terrain. The other unsuccessful mission was due to lack of fuel---the Dash ISS used far more fuel than anticipated.

Unit Mission Accomplishment

Unit mission success for the Infantry Company was evaluated against mission-specific and common criteria. The mission-specific criteria were the unit's assigned tasks and purpose as stated in the Operations Order. Table 3-1 shows success during the LUT. The criteria used to evaluate mission success include the following:

Common Criteria

- Meet Commander's intent - accomplish the major elements of the mission in the time required with the unit postured and capable of follow-on missions.
- Depart the mission within 15 minutes of the specified time.
- Begin the mission with four of six Dash ISSs and M-ATVs and maintain at least four of six vehicles in a fully mission capable status throughout the mission.
- Maintain at least 90 percent personnel strength.
- Traverse the entire route specified in the operational plan.

Mission-specific Criteria

- *Convoy Security.* Provide security, deliver supplies, and deter or destroy enemy along route.
- *Route Reconnaissance.* Detect, observe, and report enemy activity, obstacles, key terrain, and IEDs on the route.
- *Show of Force/Presence Patrol.* Obtain detailed information concerning terrain and enemy activity within prescribed area.

Table 3-1. Unit Mission Accomplishment

	Common Criteria					Mission Specific Criteria			Mission Success, Comments
Operational Mission Profile (OMP)	Meet Commander's Intent	Depart Mission within 15 minutes of designated time	4 of 6 vehicles available throughout mission	Maintain 90% crew strength throughout mission	All vehicles traverse entire routes	Convoy Security	Route Recon	Presence Patrol	
OMP 1A Presence Patrol	YES	YES	YES	YES	YES	N/A	N/A	YES	Successful
OMP 1B Presence Patrol	YES	YES	YES	YES	YES	N/A	N/A	YES	Successful
OMP 2A Convoy Security	YES	YES	YES	YES	YES	YES	N/A	N/A	Successful
OMP 2B Convoy Security	YES	YES	NO	YES	YES	NO	N/A	N/A	Not Successful, the Dash ISS used more fuel than anticipated. Onboard fuel not sufficient to complete mission
OMP 3A Route Recon	YES	YES	YES	YES	YES	N/A	YES	N/A	Successful
OMP 3B Route Recon	YES	YES	YES	YES	YES	N/A	YES	N/A	Successful
OMP 3 Route Recon	YES	YES	YES	YES	YES	N/A	YES	N/A	Successful
OMP 3D Route Recon	YES	YES	YES	YES	YES	N/A	NO	N/A	Unsuccessful, 2 Dashes could not negotiate hilly terrain, needed tow assistance
OMP 2C Convoy Security	YES	YES	YES	YES	YES	YES	N/A	N/A	Successful
OMP 2D Convoy Security	YES	YES	YES	YES	YES	YES	N/A	N/A	Successful
OMP 1C Presence Patrol	YES	YES	YES	YES	YES	N/A	N/A	YES	Successful
OMP 1D Presence Patrol	YES	YES	YES	YES	YES	N/A	N/A	YES	Successful

System Performance

Mobility/Cruising Range

The Navistar Dash ISS is required to travel on improved roads at 45 miles per hour for 300 miles without refueling. In operational usage over theater-representative terrain, the Dash demonstrated less than the required unrefueled range in the LUT. During the LUT, the unrefueled range of the Dash was approximately 188 miles using fuel from its fuel tank (57 gallons) and two externally carried 5-gallon cans; thus, the vehicle averaged 2.8 miles per gallon. The short unrefueled range is likely attributable to rough terrain and the need for continuous engine idling during missions to maintain power and cooling. In comparison, the M-ATV unrefueled range during the LUT, when crews operated the M-ATV's over the same terrain with equivalent idling, was approximately 234 miles despite its smaller 47-gallon fuel tank (and including its two 5-gallon cans in the calculation). The M-ATV averaged 4.1 miles per gallon.

Operational Suitability

The Navistar Dash ISS is operationally suitable. During the LUT, the Dash met or exceeded requirements for reliability, maintainability, and availability, demonstrating improved reliability relative to the non-ISS version of the vehicle. The Dash ISS did not experience the terrain-induced failures the non-ISS Dash encountered when traversing rough terrain. There were no human factors or safety issues with the Navistar Dash ISS.

Reliability, Availability, and Maintainability

The MRAP FoV reliability, availability, and maintainability (RAM) parameters are the following: Mean Miles Between Operational Mission Failure (MMBOMF), Maintenance Ratio (MR) expressed as Maintenance Man-hours (MMH) per mile, Mean Time To Repair (MTTR) expressed as the total maintenance clock time divided by the number of unscheduled repair actions, and Operational Availability (A_O) expressed as the ratio of system uptime to the sum of uptime and downtime (total time). Table 3-2 depicts the LUT data used to estimate the parameters, and Table 3-3 shows the RAM parameter estimates.

Table 3-2. Dash ISS LUT RAM Data

Miles	Operational Mission Failures	Maintenance Man-Hours	Uptime (hrs)	Downtime (hrs)	Maintenance Clock Hours	Number of Repair Actions
2,517	2	16.5	976.3	89.6	9.1	26

Table 3-3. Dash ISS RAM Parameter Estimates

Parameter	Requirement	Demonstrated
Reliability (MMBOMF)	≥ 600 miles	1,259 miles
		80% confident MMBOMF ≥ 596 miles
Maintainability (MR)	≤ 0.0065 MMH/mile	0.0065 MMH/mile
Maintainability (MTTR)	≤ 0.75 hours	0.35 hours
Operational Availability (Ao)	≥ 0.90	0.92

The Navistar Dash ISS demonstrated its reliability with 79 percent confidence. During the LUT, the Dash experienced two Operational Mission Failures (OMFs): one flat tire and one stuck door handle, which degraded the crew's ability to exit the vehicle. The Navistar Dash ISS met its MR, MTTR, and Ao requirements during the LUT.

Human Factors Engineering and Safety Shortfalls

The Dash ISS was able to carry assigned crew and mission equipment. The vehicle lacks internal and external tie-down points for securing heavy equipment such as a tow bar and ammunition. The vehicle commander does not have easy access to displays and controls of command and control equipment.

This page intentionally left blank.

Section Four

Navistar MRAP Recovery Vehicle (MRV)



Figure 4-1. Navistar MRV

Operational Effectiveness

The Navistar MRV is not operationally effective for recovery operations. The MRV provides poor combat towing and poor mobility to recover damaged MRAP vehicles over Afghanistan-like terrain. The MRV is not able to traverse most cross-country terrain, rough trails, or steep hills with or without a vehicle in tow. The lack of vehicle mobility affects a unit's ability to accomplish missions in those conditions. The Navistar MRV can combat tow and recover damaged MRAPs on flat improved roads and trails.

During the LUT, the Army and Marine Corps Recovery crews equipped with the Navistar MRV successfully completed seven of 15 missions. The crews failed to accomplish eight assigned missions:

- In two 45-degree recovery and combat tow missions, the Navistar MRV got mired in sand and could not traverse hilly terrain.
- In four combat tow missions, the Navistar MRV could not traverse hills on three missions and lost engine power on one mission.
- In two 90-degree recovery and combat missions, the Navistar MRV got stuck in soft soil en-route to the recovery site.

In all missions, the crews successfully conducted tasks employing the Navistar MRV such as rotating the boom, boom winches, and main drag winch to recover damaged MRAPs in a variety of positions. These capabilities are meant to provide a Recovery crew with the flexibility to recover MRAPs in a variety of positions and states of damage. Figure 4-2 shows the Navistar MRV performing a 90-degree recovery.



Figure 4-2. Navistar MRV Performs 90-Degree Recovery

Recovery Element Mission Success

The mission success criteria for the Navistar MRV element were the following:

- Traverse the entire mission route
- Successfully perform recovery
- Tow damaged MRAPs without further damage to the towed vehicle or injury to personnel

The notional Infantry battalion headquarters assigned the Navistar MRV element 15 recovery missions, including five Special Test Events (STEs) (one self-recovery from a mud pit, one recovery of an MRAP that was mired in mud, and three other MRAP recovery missions), five combat tow missions, and five combined recovery and combat tow missions. Recovery missions were systematically varied based on the angle of recovery formed between the Navistar MRV boom and the longitudinal axis of the Navistar MRV.

Table 4-1. Recovery Element Mission Success

Operational Mission Profile (OMP)	Accomplish Recovery	Tow over specified route without damage or injury	Traverse entire mission route	Mission Success, Comments
OMP-1P 90-degree Recovery and Combat Tow	YES	YES	YES	Successful
OMP-1P 45-degree Recovery and Combat Tow	YES	NO	NO	Not Successful, Navistar MRV stuck in sand and not able to traverse hill
Special Test Event (STE): Self Recovery	YES	N/A	N/A	Successful
STE: Mired Recovery	YES	N/A	N/A	Successful
OMP-1A/B 45-degree Recovery	YES	N/A	YES	Successful
OMP-1A/B 90-degree Recovery and Combat Tow	YES	YES	YES	Successful
OMB-1A/B Combat Tow	N/A	YES	YES	Successful
OMP-2A/B Combat Tow	N/A	NO	NO	Not Successful, Navistar MRV could not traverse hill
OMP-3A/B 45-degree Recovery	YES	N/A	YES	Successful
OMP-3A/B 90-degree Recovery and Combat Tow	YES	YES	NO	Not Successful, Navistar MRV stuck in sand en-route to recovery site
OMP-3C/D 90-degree Recovery and Combat Tow	YES	YES	NO	Not Successful, Navistar MRV stuck in sand
OMP-3C/D 45-degree Recovery and Combat Tow	YES	NO	NO	Not Successful, Navistar MRV stuck in sand with tow
OMP-2C/D Combat Tow	N/A	NO	NO	Not Successful, Navistar MRV delayed on hill with tow
OMP-2C/D Combat Tow	N/A	NO	NO	Not Successful, Navistar MRV Engine Died
OMP-1C/D Combat Tow	N/A	NO	NO	Not Successful, Navistar MRV could not traverse hill with tow

System Performance

Mobility

During the LUT, the Navistar MRV possessed poor mobility. The vehicle was not capable of traversing all routes needed to support the Infantry unit's missions. For 47 percent (7/15) of the LUT missions, the MRV could not maneuver with a combat tow load, although it demonstrated sufficient mobility on flat surface routes. The MRV lacked the power to traverse long-steep inclines in the LUT when towing MRAPs weighing over 38,000 pounds. The MRV

has limited ground clearance and its long wheelbase prevented the vehicle from keeping all wheels on trails when turning. The MRV's movement within the simulated urban village was a slow deliberate process that required the vehicle to use multi-point turns.

Recovery

MRV elements successfully completed 10 of 10 recovery tasks. The Navistar MRV was most useful when recovering damaged vehicles. The boom winches and main drag winch provide the MRV operator with the capability to recover damaged MRAPs. During the LUT, the boom was used several times to lift and load the recovered asset onto a simulated trailer bed and to provide a lifting force on the recovered MRAP while the main drag winch pulled an MRAP from a ravine. The MRV provides the operator with three different winches.

Navistar MRV versus HEMTT Wrecker

Although the Heavy Expanded Mobility Tactical Truck (HEMTT) wrecker was not under test, its presence in the LUT in a support role allowed a qualitative comparison of Navistar MRV and HEMTT wrecker recovery and maneuver capabilities. The MRV did not demonstrate mobility comparable to that of the HEMTT wrecker during the LUT. The HEMTT wrecker successfully traversed all mission routes, including sections that were not safe for the MRV. The HEMTT towed the MRVs twice and freed MRVs from sand three times.

The Navistar MRV is authorized to lift-tow MRAPs that have a maximum weight of 55,000 pounds.¹ In the LUT, MRVs demonstrated the capability to lift-tow the Cougar Ambulance, which weighed approximately 49,000 pounds. The MRV provides better lift capability than the HEMTT due to the operational range of the two 25,000-pound boom winches for lift, and a 50,000-pound main drag/pull winch. The HEMTT wrecker is limited to one main drag winch to drag/pull 60,000-pound damaged vehicles.

Table 4-2 compares the key automotive, mobility and lift parameters measured during the HEMTT and Navistar MRV developmental tests.

¹ MRAPs weighing less than 55,000 pounds include the M-ATV, RG33, Heavy Armored Ground Ambulance (HAGA), Caiman Category I MRAP, Cougar Ambulance, Cougar (Category I and II), RG-31, MaxxPro, MaxxPro Plus, Dash (ISS and non-ISS), and Dash Ambulance.

Table 4-2. Navistar MRV and HEMTT Wrecker Comparison

Measure	Navistar MRV	HEMTT
Engine horsepower (hp)	375 hp	450 hp
Horsepower to weight ratio	12.9 hp/ton	16.6 hp/ton
Maximum speed	57 mph	64 mph
Side slope	30 degrees	40 degrees
Time to accelerate to 55 mph	62 seconds	< 26 seconds
Lateral force to effect roll over	0.38 g	0.60 g
Minimum ground clearance	9.3 inches	11.9 inches
Crane Capacity	62,000 pounds	14,000 pounds
Drag Winch Capacity	50,000 pounds	60,000 pounds
Underlift Rating	35,000 pounds	25,000 pounds
Boom Winches Capacity	25,000 pounds	None

Operational Suitability

The Navistar MRV is not operationally suitable. The vehicle has poor reliability. During the LUT, the MRV demonstrated 271 Mean Miles Between Operational Mission Failure (MMBOMF) versus its required 600 miles. The Navistar MRV had difficulty performing its mission essential functions of move and vehicle recovery/maintenance. Human factor and safety problems detracted from the ability of the Recovery element to accomplish missions. Since the Navistar MRV does not have a powered cable payout system for unwinding the winch cable or a tensioner for rewinding slack cable, recovery operations physically exhausted the crews during the LUT. The Recovery teams were able to use the Navistar MRV communication, command, and control equipment to provide communication and exchange tactical information throughout the LUT.

Reliability, Availability, and Maintainability (RAM)

Table 4-3 shows the LUT data used to estimate the RAM-related parameters, and Table 4-4 shows the RAM estimates.

Table 4-3. NAVISTAR MRV LUT RAM Data

Miles	Operational Mission Failures	Maintenance Man-Hours	Uptime (hrs)	Downtime (hrs)	Maintenance Clock Hours	Number of Repair Actions
1,356	5	114.9	553.4	243.8	57.4	46

Table 4-4. Navistar MRV RAM Parameter Estimates

Parameter	Requirement	Demonstrated
Reliability (MMBOMF)	≥ 600 miles	271 miles
		80% confident MMBOMF ≥ 147 miles
Maintainability (MR)	≤ 0.0065 MMH/mile	0.0847 MMH/mile
Maintainability (MTTR)	≤ 0.75 hours	1.25 hours
Operational Availability (Ao)	≥ 0.90	0.69

The Navistar MRV is not reliable. The vehicle demonstrated a MMBOMF of 271 miles well below the MRAP FoV 600-mile requirement. The following five operational mission failures (OMFs) affected the Recovery element employment during the LUT:

- Two engine failures
- Overheated transmission
- Transmission that would not shift into low gear
- Front axle that would not engage in 6 x 6 drive

These OMFs required considerable maintenance time to diagnose and repair. The low Operational Availability of the Navistar MRV was due to lengthy maintenance time, delays towing MRVs to maintenance, and time awaiting spare parts.

Human Factors Engineering and Safety

Unwinding Winch Cables to Recover Vehicle

During the LUT, the task of unwinding winch cables to connect to a vehicle and rewinding the cables on the winch drum after recovery physically exhausted the recovery operators. One operator required medical assistance due to heat fatigue experienced during one LUT mission. The Navistar MRV does not have a powered payout system to assist the operator in unwinding cables to connect to a vehicle. Without a powered payout system, operators must manually pull on the cable to turn the winch drum to unwind the cable. Figure 4-3 shows a Soldier unwinding one of the boom winch cables to prepare for a recovery.



Figure 4-3. Soldier Manually Unwinding Cable on Boom Winch

Rewinding Winch Cable Following Recovery

The Navistar MRV lacks a power cable tensioning system to control the cable tension when rewinding a cable onto the winch drum without a load attached. Without sufficient tension, the cable becomes tangled on the drum. This condition is known as “bird nesting.” When bird nesting occurs, the operator has difficulty with payout and rewinding the cable. Bird nesting can permanently damage or deform the cable. During the LUT, there was one incident of a frayed cable.

Figure 4-4 depicts the bird nesting condition on the main drag winch drum and the resultant bend in the cable.



Figure 4-4. Bird nesting and Result

This page intentionally left blank.

Section Five

FPI Cougar Ambulance



Figure 5-1. FPI Cougar Ambulance

Operational Effectiveness

The FPI Cougar Ambulance is operationally effective. A unit equipped with the Ambulance can provide protected transport and emergency medical care for casualties in close proximity to enemy forces. The Ambulance provides sufficient all-terrain mobility for medical teams and to support combat operations.

During the LUT, the FPI Cougar Ambulance successfully maneuvered over all terrain and demonstrated mobility comparable to the FPI Cougar Category II ISS Troop Carrier tested in November 2009. The Corpsmen successfully executed all treatment tasks. Invasive procedures were demonstrated rather than executed and were observed by medical subject matter experts. The Corpsmen effectively used the patient management/movement equipment on the ambulance.

The FPI Cougar Ambulance element successfully treated and evacuated patients in 12 of 17 missions. Three unsuccessful missions occurred while the ambulances were in the area support role:

- The FPI Cougar Ambulances could not negotiate the terrain on two missions due to failures of the suspension system mounting bracket.
- The Ambulance element was not able to accomplish one mission because both Cougar Ambulances were in maintenance.

Two unsuccessful missions occurred while the ambulances were providing direct support to the Dash ISS-equipped unit:

- An FPI Cougar Ambulance was not available to the Ambulance Element due to a reliability failure.
- The Ambulance element decided to abandon the mission because of low fuel.

Ambulance Element Mission Success

The FPI Cougar Ambulance element operated in two doctrinal roles during the LUT. In the “area support” role, the element responded to evacuation missions tasked through the Infantry unit or its notional battalion headquarters. In the “direct support” role, the Ambulance element responded to casualties in the Infantry Company caused by the enemy force. In both roles, the element was assessed against the following mission success criteria:

- The ambulances must be available to start the mission.
- The ambulances must be able to traverse all terrain on the specified route.
- The Corpsmen must be able to execute the casualty treatment steps listed on a patient-specific casualty card.

Subject matter experts developed the casualty cards before the test, focusing on injuries resulting from IEDs, small arms, and RPGs. The distribution of simulated injuries based on the casualty cards was executed in the test in order to assess the Corpsmen’s ability to treat a wide variety of patients in the possible combinations that the vehicle was expected to support. The Corpsmen were required to employ the capabilities of the ambulance’s medical equipment, such as suction devices, intravenous injections, oxygen, physiological condition monitoring, and lighting to treat casualties.

Table 5-1. FPI Cougar Ambulance Element Mission Success

Operational Mission Profile (OMP)	Number of Ambulances Participated in Mission versus Planned	Ambulances Traverse Entire Terrain Route	Treat Casualties (Treated/Planned Casualties)	Mission Success, Comments
OMP-1A/B MEDEVAC 1	N/A	N/A	N/A	N/A, First mission was No Test due to Range Conflict
OMP-1A/B MEDEVAC 2	2 of 2	YES	YES (3/3)	YES
OMP-1A/B MEDEVAC 3	2 of 2	YES	YES (4/4)	YES
OMP-2A/B MEDEVAC 1	2 of 2	YES	YES (4/4)	YES
OMP-2A/B MEDEVAC 2	1 of 2	NO	YES (2/5)	NO – At start of mission, one Cougar Ambulance experienced 2 reliability failures
OMP-2A/B MEDEVAC 3	2 of 2	YES	YES (2/3)	YES – Test Unit did not provide enough casualties
OMP-3A/B MEDEVAC 1	1 of 2	NO	YES (4/4)	NO – at end of mission, one Cougar Ambulance experienced suspension failure
OMP-3A/B MEDEVAC 2	1 of 2	NO	YES (3/5)	NO – at end of mission, the remaining Cougar Ambulance experienced suspension failure
OMP-3A/B MEDEVAC 3	0 of 2	NO	NO (0/3)	NO – neither Cougar Ambulance available to conduct mission due to earlier suspension failures
OMP-3C/D MEDEVAC 1	2 of 2	YES	YES (4/4)	YES
OMP-3C/D MEDEVAC 2	2 of 2	YES	YES (5/5)	YES
OMP-3C/D MEDEVAC 3	2 of 2	YES	YES (3/3)	YES
OMP-2C/D MEDEVAC 1	2 of 2	YES	YES (4/4)	YES
OMP-2C/D MEDEVAC 2	2 of 2	YES	YES (5/5)	YES
OMP-2C/D MEDEVAC 3	2 of 2	NO	YES (3/3)	NO – one Cougar Ambulance had rear tire splayed. Unit lost on route. After re-direction, the unit abandoned mission due to low fuel and bad tire
OMP-1C/D MEDEVAC 1	2 of 2	YES	YES (4/4)	YES
OMP-1C/D MEDEVAC 2	2 of 2	YES	YES (3/3)	YES
OMP-1C/D MEDEVAC 3	2 of 2	YES	YES (5/5)	YES

System Performance

Payload Capacity and Storage

Like other MRAP vehicles, the ambulance does not have sufficient space for equipment stowage. During the LUT, personal and mission equipment were stowed on the floor or under seats where they can become tripping hazards or projectiles in the event of an IED attack. When the ambulance is fully loaded, the ambulance crew has a cramped work area.

Operations of Weapon Station²

The ability of the ambulance crew to employ a weapon mounted on the FPI Cougar Ambulance would contribute to crew survivability. Although the Ambulance is equipped with the Objective Gunner's Protection Kit, which is capable of mounting a machine gun, the ambulance does not have a gunner's stand. The interior space of the Ambulance lacks the space to allow a gunner's stand, which would interfere with the forward medical attendant's seat and the Corpsmen's ability to treat patients.

Operational Suitability

The FPI Cougar Ambulance is not operationally suitable due to its poor reliability, which contributed to its low availability and high need for maintenance. During the LUT, the FPI Cougar Ambulance experienced two suspension system mounting bracket failures, which degraded its Maintenance Ratio (MR), Mean Time to Repair (MTTR), and Operational Availability. Based on the LUT, the Ambulance can be maintained by Marines at the organizational level. Contractor Field Service Representatives assisted the military maintenance team as required.

Reliability, Availability, and Maintainability (RAM)

Table 5-2 depicts the LUT data used to estimate the parameters, and Table 5-3 shows the RAM parameter estimates.

Table 5-2. FPI Cougar Ambulance LUT RAM Data

Miles	Operational Mission Failures	Maintenance Man-Hours	Uptime (hrs)	Downtime (hrs)	Maintenance Clock Hours	Number of Repair Actions
1,835	5	74.8	487.4	220.3	27.2	31

² U.S. Army Field Manual 27-10, *The Law of Land Warfare*, states that medical personnel are permitted to defend themselves and their patients. In 2008, the Army tested two MRAP ambulances (Navistar MaxxPro Ambulance and the BAE Heavy Armored Ground Ambulance), which were equipped with M249 5.56 mm Squad Automatic Weapons mounted in the Objective Gunner's Protection Kit.

Table 5-3. FPI Cougar Ambulance RAM Parameter Estimates

Parameter	Requirement	Demonstrated
Reliability (MMBOMF)	≥ 600 miles	376 miles
		80% confident MMBOMF ≥ 109 miles
Maintainability (MR)	≤ 0.0065	0.0407 MMH/mile
Maintainability (MTTR)	≤ 0.75 hours	0.88 hours
Operational Availability (Ao)	≥ 0.90	0.71

As summarized in Table 5-3, the FPI Cougar Ambulance demonstrated a Mean Miles Between Operational Mission Failure (MMBOMF) of 376 miles after experiencing five operational mission failures, short of its 600-mile threshold requirement. The MMBOMF for the FPI Cougar Category II ISS Troop Carrier in its 2009 operational test was 1,521 miles.

Suspension system mounting bracket failures caused two of the operational mission failures. This failure mode was not observed in the 2009 operational testing of the FPI Cougar Category II ISS Troop Carrier. The three other operational mission failures consisted of a flat tire, a spurious activation of the automatic fire extinguishing system, and an inability of the driver to unlock the differential. Ambulance-unique mission equipment did not contribute to the operational mission failures.

The demonstrated MTTR repair of .88 hours did not meet the 0.75 hour requirement. The mounting bracket failures contributed to the greater-than-desired maintenance time and low Operational Availability. Contractor maintainers required 57 man-hours to fix the suspension system mounting brackets.

Human Factors Engineering and Safety Shortfalls

The ambulance crew experienced several human factors and safety shortfalls during the LUT. The following shortfalls impede the ability of the Corpsman to provide safe, effective treatment in and evacuation from the ambulance.

- The Corpsmen lack overhead handholds to grasp onto while treating patients when the vehicle is in motion.
- Corpsmen in the rear of the vehicle lack rifle stowage racks to hold their weapons while they are treating patients.
- Several command and control system switches are adjacent to the forward Corpsman seat as shown in Figure 5-2. Due to the close location of these switches, the Corpsman sometimes unintentionally changes the switch positions or pulls out a cable when the vehicle is moving.
- As shown in Figure 5-3, the driver's-side litter patient's head is next to several automatic fire extinguishing system valves and piping. During the LUT, one litter patient hit his head on the valves.



Figure 5-2. FPI Cougar Ambulance Medical Attendant Seat; Command and Control Switch Interference



Figure 5-3. FPI Cougar Ambulance Fire Extinguishing Valves and Litter Interference

- The rear towing pintle hook impinges on the steps to the rear door and poses a tripping hazard when loading patients as shown in Figure 5-4.



Figure 5-4. FPI Cougar Ambulance Door Handles and Pintle Hook

Section Six Recommendations

The Joint Program Manager for MRAP vehicles should consider the following recommendations to improve the operational effectiveness and operational suitability:

Navistar MRAP Dash ISS

- Improve the vehicle commander's access to communication system controls and displays.
- Provide tie-down/storage points for ammunition; provide tie-down netting for the rear cargo area; and provide better external storage points for mission equipment (such as a tow bar).

Navistar MRAP Recovery Vehicle

- Improve cross-country mobility.
- Improve system reliability.
- Provide more power for combat towing and climbing hills.
- Install a powered cable payout and tensioner system to reduce operator's physical fatigue from manually winding and unwinding cable.

FPI Cougar Ambulance

- Conduct a failure analysis of the suspension system mounting bracket failures.
- Add a protective shield around the automatic fire extinguishing system valves and piping that are near the head of the driver-side litter patient.
- Reposition communications and navigation system switches located directly adjacent to the forward Corpsman position.
- Provide overhead handholds in the rear of the vehicle.
- Add rifle storage racks in the rear of the vehicle for the Corpsmen.
- Redesign/reposition the handles on the insides of the rear doors.
- Investigate removing the rear tow pintle from Cougar Category II ISS vehicles that are converted to ambulances.



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

MAR 22 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

In FY11, the MRAP program procured ISS kits to improve the off-road capability of the Navistar Dash, the Navistar MRAP Recovery Vehicle to fulfill an urgent need to recover damaged MRAP vehicles in Afghanistan, and ambulance kits to modify existing Force Protection Industries (FPI) Cougar Category II A2 ISS vehicles to satisfy Marine Corps casualty evacuation requirements.

I have attached at TAB A my assessment of the Navistar Dash ISS, Navistar MRAP Recovery Vehicle, and the FPI Cougar Ambulance. This assessment is based on operational and live fire testing conducted with production-representative vehicles designed to meet urgent operational needs. In my report I conclude the following:


The Navistar Dash ISS is operationally effective and suitable for use in Afghanistan. Live Fire Test and Evaluation (LFT&E) of the Dash is ongoing; once this testing and evaluation are complete, the results will be provided in a classified Live Fire vulnerability assessment. My preliminary assessment of the available LFT&E data indicates the Dash is survivable. The off-road mobility and maneuver capability of the Dash with ISS enabled units to be less predictable in their movement than would be possible without the ISS, continue operations under armor protection, and conduct mounted maneuver to approach and secure an objective.

The Navistar MRV is neither operationally effective nor suitable for recovery operations. The MRV does not possess the capability to traverse most cross-country terrain, rough trails, or steep hills with or without a vehicle in tow. This lack of mobility precludes its effectiveness for use in Afghanistan. The MRV can, however, perform combat tow and recover damaged MRAPs on flat improved roads and trails. LFT&E results indicate the MRV is survivable.

The FPI Cougar Ambulance is operationally effective and survivable. A unit equipped with the Ambulance can provide protected transport and emergency medical care for casualties in close proximity to enemy forces. In 2010, I assessed the FPI Cougar Category II A2 with ISS as survivable. Based on Live Fire testing, the integration of an ambulance kit did not affect the survivability of the vehicle. The FPI Cougar Ambulance provides sufficient all-terrain mobility for medical teams to support combat operations. However, the Ambulance is not operationally suitable due to its poor reliability, which contributed to its low availability and high need for maintenance.



The Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.



J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Adam Smith
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

MAR 22 2012

The Honorable C. W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

Dear Mr. Chairman:

In FY11, the MRAP program procured ISS kits to improve the off-road capability of the Navistar Dash, the Navistar MRAP Recovery Vehicle to fulfill an urgent need to recover damaged MRAP vehicles in Afghanistan, and ambulance kits to modify existing Force Protection Industries (FPI) Cougar Category II A2 ISS vehicles to satisfy Marine Corps casualty evacuation requirements.

I have attached at TAB A my assessment of the Navistar Dash ISS, Navistar MRAP Recovery Vehicle, and the FPI Cougar Ambulance. This assessment is based on operational and live fire testing conducted with production-representative vehicles designed to meet urgent operational needs. In my report I conclude the following:

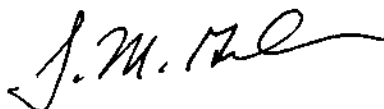
The Navistar Dash ISS is operationally effective and suitable for use in Afghanistan. Live Fire Test and Evaluation (LFT&E) of the Dash is ongoing; once this testing and evaluation are complete, the results will be provided in a classified Live Fire vulnerability assessment. My preliminary assessment of the available LFT&E data indicates the Dash is survivable. The off-road mobility and maneuver capability of the Dash with ISS enabled units to be less predictable in their movement than would be possible without the ISS, continue operations under armor protection, and conduct mounted maneuver to approach and secure an objective.

The Navistar MRV is neither operationally effective nor suitable for recovery operations. The MRV does not possess the capability to traverse most cross-country terrain, rough trails, or steep hills with or without a vehicle in tow. This lack of mobility precludes its effectiveness for use in Afghanistan. The MRV can, however, perform combat tow and recover damaged MRAPs on flat improved roads and trails. LFT&E results indicate the MRV is survivable.

The FPI Cougar Ambulance is operationally effective and survivable. A unit equipped with the Ambulance can provide protected transport and emergency medical care for casualties in close proximity to enemy forces. In 2010, I assessed the FPI Cougar Category II A2 with ISS as survivable. Based on Live Fire testing, the integration of an ambulance kit did not affect the survivability of the vehicle. The FPI Cougar Ambulance provides sufficient all-terrain mobility for medical teams to support combat operations. However, the Ambulance is not operationally suitable due to its poor reliability, which contributed to its low availability and high need for maintenance.



The Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.

A handwritten signature in black ink, appearing to read "J. M. Gilmore", with a stylized flourish at the end.

J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member



OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

MAR 22 2012

OPERATIONAL TEST
AND EVALUATION

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

Dear Mr. Chairman:

In FY11, the MRAP program procured ISS kits to improve the off-road capability of the Navistar Dash, the Navistar MRAP Recovery Vehicle to fulfill an urgent need to recover damaged MRAP vehicles in Afghanistan, and ambulance kits to modify existing Force Protection Industries (FPI) Cougar Category II A2 ISS vehicles to satisfy Marine Corps casualty evacuation requirements.

I have attached at TAB A my assessment of the Navistar Dash ISS, Navistar MRAP Recovery Vehicle, and the FPI Cougar Ambulance. This assessment is based on operational and live fire testing conducted with production-representative vehicles designed to meet urgent operational needs. In my report I conclude the following:

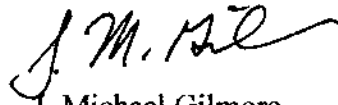
The Navistar Dash ISS is operationally effective and suitable for use in Afghanistan. Live Fire Test and Evaluation (LFT&E) of the Dash is ongoing; once this testing and evaluation are complete, the results will be provided in a classified Live Fire vulnerability assessment. My preliminary assessment of the available LFT&E data indicates the Dash is survivable. The off-road mobility and maneuver capability of the Dash with ISS enabled units to be less predictable in their movement than would be possible without the ISS, continue operations under armor protection, and conduct mounted maneuver to approach and secure an objective.

The Navistar MRV is neither operationally effective nor suitable for recovery operations. The MRV does not possess the capability to traverse most cross-country terrain, rough trails, or steep hills with or without a vehicle in tow. This lack of mobility precludes its effectiveness for use in Afghanistan. The MRV can, however, perform combat tow and recover damaged MRAPs on flat improved roads and trails. LFT&E results indicate the MRV is survivable.

The FPI Cougar Ambulance is operationally effective and survivable. A unit equipped with the Ambulance can provide protected transport and emergency medical care for casualties in close proximity to enemy forces. In 2010, I assessed the FPI Cougar Category II A2 with ISS as survivable. Based on Live Fire testing, the integration of an ambulance kit did not affect the survivability of the vehicle. The FPI Cougar Ambulance provides sufficient all-terrain mobility for medical teams to support combat operations. However, the Ambulance is not operationally suitable due to its poor reliability, which contributed to its low availability and high need for maintenance.



The Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.

A handwritten signature in black ink, appearing to read "J. M. Gilmore", written in a cursive style.

J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable John McCain
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

MAR 22 2012

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6025

Dear Mr. Chairman:

In FY11, the MRAP program procured ISS kits to improve the off-road capability of the Navistar Dash, the Navistar MRAP Recovery Vehicle to fulfill an urgent need to recover damaged MRAP vehicles in Afghanistan, and ambulance kits to modify existing Force Protection Industries (FPI) Cougar Category II A2 ISS vehicles to satisfy Marine Corps casualty evacuation requirements.

I have attached at TAB A my assessment of the Navistar Dash ISS, Navistar MRAP Recovery Vehicle, and the FPI Cougar Ambulance. This assessment is based on operational and live fire testing conducted with production-representative vehicles designed to meet urgent operational needs. In my report I conclude the following:

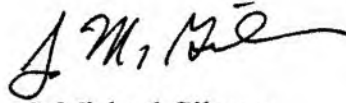
The Navistar Dash ISS is operationally effective and suitable for use in Afghanistan. Live Fire Test and Evaluation (LFT&E) of the Dash is ongoing; once this testing and evaluation are complete, the results will be provided in a classified Live Fire vulnerability assessment. My preliminary assessment of the available LFT&E data indicates the Dash is survivable. The off-road mobility and maneuver capability of the Dash with ISS enabled units to be less predictable in their movement than would be possible without the ISS, continue operations under armor protection, and conduct mounted maneuver to approach and secure an objective.

The Navistar MRV is neither operationally effective nor suitable for recovery operations. The MRV does not possess the capability to traverse most cross-country terrain, rough trails, or steep hills with or without a vehicle in tow. This lack of mobility precludes its effectiveness for use in Afghanistan. The MRV can, however, perform combat tow and recover damaged MRAPs on flat improved roads and trails. LFT&E results indicate the MRV is survivable.

The FPI Cougar Ambulance is operationally effective and survivable. A unit equipped with the Ambulance can provide protected transport and emergency medical care for casualties in close proximity to enemy forces. In 2010, I assessed the FPI Cougar Category II A2 with ISS as survivable. Based on Live Fire testing, the integration of an ambulance kit did not affect the survivability of the vehicle. The FPI Cougar Ambulance provides sufficient all-terrain mobility for medical teams to support combat operations. However, the Ambulance is not operationally suitable due to its poor reliability, which contributed to its low availability and high need for maintenance.



The Secretary of Defense may submit separate comments on this report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.

A handwritten signature in black ink, appearing to read "J. Michael Gilmore".

J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Thad Cochran
Ranking Member


Spider XM7 Network Command Munition

Combined Operational and Live Fire Test and Evaluation Report



February 2012

This report on the Spider XM7 Network Command Munition fulfills the provisions of Title 10, United States Code, Sections 2399 and 2366. It assesses the adequacy of testing and the operational effectiveness, operational suitability, and survivability of Spider.


J. Michael Gilmore
Director

The marginal cost of producing this report is estimated to be approximately \$37K. The estimated acquisition cost of the program with which this report deals is \$647M.



Spider XM7 Network Command Munition

Executive Summary

This document reports on the evaluation of test adequacy, operational effectiveness, operational suitability, and survivability of the Spider XM7 Network Command Munition. This report provides input for the Army's full-rate production decision review in 3QFY12. A classified annex accompanies this report providing additional details on Spider lethality.

System Overview

The Spider XM-7 Network Command Munition is an automated, anti-personnel munition system designed to provide a secure, "man-in-the-loop," remote command and control capability with a range of up to 1,500 meters. Spider allows the operator to monitor, control, fire or deactivate individual munitions or an entire munition field from a safe vantage point. Spider XM-7 has a self-destruct function that causes the munitions to detonate after a preset time and a command destruct function to engage the threat or eliminate residual hazards. The Spider XM-7 replaces conventional, non-self-destructing, anti-personnel landmines in accordance with 2004 National Landmine Policy. The Army is fielding the Spider system to deploying forces and to deployed units in combat theaters. In response to an approved Operational Needs Statement, the Army fielded 66 Spider systems to units supporting Operation Enduring Freedom between February and May 2009. The program achieved Initial Operational Capability in June 2011 with the fielding of Spider to the 4th Brigade Combat Team, 25th Infantry Division, Fort Richardson, Alaska.

Test Adequacy

The Army has conducted four post-Milestone C operational tests and a Live Fire Test and Evaluation (LFT&E) of the Spider XM-7 Network Command Munition. The Army conducted the Spider Initial Operational Test (IOT) at Fort Hood, Texas in March 2007; a Follow-on Operational Test 1 (FOT1) at Fort Bragg, North Carolina in March 2009; a Follow-on Operational Test 2 (FOT2) at Fort Leonard Wood, Missouri in May 2010; and a Limited User Test 2 (LUT2) in June 2011 at Fort Bliss, Texas. All testing was conducted in accordance with DOT&E-approved test plans and was adequate to support the test objectives.

The primary sources of data supporting this operational assessment are from the FOT2 in May 2010, the LUT2 in June 2011, and LFT&E in May 2005. During these test events, Engineer and Infantry units employed Spider munitions with upgraded production-representative hardware and software, incorporating lessons learned from previous testing. Additional data from previous operational and developmental testing, and relevant modeling and simulation are included.

Operational Effectiveness and Lethality

The Spider XM-7 Network Command Munition is operationally effective and lethal.

A properly trained unit can emplace and maintain a Spider munition field in order to contribute to protective obstacle effects – warn, mitigate, and prevent. In every FOT2 mission,

Spider demonstrated the capability to detect a threat, and in 94 percent of the missions, Spider demonstrated the ability to produce lethal effects.

Although Spider is not a standalone system, it can, when internal system communications are maintained, provide all doctrinal obstacle effects in some missions, including prevention of threat mission success. During FOT2, Spider was estimated to provide sufficient lethal effects to prevent threat success in 76 percent of threat intrusions against units protected by emplaced Spider munition fields. In the remaining 24 percent of threat intrusions, Spider provided either early warning or effects-mitigating threat activities.

Spider is a lethal system and can produce incapacitating injuries with both grenade and Claymore munitions. During FOT2, Spider munitions were estimated to incapacitate 53 percent of individual threat intruders entering Spider munition fields. Claymore munitions produced two-thirds of these incapacitations.

Operational Suitability

The Spider XM7 Network Command Munition is not operationally suitable. Units employing Spider have not achieved two of its key requirements: Munition Control Unit mission reliability and Munition Control Unit reuse. Only in narrowly focused, limited-scope operational testing of LUT2, have units demonstrated that Spider software and training enhancements have increased the likelihood of achieving Munition Control Unit reliability and reuse requirements. Units cannot efficiently follow the Army's "train as they fight" doctrine when training to employ a Spider munition field. Spider hardware and software will not permit units to train with inert grenades and inert Claymore mines in the same munition field controlled by one operator. The Spider program is developing software and hardware fixes to allow Soldiers to "train as they fight."

Spider is more complex than its predecessor system and necessitates extensive training to maintain proficiency. Effective training will depend on successful Unit Master Trainer (UMT) and Sustainment Training programs.

Extensive battery management requirements and increased unit transportation requirements create a logistics planning challenge for units employing Spider.

Units employing Spider will have a sustained manpower requirement. Spider munition fields require dedicated operators to employ, fight, maintain, and recover.

The Spider program office is developing system hardware and software improvements to mitigate the reliability, reuse, and training challenges and expects to demonstrate the improvements in an operational test in 1QFY13.

Survivability

The Spider XM7 Network Command Munition is survivable.

Although Spider Munition Control Units are vulnerable to the effects of direct small arms and crew served weapons engagements, unit tactics, techniques, and procedures can mitigate these effects.

Spider is temporarily ineffective in some Electronic Warfare and electromagnetic environments.

Recommendations


The Spider XM7 Network Command Munition is operationally effective, lethal, and survivable. It is not operationally suitable. The Spider program executed the operational and live fire testing in accordance with DOT&E-approved test plans. I recommend the Army consider the following recommendations:

Operational Effectiveness and Lethality

- In support of systems fielded to operational forces, develop in-theater capability to reprogram sterilized Munition Control Units and return them to the supply system.
- Review Spider system design with the goal of reducing the need for three different types of batteries.
- Develop Tactics, Techniques, and Procedures for the Remote Control Unit and Remote Control Unit Transceiver to use reliable commercial or military power sources in lieu of battery power whenever possible.
- Implement and validate the Unit Master Trainer and Sustainment Training programs and ensure that these programs are incorporated in the Army's training standards program.

Operational Suitability

- Implement and test the planned Spider software modifications to eliminate the possibility of Munition Control Unit sterilization during emplacement, field operations, and recovery of a Spider munition field.
- Pursue and test a Munition Adaptor Module trainer so units can "Train as they Fight."
- Continue the upgrading of Remote Control Unit and Munition Control Unit software to improve user interface.
- Develop and implement the capability for Munition Control Units to monitor and accurately report current battery status.
- Pursue solutions and update the Tactics, Techniques, and Procedures to implement Spider enhancements and non-lethal munitions.


J. Michael Gilmore
Director

This page intentionally left blank.

Contents

System Overview1

Test Adequacy11

Operational Effectiveness and Lethality15

Operational Suitability23

Survivability.....39

Recommendations41

Annex: Spider Live Fire Test and Evaluation..... Separate Cover

This page intentionally left blank.

Section One

System Overview

System Overview

The Spider XM-7 Network Command Munition is an automated, anti-personnel munition system designed to provide a secure, "man-in-the-loop," remote command and control capability with a range of up to 1,500 meters. Spider allows the operator to monitor, control, fire, or deactivate individual munitions or an entire munition field from a safe vantage point. Spider XM-7 has a self-destruct function that causes the munitions to detonate after a preset time and a command destruct function to engage the threat or eliminate residual hazards. The Spider XM-7 replaces conventional, non-self-destructing, anti-personnel landmines in accordance with 2004 National Landmine Policy. The Army is fielding the Spider system to deploying forces and to deployed units in combat theaters. In response to an approved Operational Needs Statement, the Army fielded 66 Spider systems to units supporting Operation Enduring Freedom between February and May 2009. The program achieved Initial Operational Capability in June 2011 with the fielding of Spider to the 4th Brigade Combat Team, 25th Infantry Division, Fort Richardson, Alaska. The Spider Full-Rate Production decision is scheduled for 3QFY13.

Background

Presidential Decision Directives and current landmine policy established a timeline to eliminate persistent U.S. landmines by December 2010. The Joint Staff approved the operational requirements for a non-persistent landmine alternative in December 2000. The requirements stated that a suitable alternative to persistent landmines must produce casualties equal to the M16A2 anti-personnel mine. In April 2006, the Joint Staff approved the Spider production requirements supporting the program's Milestone C.

Following Spider's Initial Operational Test in March – April 2007, the Army decided to field Spider as a "man-in-the-loop"-only system so that Spider could no longer engage targets autonomously. This decision led to an update of the production requirements, which was approved by the Joint Staff in May 2008. The update changed the casualty requirement from a comparison to M16A2 capability to a Spider-only requirement: "Given continuous communications and 20 meter munition spacing, Spider generates a minimum of 30 percent enemy losses in a 10 person formation advancing at 1.7 kilometers per hour."

Doctrinal Concept

The Maneuver Support Center of Excellence – Assured Mobility (MSCoE-AM), which is responsible for writing Spider doctrine, defines Spider as a contributor to the effects of reinforcing obstacles and not a standalone system. Figure 1-1 depicts the force protection and countermobility role of reinforcing obstacles. Units will primarily use Spider with protective obstacles.

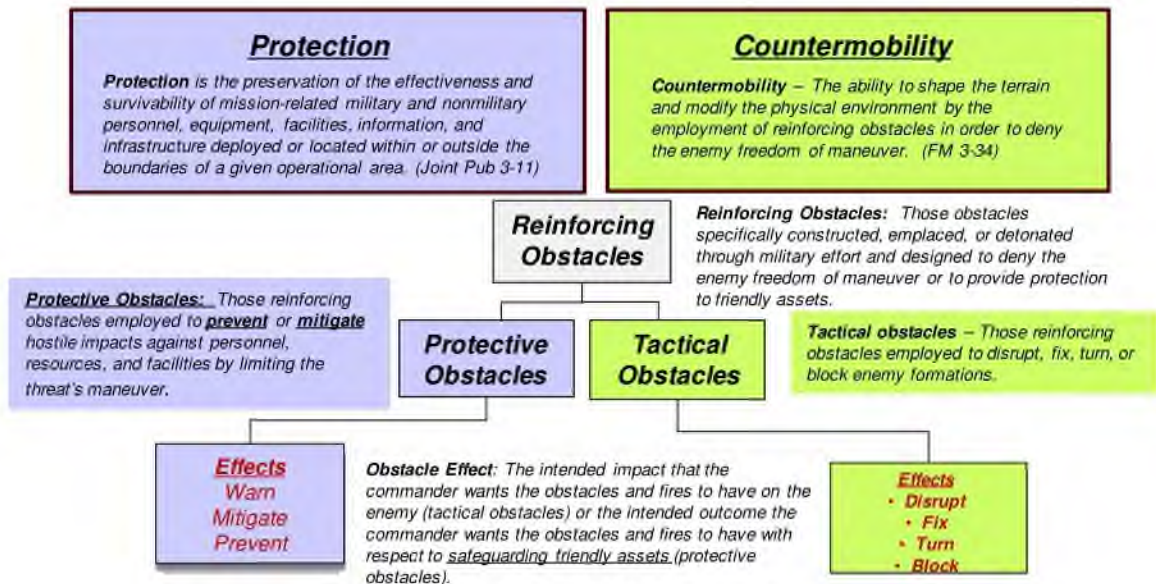


Figure 1-1. Reinforcing Obstacles

Soldiers use protective obstacles to warn of threat activity and to mitigate or prevent hostile actions against personnel, resources, and facilities by limiting the threat's ability to maneuver. Units augment protective obstacles with supporting fires to mitigate or prevent threat activity. Protective obstacles generally include:

- Overwatch and surveillance provided by unattended ground sensors, unmanned aerial vehicles, or direct observation of the obstacle. Soldiers use the Spider tripwires as unattended ground sensors to warn of threat activity.
- Direct and indirect fires such as individual weapons, crew served weapons, and mortar and artillery fires. Soldiers use the Spider grenades to engage threat forces to mitigate or prevent their activity.

System Description

The Spider XM-7 system has four major components: the Remote Control Unit, the Remote Control Unit Transceiver, a Repeater, and the Munition Control Unit. When employed, these components provide a munition field that allows the operator to detect intruding personnel, and then engage threat forces with lethal or non-lethal effects. Spider munition fields use "man-in-the-loop" control to comply with unit Rules of Engagement and avoid engaging non-combatants.

In 2008, the Army initiated the Spider Stand-off Capability Enhancement program to mitigate the close proximity of Soldiers to the munition field caused by "man-in-the-loop" control. The enhancement efforts add capability to the baseline Spider system in four areas: improved tactical and training software, greater command and control range, greater range capability for non-grenade munitions, and the addition of non-lethal grenade munitions. Figure 1-2 identifies Spider's baseline and Stand-off Capability Enhancement components, each of which is described below.

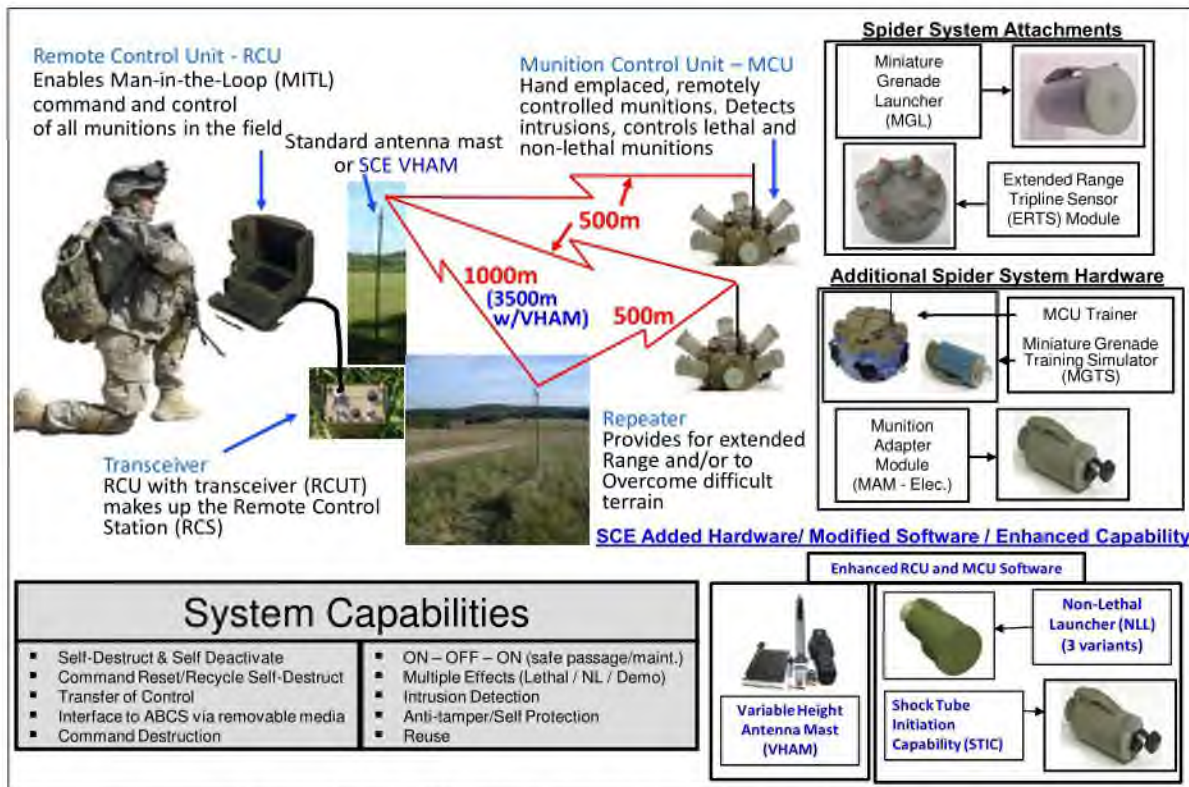


Figure 1-2. Spider Baseline and SCE System Components

Baseline Spider System

Remote Control Station

The Remote Control Station consists of the Remote Control Unit and the Remote Control Unit Transceiver. When the two are connected, they become the Remote Control Station. Each Spider system includes two Remote Control Stations and a short-range and long-range antenna.

The Remote Control Unit (see Figure 1-3) is a common, ruggedized, hand-held computer and is the command and control component of the Spider system. The Remote Control Unit is loaded with the Spider tactical software, Embedded Training software, and the Interactive Electronic Technical Manual.



Figure 1-3. Spider Remote Control Unit

The Remote Control Unit provides the Soldier-machine interface required to emplace, control, and recover a munition field. To control a munition field, the Remote Control Unit must be within 500 meters of the farthest Munition Control Unit in the field unless the Repeater is employed to extend this distance. The Remote Control Unit Transceiver is a high frequency man-pack radio that provides secure tactical communications between the Remote Control Unit, the Repeater, and the Munition Control Units.

Repeater

The Repeater is a standalone radio relay that extends the line-of-sight communication range between the Remote Control Station and Munition Control Units an additional 1,000 meters. The Repeater contains two radios for redundant communications.

Munition Control Unit (MCU)/MCU Trainer (MCUT)

The Munition Control Unit (see Figure 1-4) communicates with the Remote Control Station and provides the platform for attaching six lethal or non-lethal munitions. The Munition Control Unit contains operator control and safety electronics, an intrusion detection module, a battery tray for four internal non-rechargeable lithium batteries, and a short-range antenna. Munition Control Units alert the Remote Control Unit operator of intruders and tampering, and provide system status. The operator controls the munitions attached to the Munition Control Units to engage threat forces.

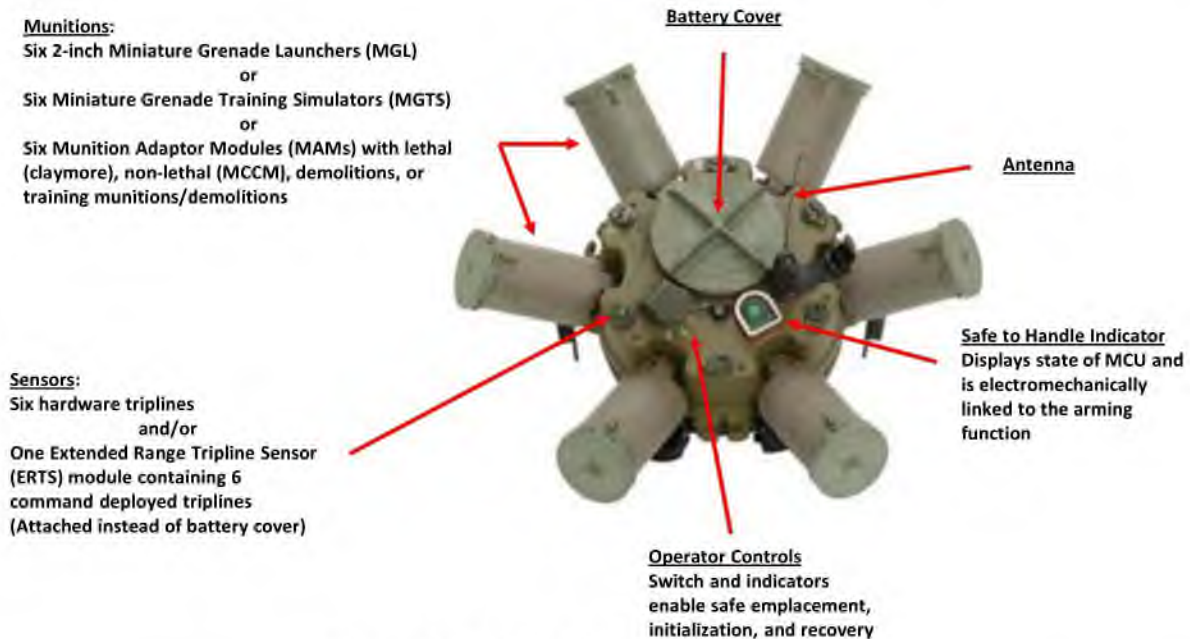


Figure 1-4. Spider Munition Control Unit

A Munition Control Unit has two tripline options used to transmit intruder alerts. Both types of triplines can be deployed together. Units can employ Munition Control Units with triplines and no munitions as a standalone sensor. The tripline options are:

- Six hardwire triplines manually attached to the Munition Control Unit during emplacement. Each tripline extends 10 meters from the Munition Control Unit.
- A single use Extended Range Tripline Sensor module attached to the top of the Munition Control Unit during emplacement. The module contains six remotely fired triplines that extend 10 to 12 meters from the Munition Control Unit.

A Munition Control Unit has six ports that can accommodate a Miniature Grenade Launcher, Munition Adapter Module, or an Inert Miniature Grenade Training Simulator (see Figure 1-5). Soldiers are not required to load all six ports before employment and are limited to using one type of attachment on a single Munition Control Unit.

- The Miniature Grenade Launcher is the primary lethal munition of the Spider system. Each launcher houses a 2-inch round anti-personnel grenade. When fired, the grenade travels 5 to 7 meters and detonates 2 meters in the air. The operator can fire an individual grenade or several in sequence, randomly, or all at once. Each grenade has a circular lethal coverage area of approximately 24 meters in diameter. One Munition Control Unit, with six Miniature Grenade Launchers attached, has a circular lethal coverage area of approximately 36 meters in diameter when all grenades are fired simultaneously.¹
- The Munition Adapter Module allows the use of other lethal and non-lethal munitions with the Spider Munition Control Unit. The Munition Adapter Module provides the interface for the Remote Control Unit operator to fire the lethal M18 Claymore, the non-lethal M5 Modular Crowd Control Munition, the Non-lethal Launcher payloads, and Modern Demolition Initiator initiated explosives. These devices are attached to the Munition Adapter Module through an M4 blasting cap that provides electric initiation of the munition and allows placement of munitions out to a distance of 100 feet from the Munition Control Unit. When detonated, a Claymore has a fan-shaped casualty-producing area defined by a 60-degree arc and a 100-meter radius.²
- An inert Miniature Grenade Training Simulator can be attached instead of Miniature Grenade Launchers during training or testing. The Miniature Grenade Training Simulator is similar to the Miniature Grenade Launcher in physical form, but instead of launching a grenade, the simulator has a ball indicator that flips from black to white to indicate that it has been fired. This indicator can be magnetically reset. The body of the Miniature Grenade Training Simulator is painted blue to identify it as a training device.

¹ The area in which a single Spider grenade can produce incapacitating injuries is 452 square meters. A Munition Control Unit with six grenades fired simultaneously can produce incapacitations over an area of 1,018 square meters.

² The area in which a single Claymore can produce incapacitating injuries is 5,236 square meters.



Figure 1-5. Munition Control Unit Attachments

The Munition Control Unit Trainer is used for training or testing. The trainer has the same size, weight, and functionality as the tactical Munition Control Unit. Both hardwire triplines and Extended Range Tripline Sensor modules can be used with the trainer. Soldiers can only attach Miniature Grenade Training Simulators to the trainer. Munition Adapter Modules that are used to control Claymore mines cannot be used with the trainer. This limits training and testing to fields with only simulated grenades. Munition Control Unit Trainers are painted blue to identify them as training devices.

Stand-off Capability Enhancements

The Army initiated the Spider Stand-off Capability Enhancement program to mitigate the close proximity of Soldiers to the munition field using the "man-in-the-loop" control method. These enhancements add capability to the baseline Spider system in four areas.

Remote Control Unit Tactical Software and Embedded Trainer Software

Software updates implemented during the Stand-off Capability Enhancement effort were made to support new hardware and capabilities. Additional software changes were made to simplify operator functions and improve the display of information, provide fixes for specific deficiencies identified during previous testing, improve system performance, and update embedded training software.

Variable Height Antenna Mast (VHAM)

The VHAM is an adjustable antenna mast that extends to 8 meters. Soldiers attaching the Spider long-range antenna to the VHAM can increase the distance from the Remote Control Station to an emplaced field up to 4,000 meters. The VHAM is designed to operate in the same environments as the current Spider antenna system. The new adjustable antenna mast is not an

issued component of the Spider system. Units must purchase the VHAM through the supply system. The Army introduced and tested the VHAM enhancement in Follow-on Operational Test 2 (FOT2).

Shock Tube Initiation Capability

The Shock Tube Initiation Capability allows for non-electrical triggering of lethal and non-lethal munitions. Shock Tube is a non-electric explosive initiator in the form of flexible, small-diameter hollow plastic tubing. Shock Tubes provide the non-electrical connection between the Munition Adaptor Module attached to the Munition Control Unit and the lethal or non-lethal munition. When electrically fired by the Munition Adaptor Module, a non-electrical percussive wave traveling the length of the Shock Tube triggers an M4 Blasting Cap attached to the lethal or non-lethal munition. It is less sensitive to static electricity and radio frequency energy that can cause premature initiation when using legacy hardwire electrical connections with lethal or non-lethal munitions. Using Shock Tubes, Soldiers can emplace munitions such as the Claymore mine or demolition charges up to 1,000 feet from the Munition Control Unit. Legacy hardwire connections limited the extended emplacement range to 100 feet. Any device that is initiated with an M4 blasting cap can be triggered with a Shock Tube. No additional hardware is required because the Shock Tube is fired using the existing Munition Adapter Module. The Army introduced and tested the Shock Tube Initiation Capability enhancement in operational testing in 2010.

Non-Lethal Launcher Grenades

The Army is developing two non-lethal grenades variants: the Flash-Bang Grenade and the Sting Ball Grenade. Both variants can be attached to a single Munition Control Unit using standard emplacement procedures. Soldiers cannot mix lethal and non-lethal munitions on the same Munition Control Unit. Non-lethal grenades cannot be installed on the Munition Control Unit trainer. Soldiers can fire an individual non-lethal grenade or several in sequence, randomly, or all at once. When launched, the non-lethal grenade travels 5 meters along its tripline axis and detonates less than 2 seconds after launch. Both non-lethal grenades have a bursting radius of 5 meters. The Army plans to update Munition Control Unit software to enable tactical employment of non-lethal grenades after completing non-lethal grenade developmental testing.

Full System Characteristics

A complete Spider system is listed in Table 1-1 organized by component supply classification. The Army divides supplies into 10 Classes of Supply. Class VII items are issued directly to the unit and are maintained and stored within the unit. Class V items are maintained at the unit's supporting Ammunition Supply Point (ASP) and must be drawn to support unit training or tactical operations.

Table 1-1. Spider System Component List

Class of Supply	Item	Issued to Unit	Combat Load	Additional Stockage
VII	RCS – Remote Control Stations (Remote Control Unit and Transceiver)	2	-	-
VII	RCS Accessory Kit	1	-	-
VII	Repeater	1	-	-
VII	MCUT – Munition Control Unit Trainer	4	-	-
VII	MGTS – Grenade Training Simulator	24	-	-
VII	MAM – Munition Adapter Module	24	-	-
V	MGL – Grenade	-	60	192
V	ERTS – Tripline Module	-	20	60
V	MCU – Munition Control Unit	-	10	32

Spider components are transported to a deployment location in one of three container types (see Figure 1-6). Each container is rigid, reusable, and transportable throughout the Army's logistics system without the use of specialized equipment.



Figure 1-6. Spider System Containers

Remote Control Stations, Repeaters, and Accessory Kits are packaged in a container weighing approximately 50 pounds. Munition Control Units and Munition Control Unit Trainers are packaged two each in a 7.5-gallon pail weighing 31 pounds. Miniature Grenade Launchers, Munition Adapter Modules, and Miniature Grenade Training Simulators are packaged 12 per M548 ammunition containers weighing between 29 and 37 pounds. Extended Range Tripline Sensors are packaged 20 per container, weighing approximately 26 pounds.

A complete baseline Spider system (including additional stockage MCUs and materiel) weighs over 1,900 pounds and requires approximately 83 cubic feet of space to store and transport. Including the VHAM as part of the system adds an additional 85 pounds and nearly 12 cubic feet of volume. Since Class VII Spider components are stored with the unit and both Class VII and Class V components are transported in organic unit assets, the weight and size of a Spider system have implications for unit storage and transportation.

Operational Concept

Spider detects and warns friendly forces of obstacle activity and, if commanded by Soldiers, delivers lethal effects to mitigate or prevent threat activity.

Spider system hardware and software provide flexibility in the configuration of a Spider munition field. Units may employ Spider in standard or non-standard configurations using lethal, nonlethal, or a mix of lethal and nonlethal munitions. As shown in Figure 1-7, a standard configuration Hasty Protective field employing only Spider grenades on 10 Munition Control Units is rectangular in shape with 110 meters width and 45 meters depth.

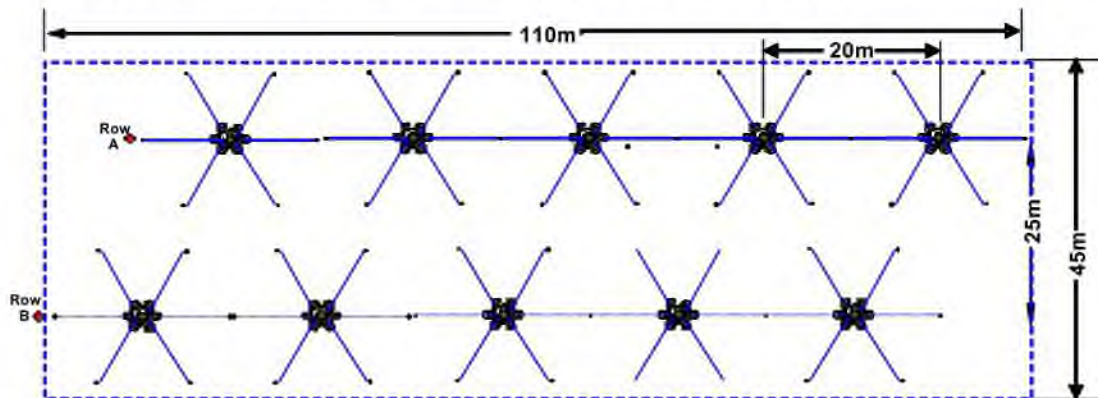


Figure 1-7. Schematic of a Typical Hasty Protective Spider Munition Field

Soldiers consider METT-T when emplacing Spider munition fields.³ Field setup begins with Soldiers positioning individual Munition Control Units per the field configuration then attaching grenades or Claymore mines and triplines. This is followed by electronic setup of each Munition Control Unit.

For Munition Control Unit electronic setup, the operator must take the Remote Control Unit and Transceiver to each Munition Control Unit. This establishes communications and completes coordination of location, configuration, and communications protocol information between the two devices. If the field includes Claymore mines, the operator must physically move to each Claymore mine in order to enter the exact location into the Remote Control Unit field database. The operator then powers on the Munition Control Unit, activating the triplines and anti-tamper features, and proceeds to the next Munition Control Unit in the field and repeats the process.

After Munition Control Unit electronic setup, the operator moves to where he will control the field, installing a repeater along the way for extended range if necessary. The final step of field emplacement is networking the Remote Control Unit to Munition Control Unit communications link.

³ METT-T = Mission, Enemy, Terrain, Troops, and Time. These are the factors on which military commander's plan and execute operational missions.

For field configurations where the operator is not able to physically observe the field, a separate observer must be employed with a direct communications link between the observer and the Remote Control Unit operator. Figure 1-8 shows the typical communications configuration when using a separate munition field observer.

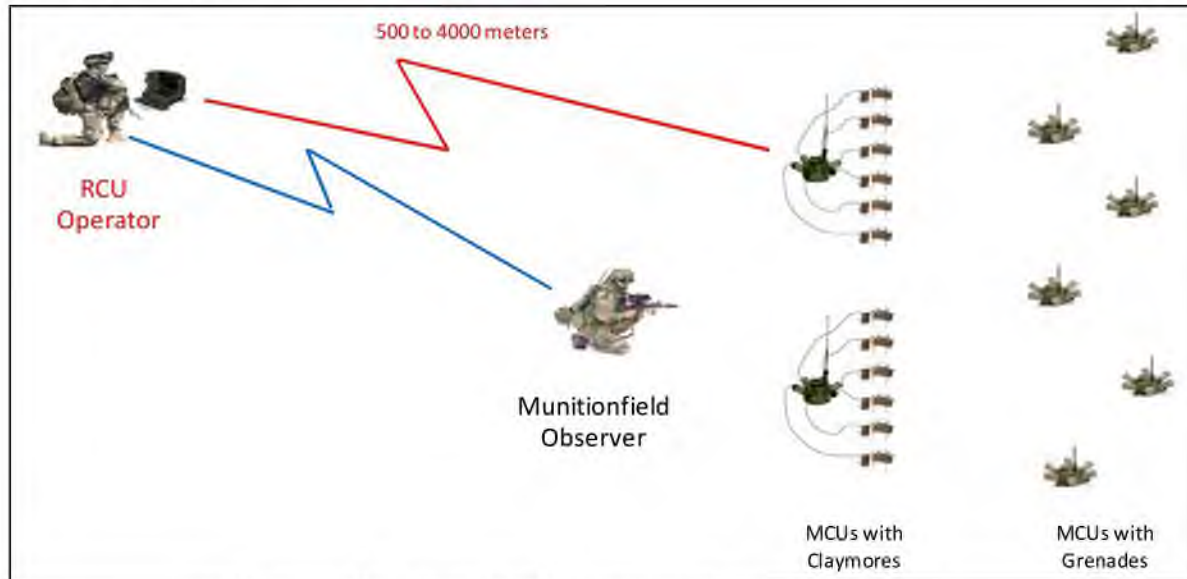


Figure 1-8. Tactical Field Communications Configuration

When the field has been networked and, if required, communications established with a dedicated observer, the unit will “fight” the field using approved Operations Plans/Orders; Tactics, Techniques and Procedures; and Rules of Engagement. As a “man-in-the-loop” system, operators will use Spider to engage an intruder after positive identification of the intruder has been made by a munition field observer. If a decision is made to engage an intruder, the Remote Control Unit operator sends a fire command to one or more Munition Control Units. Timely execution of this chain of events is critical as the intruders move through the obstacle.

Section Two

Test Adequacy

Test Adequacy

The Army has conducted four post-Milestone C operational tests and a Live Fire Test and Evaluation (LFT&E) of the Spider XM-7 Network Command Munition as shown in Table 2-1. All testing was conducted in accordance with DOT&E-approved test plans and was adequate to support the test objectives.

Following Spider's Initial Operational Test (IOT) in March – April 2007, the Army chose to eliminate the autonomous engagement capability of the system and field Spider as a "man-in-the-loop" system. During the Follow-on Operational Test One (FOT1), conducted at Fort Bragg, North Carolina, in February – March 2009, the test unit employed Spider as a "man-in-the-loop" system providing protective and hasty protective munition fields.

The primary sources of data supporting this operational assessment are from the Follow-on Operational Test 2 (FOT2) in May 2010, the Limited User Test 2 (LUT2) in June 2011, and LFT&E in May 2005. Additional data from previous operational and developmental testing, and relevant modeling and simulation are also included.

Table 2-1. Spider Post-Milestone C Testing

Date	Test	Location
May 2005	Live Fire Test and Evaluation (LFT&E)	ATK Proving Grounds, Elk River, Minnesota
March 2007	Initial Operational Test (IOT)	Fort Hood, Texas
March 2009	Follow-on Operational Test 1 (FOT1)	Fort Bragg, North Carolina
May 2010	Follow-on Operational Test 2 (FOT2)	Fort Leonard Wood, Missouri
June 2011	Limited User Test 2 (LUT2)	Fort Bliss, Texas

Follow-on Operational Test Two (FOT2)

The U.S. Army Operational Test Command (OTC) conducted the FOT2 Record Test May 18-26, 2010, at Fort Leonard Wood, Missouri. Pre-test activities included five days of new equipment training, five days of doctrine and tactics training (DTT), five days of sustainment training, a two-day synchronization event, and a two-day pilot test.

The test unit for FOT2 was an engineer company with four platoons. The test company executed 16 missions over varied terrain in ambient weather conditions with both day and night operations:

- Eight company-sized Combat Outpost (COP) missions providing perimeter security for an outlying operations center. The purpose of the COP defensive mission was to prevent threat forces from entering the perimeter or conducting operations against the outpost that would inflict friendly casualties or damage facilities or materiel.
- Four Presence Patrol (PP) missions during which platoon-sized units conducted operations to defeat threat activities and demonstrate friendly force resolve and commitment.

- Four Area Security (AS) missions during which platoon-sized units operated to deny terrain to threat forces that were either conducting mortar missions against the COP or emplacing improvised explosive devices along routes used by friendly forces.

Two squads of engineer Soldiers with non-commissioned officer leadership represented threat personnel and conducted operations against units protected by emplaced Spider munition fields. The threat personnel conducted operations as uniformed military personnel, insurgents, and civilian non-combatants.

Limited User Test Two (LUT2) and NIE Brigade Capstone Exercise

Army OTC conducted the LUT2 record test June 14-23, 2011, as part of the Network Integration Evaluation (NIE) at Fort Bliss, Texas. The purpose of this test was to assess post-FOT2 improvements in system suitability with respect to Munition Control Unit reliability and the reuse requirements. Pre-test activities were similar to previous operational testing with the exception that sustainment training included a two-day synchronization event followed by the two-day pilot test. The Maneuver Support Center of Excellence – Assured Mobility (MSCoE-AM) held a separate one-hour refresher training class the day prior to the start of the record test.

The test unit for the LUT2 was an engineer company command section with one engineer platoon and one infantry platoon. During the LUT2, the company executed eight missions over high desert terrain in ambient weather conditions in both day and night operations.

Two types of missions were executed during the LUT2: Combat Outpost Security/Defense and Area Security Operations. The eight missions conducted by the test unit included mission planning, emplacement, operation, and recovery of a single Spider munition field. Threat forces conducted one or two missions against each Spider munition field.

One squad of Soldiers under the control of a non-commissioned officer represented threat personnel and conducted operations against units protected by emplaced Spider munition fields. Threat personnel conducted operations as uniformed military personnel, insurgents, and civilian non-combatants. The threat forces employed smoke grenades, small arms blank ammunition, and night vision devices in both day and night operations.

The final event of the NIE was a Brigade Capstone Exercise conducted July 9-12, 2011. Both Spider-trained platoons participated in this exercise. The infantry platoon participated as part of its parent battalion, 1-6 Infantry, while the engineer platoon was task organized to support the operations of 1-35 Armor. Spider activities during the Capstone Exercise were at the discretion of the supported battalions. These activities were not a part of the formal LUT2 test plan but were observed as representative of Spider employment in an operational environment.

During the Capstone Exercise, 1-35 Armor employed Spider in two Forward Operating Base defense missions, while 1-6 Infantry did not employ Spider.

Live Fire Testing and Evaluation (LFT&E)

The Army Research Lab conducted the Spider LFT&E at the Alliant Techsystems Proving Ground in Elk River, Minnesota, in May 2005 to assess the lethality of Spider's high explosive fragmentation grenade against personnel targets. Government personnel from the

Army Research Laboratory supervised testing of the production-representative munitions and collected data necessary to evaluate Spider lethality. Static and dynamic arena tests were used to characterize the warhead. Static arena tests characterized warhead fragmentation following static detonation of a grenade, while dynamic arena tests captured similar data following launch of the grenade from the Munition Control Unit. Spider munition field dynamic firings were conducted against plywood mannequins in various postures and orientations (see Figure 2-1). Army Research Laboratory analysts used data collected during the testing to populate incapacitation models for estimating Spider lethality.



Figure 2-1. Example of Mannequin Positions During Spider Live Fire Testing

This page intentionally left blank.

Section Three

Operational Effectiveness and Lethality

Operational Effectiveness and Lethality

The Spider XM-7 Network Command Munition is operationally effective and lethal.

Spider is not persistent and does not allow autonomous engagements, features of previous anti-personnel munitions that violate current National Landmine Policy. Spider provides remote firing of munitions from up to 4 kilometers, collection of situational awareness information, and support of friendly maneuver.

A properly trained unit can emplace and maintain a Spider munition field in order to contribute to protective obstacle effects – warn, mitigate, and prevent. In every FOT2 mission, Spider demonstrated the capability to detect a threat, and in 94 percent of the missions, Spider demonstrated the ability to produce lethal effects.

Although Spider is not a standalone system, it can, when internal system communications are maintained, provide all doctrinal obstacle effects in some missions, including prevention of threat mission success. During FOT2, Spider was estimated to provide sufficient lethal effects to prevent threat success in 76 percent of threat intrusions against units protected by emplaced Spider munition fields. In the remaining 24 percent of threat intrusions, Spider provided either early warning or effects-mitigating threat activities.

When internal system communications between the Remote Control Units and Munition Control Units are lost due to hardware failure, electronic warfare activity, or any other reason, Spider cannot process trip alert and fire command messages and cannot directly contribute to achieving obstacle effects.

Spider is a lethal system and can produce incapacitating injuries with both grenade and Claymore munitions. During FOT2, Spider munitions were estimated to incapacitate 53 percent of individual threat intruders entering Spider munition fields. Claymore munitions produced two-thirds of these incapacitations.

New Capabilities

The Army developed Spider as a replacement for legacy hand-emplaced, target-activated antipersonnel landmines, specifically the M14 and M16 landmines (see Figure 3-1).

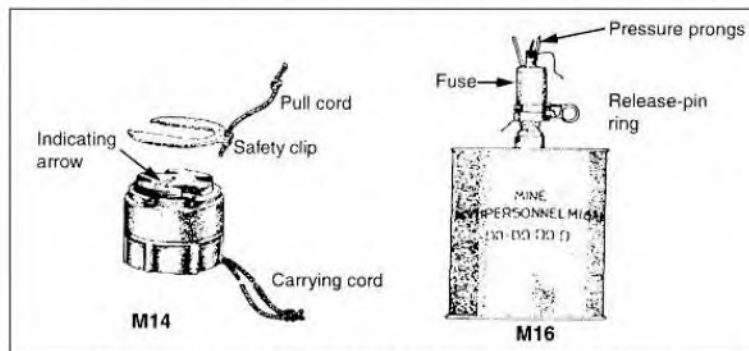


Figure 3-1. M14 and M16 Legacy Land Mines

Key characteristics of these mines, including persistence and autonomous operation violate National Landmine Policy. These mines do not have a self-destruct capability. Once emplaced and armed, they remain capable of detonating indefinitely. This creates lethal hazards after hostilities end, if the mines are not recovered.

Spider is consistent with National Land Mine Policy because it provides a system featuring:

- Non-persistent munitions with timed and command-activated self-destruct capability
- Positive "man-in-the-loop" control of both lethal and non-lethal munitions

The Spider system provides capabilities not available with previous antipersonnel landmines. These include:

- Remote electrical and non-electrical (using Shock Tube initiators) firing capabilities for munitions and demolitions to a range of 4 kilometers
- Capability to fire single munitions or to fire multiple munitions simultaneously
- Capability to collect situational awareness information through tripline activation and electronic notification of the Remote Control Unit operator
- Capability to safe all or part of a munition field to support friendly maneuver and maintain and rearm all or part of a munition field

Because Spider is a "man-in-the-loop" system, units must have accurate, real-time situational awareness to employ Spider. Direct observation of threat activity by munition field observers provides this situational awareness. During periods of reduced visibility or when an obstacle is emplaced in terrain where direct observation of the field is limited, units rely on the Spider tripwire sensors to detect threat activity.

Operational Effectiveness

When Soldiers employ an obstacle in support of their unit's mission, the unit commander will specify the location of the obstacle, the time the obstacle must be in place and ready to support, and an expected duration of the obstacle's employment. Soldiers must emplace the Spider field by the designated time and, once in place, operate the field to contribute to the commander's intent for the protective obstacle.

Emplacement

Units must plan how long it takes to emplace fields of varying size under a variety of operational and environmental conditions in order to ensure munition field availability in the designated time. In FOT2, units emplaced Spider fields during day and night operations in varied terrain to support three mission types: Combat Outpost, Presence Patrols, and Area Security. Mission orders were issued to the unit in advance of the desired field emplacement time to allow operationally sufficient time for the planning, preparation, and execution of the emplacement.

There is no time standard for field emplacement. The average emplacement time for FOT2 missions was 2 hours and 47 minutes. This represents a significant improvement from the 3 hours and 45 minute average demonstrated by the test unit during the 2009 FOT1. Emplacement activities during FOT2 supported the commander's intent in employing a protective obstacle. During the test, units emplaced 14 of 14 fields no later than the commander's desired start time (compared to the FOT1 test unit that emplaced 11 of 19 fields on time). Units in the LUT2 averaged 2 hours for field emplacements with 7 of 8 fields in place on time.

Availability

A Spider field must have continuous communication between the Remote Control Unit and the Munition Control Units in order to provide obstacle effects. For tactical operations when the Remote Control Unit operator is controlling the field from a distance of up to 4,000 meters, the operator and observer(s) overwatching the field must have continuous communications. Figure 3-2 provides an overview of these two required communications links.

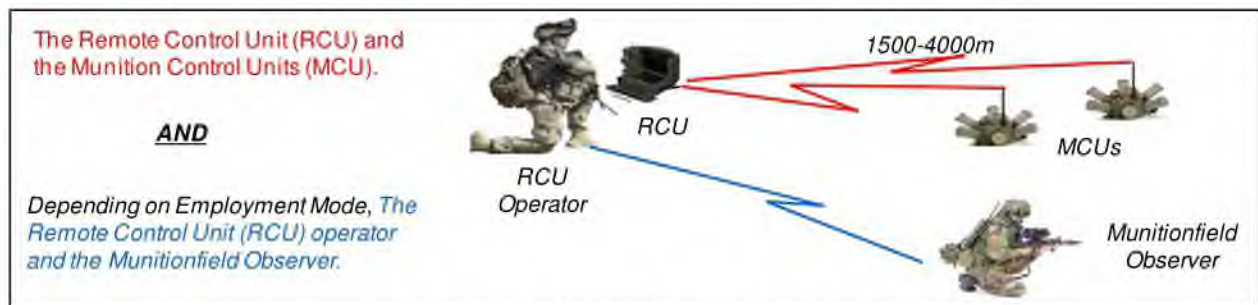


Figure 3-2. Spider Communications

Observers overwatching a munition field indirectly support Spider's contribution to obstacle effects by detecting and reporting threat activity. Spider cannot contribute lethal effects to the obstacle if the communications link between the Remote Control Unit and Munition Control Units is not active. When communications are lost, the Remote Control Unit operator cannot receive Spider trip alerts or send fire command messages regardless of whether the observer confirms threat intruders are in the munition field. The system cannot autonomously engage threat intruders. The system does not automatically notify the operator when the communication link between the two components is down. System operators must periodically query the Munition Control Units to verify active communications. Not contributing to obstacle effects during periods of lost communications is a consequence of the "man-in-the-loop" capability of the Spider system.

The loss of communication between the Remote Control Unit and Munition Control Units can be caused by hardware failures, incorrect Soldier actions, and threat jamming. Remote Control Unit to Munition Control Units communications availability during FOT2 was 99.7 percent, a significant improvement over the 92.0 percent demonstrated during FOT1. This increase was due to improvements in Spider hardware reliability. In the LUT2, overall Remote Control Unit to Munition Control Units communications availability was above 95 percent throughout the test.

Remote Control Unit operators controlling the Spider system and observers overwatching the munition field communicate using their assigned unit radios and equipment. Availability of this communications link during FOT2 was 100 percent, compared to 99.6 percent during FOT1.

FOT2 and LUT2 test results indicate units that employ the Spider system can, in the absence of threat jamming activity, achieve a high level of Spider availability to support obstacle effects.

Spider as a Contributor to Obstacle Effects

The Army does not intend to employ Spider as a standalone system. It is employed as an element of combined arms obstacle. Units use Spider with other components such as Concertina wire, picket fencing, and HESCO barriers to build complex protective obstacles. As a contributor to obstacle effects, Spider must:

- Demonstrate the capability to detect threat presence/activity, or
- Demonstrate the capability to deliver lethal effects sufficient to mitigate or prevent threat success.⁴

Detections occur when tripline alerts are electronically sent to the Remote Control Unit operator or visually sent by the observer overwatching the munition field. Visual detection is necessary when Soldiers emplace Munition Control Units without triplines.⁵

The test unit detected all threat intrusions (16 of 16 fields) in the FOT2 and demonstrated the ability to produce lethal effects with Spider in 94 percent of the missions (15 of 16 fields). Both of these results are consistent with test results from the 2009 FOT1 where Spider fields detected all threat intrusions (12 of 12 fields) and provided lethal effects to at least one intruder 92 percent of the time (11 of 12 fields). The data show that with 80 percent confidence we can expect that Spider will meet the user's desire to contribute to obstacle effects at least 70 percent of the time for Presence Patrol and Area Security type missions and 83 percent of the time for Combat Observation Post missions.

Table 3-1 below summarizes Spider's contributions to obstacle effects in the 16 FOT2 missions.

⁴ These requirements are based on Army refinement of the operational concept for the employment of Spider as discussed in the System Overview section of this report. The requirements are not formalized in an approved Spider requirements document. Spider's formally approved requirement pertaining to effectiveness is the Combat Casualty Key Performance Parameter discussed later in this section.

⁵ Details of the efficiency and reliability of triplines, both hardwire and ERTS, are not available during operational testing. Instrumentation is not available to identify with certainty when a tripline has been tripped and the Remote Control Unit operator should receive an electronic alert. Tripline reliability data were collected during developmental test events and are discussed in the Suitability section of this report.

Table 3-1. Spider Contribution to Obstacle Effects by Mission Type

Mission Type	Proportion of Missions where Spider Contributed to Obstacle Effects			Overall Proportion of Missions where Spider Contributed to Obstacle Effects	80% Confidence that Proportion is Greater Than:
	By Detecting the Threat	By Demonstrating Lethality			
		To Mitigate Threat Mission Success	To Prevent Threat Mission Success		
COP	100% (8/8)	100% (8/8)	63% (5/8)	100% (8/8)	83%
Presence Patrol	100% (4/4)	75% (3/4)	75% (3/4)	100% (4/4)	70%
Area Security	100% (4/4)	100% (4/4)	75% (3/4)	100% (4/4)	70%
Overall	100% (16/16)	94% (15/16)	69% (11/16)	100% (16/16)	90%

Lethality

The primary lethal mechanism of the Spider system is a 2-inch spherical anti-personnel grenade launched from a Miniature Grenade Launcher. The grenade's fuse is preset to provide time of flight initiation of the grenade at a range of approximately 6 meters from the launcher and a height of burst of approximately 2 meters. The grenade is a serrated steel shell filled with an insensitive munition explosive, creating high velocity fragments to cause personnel incapacitation over the grenade's lethal footprint.⁶

The Spider requirements document contains no explicit lethality requirement for the individual grenade. Grenade lethality must support the requirement for the system to produce combatant casualties. Army Research Laboratory analysts used warhead characterization test data as input to lethality estimation models to create Probability of Incapacitation (P_I) curves used in effectiveness modeling.

The Spider system can also initiate the firing of the M18 Claymore mines. Claymores are anti-personnel fragmentation munitions used by the Army and Marine Corps for over four decades. When detonated, a Claymore projects a fan-shaped pattern of steel balls in a 60-degree arc, at a maximum height of 2 meters, and covers a casualty radius of 100 meters. The forward danger radius for friendly forces is 250 meters. When used with Spider, Claymores are detonated with electrical or non-electrical firing wire when triggered by the Remote Control Unit operator. Like the grenades, Claymores support the requirement for Spider to produce combatant casualties.

⁶ During warhead characterization testing, the average warhead fragment weight was 1.5 grains, and the average fragment velocity was 5,851 feet per second. Less than 5 percent of the fragments had a weight greater than 3 grains. By comparison, a standard copper-coated steel BB weighs about 5.3 grains (approximately one-third of a gram).

In addition to lethal munitions, Spider can also fire the non-lethal Modular Crowd Control Munition (MCCM), which was incorporated in operational testing. The Army is developing additional non-lethal sting-ball and flash bang grenades for future use with Spider.

Combat Casualty Key Performance Parameter

When the Army decided to field Spider as a "man-in-the-loop" system in May 2008, the Joint Requirements Oversight Council approved modification of the previous combat casualty Key Performance Parameter:

- Threshold. Given uninterrupted communications and 20-meter munition spacing, Spider generates a minimum of 30 percent enemy losses in a 10-person formation advancing at 1.7 kilometers per hour.
- Objective. Regardless of communications status, and given 20-meter munition spacing, Spider generates a minimum of 30 percent enemy losses in a 120-person formation advancing at 5.0 kilometers per hour.

This key requirement is not stated in operationally realistic terms and the successful achievement of this requirement does not necessarily indicate the effectiveness of the Spider system in an operational environment.

The two primary factors that define the non-operational nature of this Key Performance Parameter (KPP) are:

1. The assumption of continuous communications, and
2. The expectation that a threat force, including a force conducting a deliberate reconnaissance mission, would attempt to breach a field in a specific formation and at a constant speed.

Combat Casualty KPP Modeling and Simulation (M&S) Results

The Army directed the Army Materiel Systems Analysis Activity (AMSAA) to conduct a study and determine if units employing the Spider could achieve the combat casualty requirements. The modeling and simulation study was necessary because, as written and approved, the requirements are not operationally realistic or testable. AMSAA used the Combined Arms and Support Task Force Evaluation Model (CASTFOREM) to determine Spider lethality.⁷ AMSAA published (and DOT&E reviewed) the results of this study in a classified briefing in April 2009.

The study concluded the Spider system could achieve at least 30 percent casualties in both the threshold (10-person formation advancing at 1.7 kilometers per hour) and objective (120-person formation advancing at 5.0 kilometers per hour) requirements. The AMSAA study addressed combat casualties in modeling and simulation and did not address the effectiveness of the Spider system in an operational environment.

⁷ CASTFOREM is the Army's standard brigade and below combined arms effects model with resolution down to individual vehicles, weapon systems, sensors, and Soldiers.

Spider Lethality in an Operational Environment

Spider lethality in an operational environment was assessed during the FOT2. The ATEC Player and Event Tracking System (TAPETS) real-time casualty assessment system provided incapacitation data. Table 3-2 presents a summary of combat casualties (incapacitations) produced during FOT2 solely by the Spider system using only its lethal grenade and M18 Claymore munitions.

Spider produced greater than 30 percent casualties in 94 percent (15 of 16) of FOT2 missions and 76 percent (26 of 34) of individual threat intrusions. With respect to casualties produced across all missions and all intrusions, Spider produced 53 percent casualties (82 of 155), well above the minimum requirement of 30 percent.

Table 3-2. Summary of Combat Casualties and Munitions

Mission Type	% of Missions with ≥ 30% Casualties*	% of Intrusions with ≥ 30% Casualties*	% of Casualties across Mission Type	Number of MGLs fired by Mission Type	Number of Casualties from MGLs by Mission Type	Number of M18 fired by Mission Type	Number of Casualties from M18s by Mission Type
COP	100% (8/8)	76% (16/21)	54% (48/89)	243	26 (.11)**	75	22 (.29)**
Presence Patrol	75% (3/4)	67% (6/9)	38% (19/50)	105	2 (.02)**	43	17 (.40)**
Area Security	100% (4/4)	100% (4/4)	94% (15/16)	Not Used	N/A	60	15 (.25)**
Overall	94% (15/16)	76% (26/34)	53% (82/155)	348	28 (.08)**	178	54 (.30)**

* 30% is the casualty requirement in the Combat Casualty KPP

** Numbers in parentheses are casualties per munition fired.

The table indicates that units using Spider rely more on the M18 Claymore mine to produce casualties than the Spider grenades. The table indicates the number of threat casualties varies by mission type.

Casualties by Mission Type

During FOT2, the test unit employed Spider to support protective obstacles in three different missions. Each mission had a different operational environment resulting in different threat casualty levels.

- In Combat Outpost missions, Spider was employed in defense of a fixed installation that friendly forces intended to occupy for an extended period of time. Fields were large and predominantly in open terrain with clear fields of observation and fire and well defined rules of engagement. Intruders entering the obstacle were fully exposed

to direct observation and engagement. These conditions were ideal for a successful defense of the Combat Outpost and resulted in 54 percent threat casualties across eight missions.

- In Presence Patrol missions, Spider was employed as a hasty protective obstacle to deny threat force access to a temporary, small, and generally unimproved friendly position. These fields were generally emplaced in mixed terrain with limited observation and fields of fire. Threat forces approaching, and in some cases within, these fields could take advantage of natural cover and concealment, making the engagement process more difficult for the friendly force. Despite these conditions being the most difficult for demonstrating Spider lethality, the friendly force inflicted 38 percent threat casualties across four missions.
- In Area Security missions, Spider was employed using only Claymore mines in small fields specifically designed to deny threat forces the limited terrain. The test unit concealed the Munition Control Units and Claymore mines, then simultaneously fired all the Claymore mines when the intruders encountered the obstacle. This mission profile was designed specifically for inflicting maximum casualties on the threat force and resulted in 94 percent threat casualties across four missions.

Casualties by Munition Type

Of the 67 simulated casualties produced in Combat Outpost and Presence Patrol missions in which both Spider grenades and Claymores were used, 42 percent (28 of 67) were produced by grenades and 58 percent (39 of 67) were produced by Claymores.

For all FOT2 missions, including the Area Security missions in which only Claymores were used, each grenade fired produced 8 percent casualties and each Claymore fired produced 30 percent casualties.

When employed by Spider, Claymores are more effective and more efficient at producing casualties than Spider grenades.

Spider Combat Employment

Data provided by the Army and reviewed by DOT&E indicate units deployed in the Afghanistan Theater of Operations are integrating Spider munitions into Combat Observation Post force protection plans. The Army reports four Brigade Combat Teams are employing Spider with 28 field munitions in place. Units have successfully mitigated or prevented threat activity using judicious placement of Munition Control Units in small munition fields positioned to defend against known insurgent engagement areas.

Section Four

Operational Suitability

Operational Suitability

The Spider XM7 Network Command Munition is not operationally suitable. Units employing Spider have not achieved two of its key requirements: Munition Control Unit mission reliability and Munition Control Unit reuse. Only in narrowly focused, limited-scope operational testing of LUT2, have units demonstrated that Spider software and training enhancements have increased the likelihood of achieving Munition Control Unit reliability and reuse requirements. Units cannot "train as they fight" when training to employ a Spider munition field. The Spider program is developing software and hardware fixes to allow Soldiers to "train as they fight."

Spider is more complex than its predecessor system and necessitates extensive training to maintain proficiency. Effective training will depend on successful Unit Master Trainer (UMT) and Sustainment Training programs.

Extensive battery management requirements and increased unit transportation requirements create a logistics planning challenge for units employing Spider.

Units employing Spider will have a sustained manpower requirement. Spider munition fields require dedicated operators to employ, fight, maintain, and recover.

The Spider program office is developing system hardware and software improvements to mitigate the reliability, reuse, and training challenges and expects to demonstrate the improvements in an operational test in 1QFY13.

Reliability

The Spider system has four reliability requirements. Data from operational and developmental testing were used to assess Spider reliability.⁸

Munition Self-Destruct Reliability

During the self-destruct sequence, all of the grenades and Claymore mines attached to the Munition Control Unit are fired, leaving no unexploded ordnance on the battlefield. The requirement states that, "There must be at least a 99 percent probability that an individual munition/grenade will successfully launch and detonate when initiated by a self-destruct sequence."

Tripwire (Sensor) Reliability

This requirement applies to the Spider Extended Range Tripwire Sensors and hardware triplines. The Extended Range Tripwire Sensors are triggered and deploy on command from the munition field operator. Soldiers hand-emplace the hardware triplines. The requirement states

⁸ "Capabilities Production Document for Spider Network Munitions System" dated May 2006 with Revision 1 dated June 2008.

that, “There must be at least a 0.95 probability each individual sensor/munition combination reliably deploy, sense and engage targets.”

As indicated in Table 4-1 both of these requirements were met in developmental test events.

Table 4-1. Reliability Requirements Demonstrated In Developmental Testing

CPD Requirements	Threshold	JV/Gov Tests (Apr '09-Aug '10)	PVT (Oct '08–Jan '09)	Data & Computations
Munition Self-Destruct Reliability	0.99	1.00	0.955	JV/Gov = 239 Successes / 239 Firings PVT = 318 Successes / 333 Firings
Hardwire Tripline Reliability	0.95	0.996	0.952	$P_{\text{Function}} = P_{\text{Trip}} \times P_{\text{Fire}}$ JV/Gov = 0.996 (1140/1144) x 1.000 (239/239) PVT = 0.996 (1140/1144) x 0.955 (318/333)
Extended Range Tripwire Sensors Reliability	0.95	0.992	0.863	$P_{\text{Function}} = P_{\text{Deploy}} \times P_{\text{Trip}} \times P_{\text{Fire}}$ JV/Gov = 0.9991 (1067/1068) x 0.9931 (143/144) x 1.000 (239/239) PVT = 0.9991 (1067/1068) x 0.9050 (946/1045) x 0.955 (318/333)

P_{Trip} for Hardwire Triplines and P_{Deploy} for ERTS were tested in PVT but not retested in subsequent JV/Gov testing.

Munition Control Unit Mission Reliability

Spider requirements state that there must be a 98 percent probability that a Spider Munition Control Unit complete 30 days of operation without failure.⁹ The Munition Control Unit must also complete the 30-day mission without Soldiers replacing the batteries.¹⁰ When developing the 30-day power requirement, the Army assumed the Munition Control Unit would be in sleep mode 90 percent of the time and in active mode for 10 percent of the time when Soldiers were operating an emplaced field. In the sleep mode, the batteries provide minimum power to the Munition Control Unit, which then automatically returns to the active mode when a tripline is activated or message is received from the Remote Control Unit operator.

Operational test events for Spider have been less than 30 days. During Production Verification Testing, one Spider field of 12 Munition Control Units operated for 30 days. During this test, the system was in sleep mode for 90 percent of the time and the Munition Control Units and Repeater operated for 30 days without failure or battery change.

⁹ The Spider Failure Definition Scoring Criteria (FDSC) defines an Essential Function Failure (EFF) of a Spider component (MCU, RCU, RCUT, and Repeater) as a significant degradation or the inability of the component to perform one or more of its essential functions. The essential functions of each component are specifically defined in the FDSC.

¹⁰ CPD Attribute 6 (Duration), states, “The Spider system must be capable of performing its mission for 30 days without maintenance and for one year with only operator level maintenance (e.g., change batteries or replace trip wires).”

In two of three operational test events and the NIE Brigade Capstone Exercise, the Munition Control Units used by Soldiers to emplace Spider munition fields did not achieve the required 98 percent reliability. The primary cause of Munition Control Unit failures during these events was Remote Control Unit software complexity causing incorrect Soldier actions.

In FOT1, Soldiers used a set of 66 Munition Control Units to execute a total of 291 individual emplacements in 20 missions for an average duration of 11 hours and 7 minutes. During testing, 254 (87.3 percent) of the Munition Control Units did not fail. For FOT1, 31 of the 37 MCU failures were a direct result of Soldier actions. Eliminating the Soldier-induced failures, the Munition Control Unit mission reliability during these missions would have been 97.9 percent.

The results for the test unit in the FOT2 were similar. During that test, Soldiers used a set of 43 Munition Control Units to execute a total of 131 individual emplacements in 16 missions for an average duration of 6 hours and 48 minutes. Test results showed 109 Munition Control Units (83.2 percent) did not fail and Soldier actions accounted for 20 of 22 failures. Without the Soldier-induced failures, the Munition Control Unit mission reliability would have been 98.5 percent.

During LUT2, Soldiers used a set of 22 Munition Control Units to execute a total of 176 individual emplacements in 8 missions with an average mission time of 3 hours and 31 minutes. There were no Munition Control Unit failures during the 8 missions conducted.

During the NIE Capstone Exercise, Soldiers used a set of 20 Munition Control Units to execute a total of 28 emplacements in two missions. Twelve Munition Control Units (42.9 percent) did not fail. Of the 16 failures, all were the result of Soldier actions. Without these Soldier-induced failures, the Munition Control Unit mission reliability would have been 100 percent.¹¹

To eliminate or minimize Soldier-induced Munition Control Unit sterilizations, Remote Control Unit software complexity must be addressed. In these and previous operational tests, operators reported that Remote Control Unit software was not user-friendly and difficult to follow the on screen procedures. The software contains warnings designed to preclude operator errors. The warnings are not always effective resulting in the same errors observed in successive tests. Fatigued Remote Control Unit operators under adverse environmental conditions must be able to quickly and accurately execute the proper software commands to achieve the desired system condition. More efficient and effective Remote Control Unit operator training would contribute to reducing Soldier-induced failures, but without simplified software, training improvements may prove not sufficient to achieve the reuse requirement.

¹¹ Munition Control Unit Mission Reliability results for FOT1, FOT2, and the LUT2 are shown in Table E-6. Capstone Exercise data are not included in Table E-6 because the Capstone Exercise was not a part of formal operational testing.

Command, Control and Communications (C3) Mission Reliability

The components of the Spider C3 system are the Remote Control Unit, the Remote Control Unit Transceiver, and the Repeater. A failure of any one of the components resulting in the loss of communications between the Remote Control Unit operator and an emplaced field for longer than 20 minutes is considered a C3 failure.¹² The requirement states, “There must be a 99 percent probability that the Spider C3 components successfully complete 30 days of operation without experiencing an essential function failure.” During a C3 failure, a Spider field cannot receive tripwire alerts caused by intruders, nor can it engage targets.

In the FOT1, C3 failures occurred in 3 of 21 Spider fields, for a C3 reliability of 85.7 percent. In FOT2, Spider fields experienced no C3 failures longer than 20 minutes in any of the 16 missions. In LUT2, the three C3 failures were between 19 and 31 minutes. While one of the C3 failures in LUT2 did occur during an intrusion, the overall Remote Control Unit availability for the duration of the field operating time was above 95 percent.

The Spider C3 Mission Reliability requirement of 99 percent is high. Despite the 100 percent C3 Mission Reliability estimates from the FOT2, we can say with only 12 percent confidence that system mission reliability is greater than or equal to the requirement.

Table 4-2 shows the Munition Control Unit Mission and C3 Mission reliability results from the FOT1, FOT2, and LUT2 tests.

Table 4-2. Reliability Requirements Demonstrated in Operational Testing

CPD Requirements	Threshold	LUT2 (Jun 11)	FOT2 (May 10)	FOT1 (Mar 09)	PVT (Oct 08–Jan 09)
Munition Control Unit Mission Reliability	0.980	1.000 (176/176)	All Failures: 0.832 (109/131)	All Failures: 0.873 (254/291)	1 of 1 Successful 30-day Emplacement (w/12 MCUs)
			Without Operator Induced Failures: 0.985 (129/131)	Without Operator Induced Failures: 0.979 (285/291)	
C3 Mission Reliability	0.992	0.700 (7/10)	1.000 (16/16)	0.857 (18/21)	1 of 1 Successful 30-day Emplacement (w/12 MCUs)

Munition Control Unit Reuse Key Performance Parameter (KPP)

The June 2008 Spider Capabilities Production Document (CPD) specifies a Key Performance Parameter that requires a Munition Control Unit to be reusable through seven missions. The threshold reuse requirement, as stated in the CPD is:

¹² The FDSC states “Inability to communicate due to jamming is not considered a reliability failure...”

KPP 4 Reusable: “Individual Spider munition dispensers must be able to be deployed, retrieved, and redeployed at any time prior to detonation of any one munition. Excluding battle damage, at least 90 percent of all munition control units must survive seven deployments.”

Data from the FOT1, FOT2, and LUT2 summarized in Table 4-3 describe Spider’s performance in meeting the reuse requirement. The sample size for assessing the reuse KPP was the number of Munition Control Units having the opportunity for emplacement in at least seven missions.¹³ To achieve success, Soldiers had to emplace, operate, and recover an individual Munition Control Unit at least seven times.

Table 4-3. Reuse KPP Summary

Test Event	Reuse Sample Size	Number of MCUs surviving ≥ 7 missions	Percent of MCUs surviving ≥ 7 missions	Number of MCUs surviving < 7 missions
LUT2 June 2011	22	22	100%	0
FOT2 May 2010	30	9	30%	21
FOT1 March 2009	35	23	66%	12
Combined	87	54	62%	33

All 33 of the Munition Control Units that failed to complete seven or more missions in the FOT1 and FOT2 tests could not be used for further testing and were removed from their respective tests. Over 50 percent of the Munition Control Units tracked for reuse in these two operational tests failed to complete the test. The failure of a Munition Control Unit to meet the reuse requirement has tactical and logistical implications as identified in the KPP rationale provided in the CPD. The CPD states:

“Rationale: The Spider system must be able to withstand the rigors of deployment, retrieval and redeployment (excluding combat damage) without requiring disposal or rebuild (i.e., a repair or replacement of components with a significant cost, time to complete, or which may degrade reliability of the item). Unreliable munitions and non-responsive units will be command destructed or self-destructed. Large numbers of items or components requiring frequent or major repairs would adversely impact retrieval and relocation of obstacles during wartime.”

Of the 33 Munition Control Unit failures in the FOT1 and FOT2 testing, 28 were attributed to Soldier error. As was the case with Munition Control Unit Mission Reliability failures, elimination of the Soldier-induced failures would have resulted in meeting the KPP requirement.

¹³ Although all Munition Control Units (MCUs) should be assessed against this criterion, the scope of each operational test limited the number of MCUs that could be employed in at least seven missions to a subset of the total number used.

- In FOT2, 19 of 21 failures were attributed to Soldier actions. Without these failures, Spider reuse would have been 93 percent (28 of 30).
- In FOT1, 9 of 12 failures were attributed to Soldier actions. Without these failures, Spider reuse would have been 91 percent (32 of 35).

Following these tests, the Spider program identified and initiated hardware, software, and training changes designed to reduce Soldier-induced failures. The primary purpose of LUT2 was to demonstrate the effectiveness of the interim software and training changes the program has implemented. LUT2 data in Table 4-3 indicate that these initial changes were successful and provide confidence that the Reuse requirement can be met in future operational testing after implementing all hardware, software, and training changes.

Logistics

This section addresses three areas (Munition Control Unit failures and sterilizations, battery power management, and unit transportation), that create logistic challenges for the unit employing Spider.

Munition Control Unit Failures and Sterilizations

Table 4-4 provides a summary of Munition Control Unit failure levels during the FOT1, FOT2, and LUT2 tests, as well as the NIE Brigade Capstone Exercise.

Table 4-4. Munition Control Unit Failures Summary

Test Event	Number of MCUs in Test	Number of MCUs which Failed to Complete Test	MCU Failure Rate	80% Confidence Interval for Failure Rate
NIE July 2011	20	17 ^a	85%	72% - 92%
LUT2 June 2011	22	0	0%	0 – 7%
FOT2 May 2010	43	22	51%	41% – 62%
FOT&E March 2009	66	37	56%	48% – 64%
Combined	151	76	50%	45% - 55%

^a In addition to 16 Soldier-induced sterilizations, one MCU was properly certified as destroyed (sterilized) by the field operator during a threat intrusion.

Fifty percent of the Munition Control Units employed under operational test conditions experienced failures that required them to be withdrawn from the test. All but one of the combined 76 Munition Control Unit failures resulted in the sterilization of the Munition Control Unit. For repair, sterilized Munition Control Units must be evacuated to depot-level maintenance facilities or contracted logistics support facilities. For fielded systems, all sterilized

Munition Control Units must be returned to the contractor in the United States before they can be returned to the supply system.

Based on combined data from these tests, if Munition Control Unit failure rates cannot be reduced, we are 80 percent confident that 45 percent to 55 percent more Munition Control Unit stockage will be necessary to support Spider operations.

Munition Control Unit sterilization is a design feature that makes the Munition Control Unit inoperable in the case of uncorrectable faults, loss of communications, failed safety sequence routines, low batteries, or tamper. Sterilization results in the erasing of all mission data and security parameters on the Munition Control Unit, rendering it permanently non-operational and incapable of firing munitions. Sterilization provides the Spider system with several key features:

- Protects the munition field from threat activities to capture system components for future use against friendly forces or threat engineering analyses
- Ensures munitions do not remain active in a munition field should positive "man-in-the-loop" control be lost
- Protects friendly Soldiers should positive "man-in-the-loop" control be lost during emplacement, operation, and recovery of a munition field

Sterilization can also occur due to incorrect actions by Soldiers operating in the field. Table 4-5 summarizes the proportion of sterilizations during operational testing and the NIE Brigade Capstone Exercise attributable to incorrect Soldier actions.

Table 4-5. MCU Sterilizations Summary

Test Event	Number of MCUs in Test	Number of Sterilized MCUs	Number of Sterilized MCUs Due to Soldier Actions	Point Estimate for Sterilizations Due to Soldier Actions
NIE July 2011	20	17	16	94%
LUT2 June 2011	22	0	0	0%
FOT2 May 2010	43	22	20	91%
FOT&E March 2009	66	36 ^a	31	86%
Combined	151	75	67	89%

^a One MCU failure did not result in sterilization.

With the exception of the LUT2, approximately 90 percent of all sterilizations in each test were attributable to Remote Control Unit software complexity causing incorrect Soldier actions. Munition Control Unit Mission and Reuse requirements can be met, and the additional

logistics burden of Munition Control Unit failures would be minimized with improvements to Remote Control Unit software.

In LUT2, units employing Spider did not experience Munition Control Unit sterilizations and failures during the record test missions. The LUT2 results suggest that the Army's efforts to improve software and hardware function and user interface, along with training improvements, may overcome previous Soldier-induced failures. Further planned improvements show potential for decreasing Soldier-induced failures. These improvements will be included in future operational testing.

Remote Control Unit software complexity contributes to Soldier-induced MCU sterilizations creating a logistics burden and degrading operational suitability. Planned software changes to the Remote Control Unit combined with future hardware changes to the MCU will eliminate the logistics burden by allowing Soldiers to reset sterilized MCUs for immediate use in a munition field. Without these planned software and hardware changes, Spider remains not operationally suitable.

Battery Life and Power

Units must manage three different types of batteries based on the Spider design. Four components of the Spider system use battery power during all or part of the system's operational time. Management of these components and their associated batteries presents logistical and operational challenges for units employing Spider.

Remote Control Unit (RCU). The RCU can be powered by either AC or DC power if available. Adaptor cables are provided to support these power sources, which are preferred during sustained operations. These power sources cannot be used during field emplacement and maintenance operations because the Remote Control Unit must be physically moved to the location of each Munition Control Unit. The Remote Control Unit is powered by a TRB-1264 rechargeable lithium battery. Figure 4-1 provides basic information about the battery.



Figure 4-1. Remote Control Unit Battery Information

A fully charged TRB-1264 battery can power a Remote Control Unit for up to 2 hours. With an average field emplacement time of 2 hours and 47 minutes during FOT2, nearly every emplacement required the Remote Control Unit operator to conduct at least one "hot swap" to replace the discharged battery with a fully charged battery before continuing the emplacement process. During "hot swap" procedures, the Remote Control Unit is briefly powered by the Remote Control Unit Transceiver.

A correctly executed “hot swap” has little effect on the emplacement or maintenance processes, but an incorrectly executed “hot swap” can result in Munition Control Unit sterilizations and/or the need to re-emplace all or part of the field. Longer Remote Control Unit battery life or shorter emplacement times would reduce the vulnerability of the system to potential operational impacts of a failed “hot swap.”

Remote Control Unit Transceiver (RCUT). The Remote Control Unit Transceiver is powered by either an external 28-volt DC power source or two internal, BA-5360 non-rechargeable lithium batteries. If external power is being used but drops below 11 volts, the Remote Control Unit Transceiver will automatically switch to internal battery power. Figure 4-2 provides basic information about the batteries.



Figure 4-2. Remote Control Unit Transceiver Battery Information

Fully charged BA-5360 batteries can power a Remote Control Unit Transceiver for approximately 60 hours. The Remote Control Unit Transceiver accurately tracks battery life and provides appropriate warnings to the operator when battery life reaches a critical point. Remote Control Unit Transceiver batteries can be replaced in a “hot swap” procedure that requires no external power.

Munition Control Units (MCUs) and Repeaters. The Repeater is powered by either an external 28-volt DC power source or four internal, LSH-20 non-rechargeable lithium batteries. If the DC power source drops below 11 volts, the Repeater will automatically switch to internal battery power.

The Munition Control Unit also uses four internal, LSH-20 non-rechargeable lithium batteries, but does not have an external power source capability.¹⁴ Units must closely monitor battery management because Munition Control Units do not have an external power source.

Figure 4-3 provides basic information about the Munition Control Unit and Repeater batteries and shows the battery carriage electronic assembly (BCEA) that holds the batteries in the Munition Control Unit.

¹⁴ The Mission Control Unit Mission Reliability requirement to successfully complete a 30-day mission without requiring its batteries to be replaced was discussed earlier in this section.



Figure 4-3. LSH-20 Battery Information

A set of fully charged LSH-20 batteries can power a repeater or a Munition Control Unit under full power for approximately 60 hours when either device is not in the sleep mode.

The Repeater accurately tracks battery life and provides appropriate warnings when battery life reaches a critical point. Operators can replace the Repeater batteries while it operates on external power or while temporarily removing the Repeater from the networked munition field.

The Munition Control Unit does not track battery life but instead relies on the carriage holding the batteries to monitor and report battery status. The battery carriage will provide an accurate battery life estimate only if fully charged batteries are installed and they are kept in the carriage after being removed from the Munition Control Unit. If a less than fully charged set of batteries is loaded into the battery carriage, the internal charge meter will show a full battery charge.

Based on the estimate of remaining battery life reported by the battery carriage, each Munition Control Unit updates to the Remote Control Unit when its remaining battery capacity reaches 44 percent (low power alert) and again when remaining capacity reaches 24 percent (critical power alert). The Remote Control Unit, however, does not differentiate between low and critical alerts, so when an alert is received the operator must query the Munition Control Unit for status to show the remaining battery capacity. If a Munition Control Unit's remaining battery capacity falls below 12 percent, it will sterilize without further alerting the Remote Control Unit.

The battery carriage may overestimate the actual remaining battery life (less than fully charged batteries installed), resulting in Munition Control Unit sterilizations. Soldiers must implement special handling procedures to keep track of Munition Control Unit battery life. When replacing batteries, Soldiers must ensure complete replacement with four new batteries in each Munition Control Unit.

The option of replacing non-rechargeable batteries after each use provides confidence that the battery status is correctly reported to the Remote Control Unit. A platoon-level emplacement of a Spider munition field in a training exercise or tactical mission of between one and 60 hours duration employing one Remote Control Unit Transceiver, one Repeater, and 20 Munition Control Units would require a minimum of two BA-5360 and 84 LSH-20 batteries. Including an extra 10 percent battery stockage to cover unforeseen battery losses, the non-

rechargeable batteries to support this platoon-level training/mission would cost approximately \$2,400 from the commander's unit operating funds. This cost represents a significant part of a commander's normal operating budget.

Unit Transportation

A complete Spider system, including Class V basic load and additional stockage (Table 1-1), weighs approximately 1,900 pounds and has a volume of approximately 82.6 cubic feet. The transportation requirement for one Spider system is a payload equivalent to one cargo High Mobility Multi-purpose Wheeled Vehicle (HMMWV) for a company-sized unit. The space allocation for Spider assets is in addition to requirements for other unit materiel and equipment and can cause a logistics planning challenge for some units. Additional assets may be required if the VHAM antenna (85 pounds and 11.7 cubic feet) becomes a standard component of the Spider system. Munition Control Unit sterilizations during Spider employment, as previously discussed, suggest that commanders must also consider an additional planning factor to cover unplanned losses in order to sustain obstacle integrity.

Training

Spider is a more complex system than the anti-personnel mine it replaces. Spider requires:

- Unit leaders with a thorough understanding of system capabilities and limitations
- Fully trained and proficient Remote Control Unit operators
- Soldiers trained on Spider specific tasks and unit basic tasks
- Detailed Tactics, Techniques, and Procedures (TTPs)

Spider skills are perishable and require effective initial and recurring individual and unit training. After the 2009 FOT1, the user recognized the need for a formal Spider unit training program, which would include an effective pre-fielding training program for units receiving Spider, a formal unit sustainment training program overseen by a unit master trainer (UMT), and a formal certification program for Remote Control Unit operators and UMTs.

The Spider Training Program

The first element of the Spider unit training program is pre-fielding training for units receiving the Spider system. For deploying units, the user desires that this training be conducted during the Reset/Train phase of the Army Force Generation (ARFORGEN) Model.¹⁵ The key elements of this program include:

- Five days of individual Soldier New Equipment Training (NET) conducted by the materiel developer

¹⁵ The ARFORGEN Model is the Army's structured progression of increased unit readiness over time resulting in recurring periods of availability of trained, cohesive units ready to deploy in support of combatant commanders' or civil authorities' requirements.

- Five days of individual and collective Doctrine, Tactics, and Techniques (DTT) training with practical exercises conducted by the U.S. Army Engineer School (USAES)
- Two days of Unit Master Trainer (UMT) training conducted by USAES

Following certification, UMTs are placed on unit orders and assume responsibility for the planning and execution of Spider sustainment training as directed by the unit commander.

At the completion of NET and DTT training, the USAES does not consider the unit to be proficient to effectively employ Spider in a combat environment. The sustainment training program augments formal NET and DTT and supports the achievement of unit proficiency levels adequate to effectively employ Spider in a combat environment.

Unit Sustainment Training is scheduled by the unit commander and planned and executed by the UMT and Alternate UMT. The purpose of sustainment training is to ensure continued expertise of appropriate unit personnel on the employment, maintenance, and operation of the Spider system. The training includes individual and collective tasks in a tactical environment and execution of the Spider Certification Program.

The Spider Certification Program requires the semiannual recertification of unit Remote Control Unit operators by the UMT and recertification of the UMT(s) by the USAES. The program includes a requirement for at least one annual Situational Training Exercise for assigned Spider crews. For deploying units, a pre-deployment live fire exercise with both grenades and Claymores is required.

FOT2 Training

In preparation for FOT2, the test unit received NET and DTT training in accordance with the training program.

Because the test unit was available for only a limited period of time to train and execute FOT2, the user requested, and the test unit received, an additional week of training by the USAES's DTT trainers. The purpose of this additional training was to augment formal NET and DTT and to support the achievement of unit proficiency levels adequate to effectively employ Spider in the simulated combat environment of the test. This additional training was in lieu of training a UMT and executing home station unit sustainment training in accordance with the training program.

A fourth week of training for the unit included participation in the FOT2 pilot test, in which it executed four missions under the control of the Operational Test Command, and additional unit-controlled training during which DTT trainers were available to provide assistance.

The FOT2 record test demonstrated that an engineer unit could fight Spider fields effectively but it did not demonstrate that an engineer unit could emplace, maintain, and recover Spider fields effectively. Despite having just completed four weeks of formal and informal training, the unit sterilized 51 percent of their MCU test assets (Table 4-4), 91 percent of which

was due to Soldier error (Table 4-5). The FOT2 results did not validate the effectiveness of the Spider pre-fielding training program.

LUT2 Training

In preparation for LUT2, the test unit received NET and DTT training in accordance with the training program. A third week of training for the unit included participation in the two-day LUT2 synchronization event and a two-day pilot test, during which the unit executed four missions under the control of the Operational Test Command. A final one-hour refresher training class conducted by the MSCoE preceded the record test.

The LUT2 record test demonstrated the program has made the necessary changes in the NET and DTT training program for Soldiers to properly employ Spider. The updated training program allowed an Engineer platoon and an Infantry platoon to emplace, maintain, and recover Spider fields supporting the commander's intent for protective obstacles.

Unit Sustainment Training

Effective sustainment training is essential to maintaining a unit's proficiency in employing the Spider system. Current Spider system design does not support efficient and effective training.

Spider training violates the Army's "Train as You Fight" principle. Employment doctrine, based on the tactical situation, directs the use of grenades and Claymore mines in a single field under the control of a single Remote Control Unit operator. In fields with multiple munition types, the grenades are installed on designated Munition Control Units while the Claymore mines are attached to other Munition Control Units using Munition Adaptor Modules. A single Remote Control Unit operator with a dedicated observer can control and fight a mixed munition field. This tactical field configuration is shown in Figure 1-4.

Although some scenarios may include the use of live munitions, in most training scenarios a unit uses inert grenades and Claymore mines. When using inert grenades and Claymore mines, as depicted in Figure 4-4, Spider hardware and software will not permit the training to be conducted in the same field configuration.¹⁶

¹⁶ The Remote Control Unit (RCU) has an embedded trainer, which allows RCU operators to fight a combined MGL and Claymore field using a single RCU. This training option, however, does not contribute to hands-on experience for other unit personnel in emplacing, maintaining, or recovering a tactical field or to experience for the RCU operator in coordinating with the field observer.

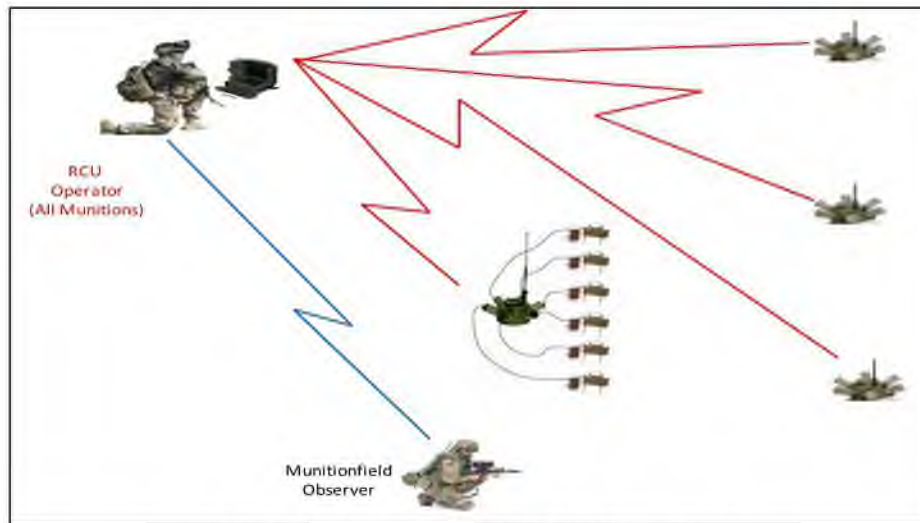


Figure 4-4. Tactical Field Configuration

Because lethal and non-lethal munitions are attached to Munition Control Units using a Munition Adaptor Module, the Remote Control Unit software considers a Munition Adaptor Module to always have a live munition attached. The Remote Control Unit software does not detect if inert lethal and non-lethal munitions are attached to the Munition Adaptor Module.

Remote Control Unit software will not permit the mixing of inert and live munitions in a field. To train to fight a mixed grenade and Claymore minefield, a unit must use two Remote Control Units and emplace, maintain, fight, and recover two separate fields – one with grenades attached to the Munition Control Units and on with Claymores attached to the Munition Control Units. This training field configuration is shown in Figure 4-5.

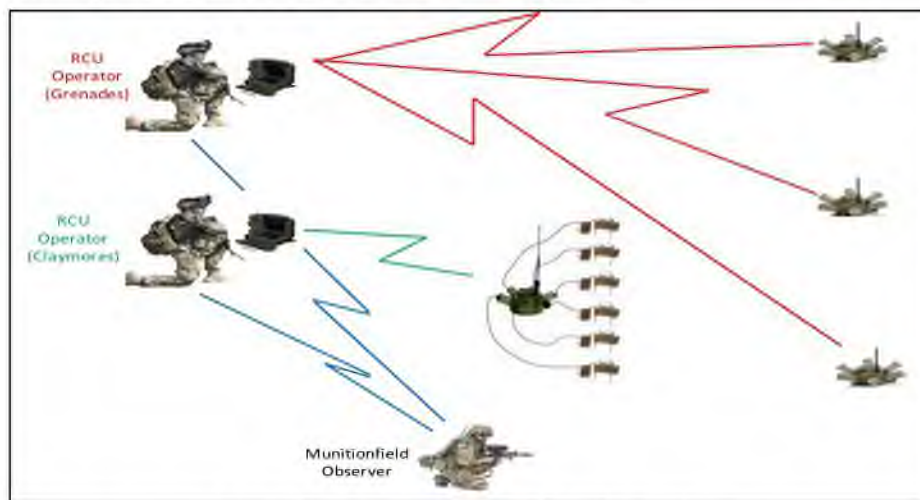


Figure 4-5. Training Field Configuration

This training deficiency can be fixed with the development of a Munition Adaptor Module trainer. The Munition Adaptor Module trainer would allow units to train with grenades and Claymore mines in the same field under control of a single Remote Control Unit. Not having a Munition Adaptor Module trainer complicates Spider training and decreases the effectiveness of unit training under the sustainment training program.

The Spider program is developing a Module Universal Trainer, which will attach to the Munition Control Unit and allow a unit to train with both inert grenades and Claymore mines in a single munition field controlled by one operator. The Army plans to have the Module Universal Trainer available to support full operational testing in 1QFY13.

Manpower

A Spider munition field requires less manpower and time to emplace than a legacy M16-Series anti-personnel minefield of the same size. Using a 200-by-200 meter munition field as an example, an M16-Series field required approximately 30 personnel working 14 hours to complete installation. During FOT2, a squad of 10 soldiers emplaced Spider fields of varying sizes (up to 20 Munition Control Units), and required an average of 2.6 hours to complete emplacement. During LUT2, this time averaged close to 2 hours. The 200-by-200 meter Spider munition field would require 10 personnel approximately 8 hours to emplace. A Spider munition field requires more manpower and time to fight, maintain, and recover than an M16-Series anti-personnel minefield of the same size.

Once emplaced, an M16-Series minefield required only overwatch personnel. In order to conduct operations with the Spider munition field, the commander must dedicate nearly a platoon's worth of personnel for specific Spider roles. Primary operation of the Spider munition field (fighting the field) requires a Remote Control Unit operator and assistant, as well as a dedicated overwatch team. For the purposes of resource analysis, we assume the unit conducts sustained combat operations and employs three 8-hour shifts. Under this scenario, the personnel requirement to fight the field becomes four personnel per shift times three shifts, or 12 personnel, dedicated to fighting the field over a 24-hour period. Additionally, Soldiers must be prepared to enter the field at any time to conduct maintenance operations such as resetting/reinstalling tripline sensors, changing batteries, or assessing damage caused by environmental factors. Our analysis allowed for an additional two personnel dedicated to the maintenance operations per field. Further, following mission completion, the unit must recover Spider for future use. The recovery actions typically require the same number of personnel as emplacement operations, and these 10 personnel could be different from the personnel conducting the original emplacement.

Table 4-6 depicts the likely manpower demands for a 200-by-200 meter Spider munition field.

Table 4-6. Manpower Requirements

Munition Field Type (200 x 200 meters)	Personnel / Time to:				Comments
	Emplace	Overwatch & Fight	Maintain	Recover	
M16-Series	30 soldiers / 14 hours	6 soldiers / 24 hours	NA	NA	No additional troop burden
Spider	10 soldiers / 8 hours	12 soldiers / 24 hours*	2 soldiers / as needed	10 soldiers / 5 hours	May require troop augmentation for security and/or field operations

* Assumes 8-hour shifts and includes two operators per shift and a two-person observer team per shift.

Spider imposes sustained manpower requirements on the unit employing it more so than the legacy M16-Series mine. In sustained operations, the need for dedicated personnel to support an employed Spider system takes personnel away from other unit tasks.

Section Five Survivability

Survivability

The Spider XM7 Network Command Munition is survivable. Spider Munition Control Units are vulnerable to the effects of direct small arms and crew-served weapons. Units using proper tactics, techniques, and procedures can mitigate the effects of these weapons. Spider is temporarily not effective in some Electronic Warfare and Electromagnetic Environmental Effects environments.

Electronic Warfare

Threat Radio Frequency Jamming

Technical Radio Frequency testing in August 2005 showed that jamming could effectively sever the Remote Control Unit to Munition Control Unit communication link. When this occurs, the Spider system cannot engage threat intruders for the duration of the jamming event. Once jamming ends, the Spider Remote Control Unit will automatically attempt to reestablish communications with the Munition Control Units and return to operational status. The effectiveness of threat Radio Frequency jamming activity and the capability of the system to reestablish communications and operational status after jamming has ceased was confirmed during operational testing in 2007 and 2009.

Interoperability Testing

Testers from the U.S. Army Electronic Proving Ground and the Yuma Proving Ground Counter-Terrorism/Counter-Insurgency Integrated Test and Evaluation Center conducted an Interoperability Test in October 2008 to determine the impacts of friendly jammers and communications systems on Spider operations. Testing was conducted with and without the Repeater in use. Analysis of the data is classified and is contained in the classified Electronic Proving Ground report "Interoperability Test Report TR08-10-013" dated December 2008.

Ballistic Survivability

Exposed, unprotected Munition Control Units are vulnerable to direct small arms and crew served weapons fire. Tactics, Techniques, and Procedures, including the use of sandbags, can successfully protect against the effects of fragments and mitigate the effects of direct fire weapons.

Electromagnetic Environmental Effects

Electromagnetic Environmental Effects testing was conducted at White Sands Missile Range, New Mexico, and at the Redstone Technical Test Center Lightning Test Facility in Huntsville, Alabama, June – August 2005. Results of the Electromagnetic Environmental Effects testing showed that Spider was temporarily not effective in three environments.

- Testing was performed to assess the survivability of Spider in the operational battlefield electromagnetic environments (EME) specified in MIL-STD-464A. The system as emplaced did not completely meet the MIL-STD-464A criteria.

- Testing was performed to assess the survivability of the Spider to the electromagnetic environment generated by a near lightning strike. Under Near-strike Lightning (NSL) conditions when the Remote Control Unit was in close proximity to the Munition Control Units, the Remote Control Unit could not communicate with the Munition Control Units. Since the Remote Control Unit and Munition Control Units are only in close proximity during emplacement operations, vulnerability appears limited to that phase of Spider operations. The NSL environment did not permanently damage the system or render it inoperable for a significant period of time. The Spider Remote Control Unit operator was able to correct all transient anomalies induced by the NSL environment.
- Testing was performed to assess the survivability of the Spider to the electromagnetic environment generated by a High Altitude Electromagnetic Pulse (HEMP). Although the HEMP environment rendered the system inoperable for a short period of time, the system was not permanently damaged. The Spider Remote Control Unit operator was able to correct all transient performance anomalies induced by the HEMP environment.

Penetration and Information Assurance Testing

The Communications-Electronics Research Development and Engineering Center conducted Penetration and Information Assurance testing in December 2007 and again in March and April 2009 after Remote Control Unit software upgrades. As a result of mitigations, the risks in both areas remain low. In June 2009, the Army provided a full Authority To Operate determination for the Spider system valid through June 2012. The program is currently on track to renew the certification.

COMSEC and Security Certification Requirements

The National Institute of Standards and Technology provided Cryptographic Module Validation Program certificates for Spider Remote Control Units, Remote Control Unit Trainers, Munition Control Units, and Repeaters.

Chemical, Biological, Radiological, and Nuclear Survivability

Spider is capable of operating in a Chemical, Biological, Radiological and Nuclear environment. Spider storage containers adequately protect stored system components from contamination.

Section Six Recommendations

Recommendations

The Spider XM7 Network Command Munition is operationally effective, lethal, and survivable. It is not operationally suitable. The Spider program executed the operational and live fire testing in accordance with DOT&E-approved test plans. I recommend the Army consider the following recommendations:

Operational Effectiveness and Lethality

- In support of systems fielded to operational forces, develop in-theater capability to reprogram sterilized Munition Control Units and return them to the supply system.
- Review Spider system design with the goal of reducing the need for three different types of batteries.
- Develop Tactics, Techniques, and Procedures for the Remote Control Unit and Remote Control Unit Transceiver to use reliable commercial or military power sources in lieu of battery power whenever possible.
- Implement and validate the Unit Master Trainer and Sustainment Training programs and ensure that these programs are incorporated in the Army's training standards program.

Operational Suitability

- Implement and test the planned Spider software modifications to eliminate the possibility of Munition Control Unit sterilization during emplacement, field operations, and recovery of a Spider munition field.
- Pursue and test a Munition Adaptor Module trainer so units can "Train as they Fight."
- Continue the upgrading of Remote Control Unit and Munition Control Unit software to improve user interface.
- Develop and implement the capability for Munition Control Units to monitor and accurately report current battery status.
- Pursue solutions and update the Tactics, Techniques, and Procedures to implement Spider enhancements and non-lethal munitions.



[REDACTED]
OFFICE OF THE SECRETARY OF DEFENSE

WASHINGTON, DC 20301

FEB 15 2012

The Honorable C. W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

Dear Mr. Chairman:

I have enclosed at TAB A the Spider XM7 Network Command Munition Combined Operational and Live Fire Test and Evaluation Report, required by Sections 2399 and 2366, Title 10, United States Code. Enclosed at TAB B is the classified annex to this report. In this report I conclude the following:

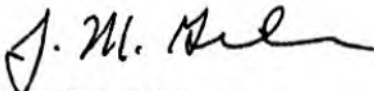
- Spider is operationally effective. Spider is not persistent and does not allow autonomous engagements. Persistence and autonomous engagements were features of previous anti-personnel munitions that violate current National Landmine Policy. Spider provides remote firing of munitions, collection of situational awareness information, and support of friendly maneuver. A properly trained unit can emplace and maintain positive "man-in-the-loop" control of Spider munitions in order to contribute to protective obstacle effects.
- Live fire testing and analyses concluded that Spider is lethal and can produce combat casualties. In addition to lethal munitions, Spider can also fire non-lethal munitions to support friendly forces.
- Spider is not operationally suitable. Spider is more complex than legacy anti-personnel munitions and requires extensive training to maintain proficiency. Spider reliability and reuse requirements are difficult to achieve and have not been demonstrated consistently under realistic operational conditions. Units employing Spider will have a sustained manpower requirement because Spider munition fields require dedicated operators to employ, fight, maintain, and recover.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the



[REDACTED]

Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosures:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member



[REDACTED]
OFFICE OF THE SECRETARY OF DEFENSE

WASHINGTON, DC 20301

FEB 15 2012

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

Dear Mr. Chairman:

I have enclosed at TAB A the Spider XM7 Network Command Munition Combined Operational and Live Fire Test and Evaluation Report, required by Sections 2399 and 2366, Title 10, United States Code. Enclosed at TAB B is the classified annex to this report. In this report I conclude the following:

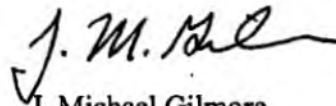
- Spider is operationally effective. Spider is not persistent and does not allow autonomous engagements. Persistence and autonomous engagements were features of previous anti-personnel munitions that violate current National Landmine Policy. Spider provides remote firing of munitions, collection of situational awareness information, and support of friendly maneuver. A properly trained unit can emplace and maintain positive "man-in-the-loop" control of Spider munitions in order to contribute to protective obstacle effects.
- Live fire testing and analyses concluded that Spider is lethal and can produce combat casualties. In addition to lethal munitions, Spider can also fire non-lethal munitions to support friendly forces.
- Spider is not operationally suitable. Spider is more complex than legacy anti-personnel munitions and requires extensive training to maintain proficiency. Spider reliability and reuse requirements are difficult to achieve and have not been demonstrated consistently under realistic operational conditions. Units employing Spider will have a sustained manpower requirement because Spider munition fields require dedicated operators to employ, fight, maintain, and recover.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the



[REDACTED]

Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosures:
As stated

cc:
The Honorable John McCain
Ranking Member



[REDACTED]
OFFICE OF THE SECRETARY OF DEFENSE

WASHINGTON, DC 20301

FEB 15 2012

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6025

Dear Mr. Chairman:

I have enclosed at TAB A the Spider XM7 Network Command Munition Combined Operational and Live Fire Test and Evaluation Report, required by Sections 2399 and 2366, Title 10, United States Code. Enclosed at TAB B is the classified annex to this report. In this report I conclude the following:

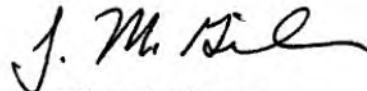
- Spider is operationally effective. Spider is not persistent and does not allow autonomous engagements. Persistence and autonomous engagements were features of previous anti-personnel munitions that violate current National Landmine Policy. Spider provides remote firing of munitions, collection of situational awareness information, and support of friendly maneuver. A properly trained unit can emplace and maintain positive "man-in-the-loop" control of Spider munitions in order to contribute to protective obstacle effects.
- Live fire testing and analyses concluded that Spider is lethal and can produce combat casualties. In addition to lethal munitions, Spider can also fire non-lethal munitions to support friendly forces.
- Spider is not operationally suitable. Spider is more complex than legacy anti-personnel munitions and requires extensive training to maintain proficiency. Spider reliability and reuse requirements are difficult to achieve and have not been demonstrated consistently under realistic operational conditions. Units employing Spider will have a sustained manpower requirement because Spider munition fields require dedicated operators to employ, fight, maintain, and recover.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the



[REDACTED]

Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosures:
As stated

cc:
The Honorable Thad Cochran
Ranking Member



[REDACTED]
OFFICE OF THE SECRETARY OF DEFENSE

WASHINGTON, DC 20301

FEB 15 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

I have enclosed at TAB A the Spider XM7 Network Command Munition Combined Operational and Live Fire Test and Evaluation Report, required by Sections 2399 and 2366, Title 10, United States Code. Enclosed at TAB B is the classified annex to this report. In this report I conclude the following:

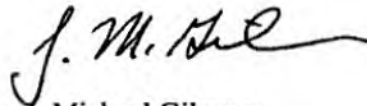
- Spider is operationally effective. Spider is not persistent and does not allow autonomous engagements. Persistence and autonomous engagements were features of previous anti-personnel munitions that violate current National Landmine Policy. Spider provides remote firing of munitions, collection of situational awareness information, and support of friendly maneuver. A properly trained unit can emplace and maintain positive "man-in-the-loop" control of Spider munitions in order to contribute to protective obstacle effects.
- Live fire testing and analyses concluded that Spider is lethal and can produce combat casualties. In addition to lethal munitions, Spider can also fire non-lethal munitions to support friendly forces.
- Spider is not operationally suitable. Spider is more complex than legacy anti-personnel munitions and requires extensive training to maintain proficiency. Spider reliability and reuse requirements are difficult to achieve and have not been demonstrated consistently under realistic operational conditions. Units employing Spider will have a sustained manpower requirement because Spider munition fields require dedicated operators to employ, fight, maintain, and recover.

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Secretary of the Army; the Vice Chairman of the

[REDACTED]

[REDACTED]

Joint Chiefs of Staff; and the Chairmen and Ranking Members of the Congressional defense committees.


J. Michael Gilmore
Director

Enclosures:
As stated

cc:
The Honorable Adam Smith
Ranking Member

Director, Operational Test and Evaluation

2011 Assessment of the Ballistic Missile Defense System (BMDS)



February 2012

This report satisfies the provisions of the National Defense Authorization Act for Fiscal Year 2002, Section 232 (h), as amended by subsequent Acts, which mandates that the Director, Operational Test and Evaluation, annually characterize the operational effectiveness, suitability, and survivability of the BMDS, and its elements, that have been fielded or tested before the end of the preceding fiscal year. The Act also requires the Director to assess the adequacy and sufficiency of the BMDS test program during the preceding fiscal year. This report is unclassified. Supporting information is contained in classified appendices to this report.

J. Michael Gilmore
Director

The marginal cost of producing this report is estimated to be approximately \$135K. Funding is projected to be \$38.0B for ballistic missile defense during the period spanning the current future year's defense program.

This page intentionally left blank.

Executive Summary

This report characterizes the Ballistic Missile Defense System (BMDS) and its weapons elements: Aegis Ballistic Missile Defense (Aegis BMD), Ground-based Midcourse Defense (GMD), Patriot, and Terminal High Altitude Area Defense (THAAD). The report characterizes Command, Control, Battle Management, and Communications (C2BMC) in its enabling role to the weapon elements. First is an assessment of progress toward demonstrating capability against the four ballistic missile threat classes: Short Range Ballistic Missiles (SRBMs), Medium Range Ballistic Missiles (MRBMs), Intermediate Range Ballistic Missiles (IRBMs), and Inter Continental Ballistic Missiles (ICBMs). Second is an assessment of the adequacy of the Missile Defense Agency (MDA) test program. Third is a characterization of overall BMDS operational effectiveness, suitability, and survivability, with supporting details included in two classified appendices. Included in this year's report is a third appendix, Appendix C, which is an operational assessment of Phase I of the European Phased Adaptive Approach (EPAA). The assessment is a standalone detailed characterization of the operational effectiveness, suitability, and survivability of Phase 1, as well as an evaluation of test adequacy. In order to include the most current information available by publication date, this report covers the period of October 1, 2010 through December 31, 2011, Fiscal Year/Calendar Year 2011 (FY/CY11).

During this period, Aegis BMD and THAAD demonstrated progress toward IRBM and SRBM threat class capability, respectively. However, GMD suffered a second consecutive flight test failure and did not demonstrate any progress toward IRBM or ICBM threat class capability. C2BMC, for the first time, demonstrated the capability to control two operationally-deployed AN/TPY-2 radars in forward-based modes, using operational communications architectures; personnel; and tactics, techniques, and procedures. Weapon inventories are growing slowly. Model and simulation verification, validation, and accreditation (VV&A) to support quantitative performance assessments will, in many instances, require several more years to complete.

The MDA conducted four intercept flight tests this past year: two for Aegis BMD, one for GMD, and one for THAAD. The U.S. Army conducted four Patriot intercept flight tests, one for the PAC-3 Missile Segment Enhancement (MSE) interceptor, and three supporting Post Deployment Build 7. The MDA conducted eleven ground tests and exercises, with the most significant ground test, the GTD-04 series, occurring late in the calendar year supporting the implementation of EPAA Phase 1 capability on January 1, 2012.

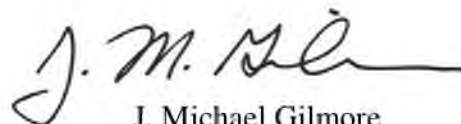
The MDA test program for FY/CY11 was adequate to support the development of the BMDS. The MDA conducted tests as scheduled in the Integrated Master Test Plan (IMTP), Versions 10.2 and 11.1, approved by the MDA Director and DOT&E in July 2010 and February 2011, respectively. Due to limited target availability, the MDA realigned several flight tests, including cancelling FTT-24 and FTT-13 and appending their objectives to existing tests. Execution as planned reflects the mature MDA IMTP scheduling process. This effort allowed the MDA to collect important data on Critical Engagement Conditions and Empirical Measurement Events supporting model and simulation VV&A. During the reporting period, the

MDA continued to emphasize operational realism when planning for and conducting both ground and flight testing.

As has been true in the past, the assessments in this report often contain subjective content due to the limited amount of test data that are available and the resulting limited progress toward VV&A of the required BMDS models and simulations. However, in the case of Aegis BMD and THAAD, for which the MDA and the BMDS Operational Test Agency have collected sufficient data to perform more quantitative assessments, this report includes estimates of the probability of engagement success for the tested battlespace of the two weapon systems. This past year, THAAD completed an initial operational test and evaluation (IOT&E). DOT&E will publish a separate detailed report supporting a decision to proceed beyond low rate initial production. Data from the IOT&E are, however, included in this report.

The MDA completed the planned EPAA Phase 1 technical capability declaration in late December 2011. Appendix C, containing a separate Executive Summary, provides an assessment of Phase 1 capability based on the results of the testing that the MDA has performed. The testing conducted thus far supports an assessment of capability demonstrated in a limited region of the EPAA's overall potential battlespace. The additional future testing contained in the IMTP will be required to validate the models and simulations needed to assess overall EPAA capability.

As the MDA executes the IMTP during the next several years, additional test data supporting quantitative assessments should be available. However, complete quantitative assessments of BMDS capability are still a number of years in the future. This is because it will take several more years to collect the test data needed to adequately verify, validate, and accredit the BMDS models and simulations required to perform such assessments. As data are collected, assessments will incrementally become more quantitative. In this report, Aegis BMD and THAAD reflect this progression.

A handwritten signature in black ink, appearing to read "J. M. Gilmore", with a stylized flourish at the end.

J. Michael Gilmore
Director

Contents

Introduction.....	1
The Ballistic Missile Defense System (BMDS)	3
Description.....	3
BMDS Architecture	4
Aegis Ballistic Missile Defense (Aegis BMD).....	4
Ground-based Midcourse Defense (GMD).....	5
Patriot.....	5
Terminal High Altitude Area Defense (THAAD)	5
Command, Control, Battle Management, and Communications (C2BMC)	6
Sensors	6
Future Capability Development.....	8
Weapons.....	9
Sensors	9
Advanced C2BMC.....	10
BMDS Development/Deployment Concept	10
Phased Adaptive Approach: European Defense.....	10
U.S. Homeland Defense	11
BMDS Progress Toward Threat Class Capabilities	13
Progress Demonstration Levels.....	13
BMDS Progress.....	17
Threat-Class Defense Progress.....	19
Short-Range Ballistic Missile (SRBM)	19
Aegis BMD	20
THAAD Fire Control and Communications (TFCC 5.2)	21
Patriot (PDB 6.5)	22
Medium-Range Ballistic Missile (MRBM)	22
Aegis BMD	23
THAAD (TFCC 5.2).....	24
Intermediate-Range Ballistic Missile (IRBM).....	24
GMD Fire Control (GFC 6B)	25
Aegis BMD	25
Intercontinental Ballistic Missiles (ICBM)	26
GMD (GFC 6B)	26
Aegis BMD	27
BMDS Battle Management Progress	27
Sensor Management.....	27
Sensor-Weapon Pairing/Track Forwarding	27
Engagement Direction/Situational Awareness	28
Assessment of BMDS Test Adequacy.....	29
BMDS Test Adequacy Assessment Methodology.....	29
Threat-Class Defense Test Adequacy Assessment.....	31

SRBM	31
Test Planning and Execution for FY/CY11	31
Operational Realism Assessment	34
Modeling and Simulation Verification, Validation, and Accreditation (VV&A) Status	35
Target Development and Employment Status	36
MRBM	37
Test Planning and Execution for FY/CY11	37
Operational Realism Assessment	38
Modeling and Simulation VV&A Status	40
Target Development and Employment Status	41
IRBM	41
Test Planning and Execution for FY/CY11	41
Operational Realism Assessment	43
Modeling and Simulation VV&A Status	44
Target Development and Employment Status	45
ICBM	45
Test Planning and Execution for FY/CY11	45
Operational Realism Assessment	46
Modeling and Simulation VV&A Status	46
Target Development and Employment Status	46
BMDS Battle Management Test Adequacy Assessment.....	47

Characterization of BMDS Operational Effectiveness, Suitability, and Survivability 51

BMDS Performance Characterization Methodology.....	51
Threat-Class Defense Performance Characterization	53
SRBM	53
Aegis BMD (SRBM)	53
THAAD (TFCC 5.2) (SRBM)	56
Patriot (PDB-6.5) (SRBM)	58
MRBM	59
Aegis BMD (MRBM).....	59
THAAD (TFCC 5.2) (MRBM).....	62
Patriot (PDB-6.5) (MRBM).....	62
IRBM	62
GMD (GFC 6B) (IRBM)	62
Aegis BMD (IRBM)	65
ICBM	66
GMD (GFC 6B) (ICBM)	66
BMDS Battle Management Performance Characterization.....	66

Appendix A (Classified).....Separate Cover

Appendix B (Classified).....Separate Cover

Appendix C (Classified).....Separate Cover

Section One Introduction

This report supports the congressional reporting requirements of the Director, Operational Test and Evaluation (DOT&E), as they pertain to the Ballistic Missile Defense System (BMDS). Congress specified these requirements in the Fiscal Year (FY) 2002 National Defense Authorization Act. The FY09 National Defense Authorization Act, Section 234, amends the FY02 Authorization Act to consolidate the reporting requirements of both the FY02 and FY06 Authorization Acts. The FY02 National Defense Authorization Act, as amended, mandates that DOT&E each year characterize the operational effectiveness, suitability, and survivability, of the BMDS and its elements that have been fielded or tested before the end of the preceding fiscal year. The act also requires DOT&E to assess the adequacy and sufficiency of the BMDS test program during the preceding fiscal year. Although the act calls for an assessment of the test program for the preceding fiscal year only, this report considers test events for the preceding fiscal year and calendar year (CY) in order for the report to be as up-to-date as possible.

In this report for FY/CY11, DOT&E assesses BMDS progress, test adequacy, and characterizes the performance of the BMDS with respect to four threat classes: short-range, medium-range, intermediate-range, and intercontinental ballistic missiles. To aid the reader, a foldout of the threat class definitions and a summary of the progress demonstration levels by key characteristics is located inside the back cover of this report.

This report is comprised of an unclassified main text and three classified appendices. Section Two of the main text describes the BMDS and its constituent elements and sensors and the BMDS development/deployment concept. Section Three assesses the progress of the BMDS and each of its elements toward a demonstration of defensive capability. Section Four assesses the adequacy and sufficiency of the BMDS test program for FY/CY11. Section Five, together with classified Appendices A and B, characterizes the operational effectiveness, suitability, and survivability of the overall BMDS and its elements. Classified Appendix C provides an operational assessment of the European Phased Adaptive Approach (EPAA) Phase 1 architecture, for which the Missile Defense Agency (MDA) issued a technical capability declaration in December 2011.

This page intentionally left blank.

Section Two The BMDS

Description

In January 2002, the Secretary of Defense established the Missile Defense Agency (MDA) to develop an integrated, layered-engagement BMDS (Figure 2-1). In December 2002, the President directed the Secretary of Defense to deploy an initial set of BMDS capabilities beginning in 2004. The Secretary identified the MDA as the requirement-generating organization and exempted it from the Joint Capabilities Integration and Development System and Department of Defense standard acquisition processes. Thus, with the exception of Patriot (which the MDA has already transitioned to the U.S. Army), MDA-produced documents, rather than user-produced and Joint Staff-approved documents, reflect the BMDS specifications in lieu of requirements.



Figure 2-1. Integrated, Layered-Engagement BMDS

The BMDS mission is to protect the United States, deployed forces, allies, and friends against ballistic missiles of all ranges and in all phases of flight. The MDA and the intelligence community group ballistic missile threats by range:

- Short-Range Ballistic Missile (SRBM) (less than 1,000 kilometers)
- Medium-Range Ballistic Missile (MRBM) (1,000 to 3,000 kilometers)
- Intermediate-Range Ballistic Missile (IRBM) (3,000 to 5,500 kilometers)

- Intercontinental Ballistic Missile (ICBM) (greater than 5,500 kilometers).

There are two potential missile types. One type is non-separating, i.e., the warhead payload, referred to as a reentry vehicle, and the rocket body remain attached throughout the entire missile flight. The second type is separating, in which the reentry vehicle separates from the missile body. Some missile threats employ a post-boost vehicle that separates from the rocket body and then reorients to fine-tune the reentry vehicle trajectory before ejecting the reentry vehicle. These missiles are referred to as complex separating threats. If no post-boost vehicle is employed, then the missile is referred to as a simple separating threat. All IRBMs and ICBMs are either simple or complex separating missiles. SRBMs and MRBMs can be either non-separating, simple separating, or complex separating missiles.

The MDA describes the defenses in terms of four phases of threat missile flight:

- Boost – from launch to booster burnout
- Ascent – from booster burnout to apogee
- Midcourse – flight above the Earth’s atmosphere (exoatmospheric) between apogee and reentry into the Earth’s atmosphere (endoatmospheric)
- Terminal – from reentry into the Earth’s atmosphere to impact.

To carry out the mission of countering ballistic missile threats in all stages of their trajectories, the BMDS is designed to combine the weapon and sensor capabilities of many different elements with a command and control element to create an integrated layered architecture.¹

BMDS Architecture

The BMDS architecture is a distributed system currently comprising the following elements and sensors.

Aegis Ballistic Missile Defense (Aegis BMD)



The Aegis BMD element is designed to provide U.S. Navy destroyers and cruisers with the capability to defeat SRBMs and MRBMs (and eventually IRBMs and ICBMs) during terminal or ascent/midcourse phases of flight. It also provides surveillance and tracking of ICBMs in support of the Ground-based Midcourse Defense (GMD) element. Aegis BMD consists of a shipboard Aegis Weapon System equipped with a modified S-band AN/SPY-1 radar, Standard Missile-2 (SM-2) interceptors for terminal defense, SM-3 interceptors for ascent/midcourse defense, and an Aegis vertical launcher

¹ An element is a complete, integrated set of subsystems capable of accomplishing an operational role or function. An integrated layered architecture is one that consists of several weapons that operate at various phases in the trajectory of a ballistic missile threat. Thus, there could be a first layer (for example, boost phase) with any remaining targets being passed on to succeeding midcourse and terminal phases. Critical to this layered defense is a command, control, battle management, and communications capability to integrate all the sensors and weapons for efficient and effective defense.

system. Aegis BMD enables simultaneous ship self-defense and BMD missions. The MDA transitioned an initial Aegis BMD build (Aegis BMD 3.6) to the U.S. Navy in October 2008; the Aegis BMD 3.6.1 build is currently deployed. In FY09, the President approved a phased, adaptive approach for missile defense of Europe using variants of the SM-3 in sea- and land-based modes. In December 2011, the MDA issued a technical capability declaration for the EPAA Phase 1 architecture. In support of the Phase 1 mission, Spain has agreed to allow four U.S. Navy Aegis BMD ships to be permanently stationed at the country's Rota Naval Base beginning in 2013.

Ground-based Midcourse Defense (GMD)

The GMD element is designed to defend the United States against IRBMs and ICBMs from North Korea and ICBMs from Iran. GMD consists of three-stage Ground-Based Interceptors (GBI) emplaced in silos located at Fort Greely, Alaska, and Vandenberg Air Force Base (AFB), California; GMD Fire Control at both Fort Greely, Alaska, and the Missile Defense Integration and Operations Center, Schriever AFB, Colorado; In-Flight Interceptor Communication System (IFICS) Data Terminals; a distributed GMD communications network; and external interfaces to the BMDS. A two-stage GBI is also under development. GMD uses sensor data provided by the Space-Based Infrared System/Defense Support Program (SBIRS/DSP), BMDS radars, and Aegis BMD. GMD is operated by Soldiers of the 100th Missile Defense Brigade, Colorado Army National Guard, and the 49th Missile Defense Battalion, Alaska Army National Guard.



Patriot

The U.S. Army Patriot air and missile defense system protects deployed forces and critical assets from SRBMs and MRBMs during terminal flight, and from air-breathing threats such as cruise missiles and aircraft. A Patriot battery includes an Engagement Control Station and Battery Command Post for battle management, a C-band phased array radar, and launchers with either hit-to-kill Patriot Advanced Capability-3 (PAC-3) missiles or older blast fragmentation PAC-2 missiles and PAC-2 Guidance Enhanced Missiles. The MDA transitioned Patriot to the U.S. Army in 2002. Patriot continues to undergo evolutionary development upgrades and testing, with major system Post-Deployment Builds (PDB) occurring approximately every 3 years.



Terminal High Altitude Area Defense (THAAD)

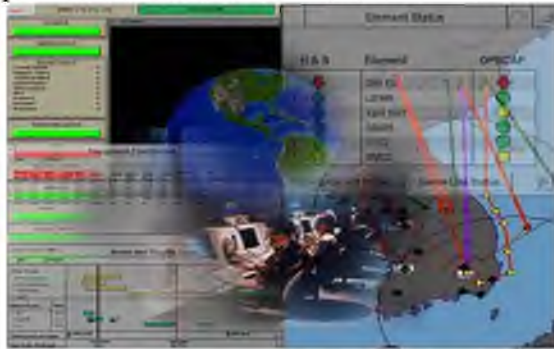
The THAAD element is designed to provide terminal-phase protection of forward-deployed forces, allies, and friends from SRBMs and MRBMs. A THAAD fire unit currently consists of 24 interceptors, three launchers, an Army Navy/Transportable Radar Surveillance (AN/TPY-2) X-band phased-array radar in its Terminal Mode (TM), THAAD Fire Control and Communications (TFCC), and associated



support equipment. The THAAD interceptor is designed to negate missiles in the mid endo-through low exo-atmosphere, providing terminal-phase, upper-tier defense to complement the Patriot lower-tier system. A materiel release decision for the first two THAAD fire units is scheduled for February 2012, which, if successful, will allow THAAD to be operationally deployable for the first time.

Command, Control, Battle Management, and Communications (C2BMC)

The C2BMC element is intended to evolve to manage and integrate globally the many sensors, interceptors, and other components that comprise the BMDS, and to provide situational awareness and planning capability. The current C2BMC hardware/software configuration provides situational awareness for the entire BMDS and command and control of the AN/TPY-2



X-band phased-array radar in its Forward-Based Mode (FBM). The C2BMC element is a networked system consisting of four types of certified sub-systems: C2BMC suites, Enterprise and Global Engagement Manager (GEM) Workstations, Communications Node Equipment, and Air Defense Systems Integrator. The primary C2BMC sites at the Combatant Commands – U.S. Central, European, Northern, Pacific, and Strategic

Commands – contain Command and Control (C2) and GEM suites. Additional workstations are located at numerous U.S. Army Air and Missile Defense Commands, Air and Space Operations Centers, and other allied warfighter organizations. C2BMC suites are connected to the host facility at the site technical control facility. This facility also houses the Communications Node Equipment and Air Defense Systems Integrator for each supported Combatant Command. C2BMC is also available via a Secret Internet Protocol Router Network (SIPRNet) C2BMC web browser to authorized users.

The Ballistic Missile Defense Communications Network ensures commanders have access to the information and data required to execute the BMD mission. It provides the infrastructure that physically connects all assets (sensors, weapons, and command and control) into an integrated missile defense system. The Ballistic Missile Defense Communications Network includes all physical and logical links providing BMDS data and voice communications. These links might be carried by numerous distinct communications systems including, but not limited to, military and commercial satellite communications, Defense Information System Agency-provided services, terrestrial leases, and the SIPRNet. The Ground-based Midcourse Communications Network, C2BMC Communication Network, and the Joint Data Network are the primary elements that comprise the Ballistic Missile Defense Communications Network.

Sensors

Aegis BMD AN/SPY-1 Radar

The Aegis BMD AN/SPY-1 radar is the Aegis Weapon System S-band phased-array radar (four faces, 360-degree



azimuth field of view) with hardware and software modifications designed to support surveillance and tracking of ballistic missiles in support of GMD. The AN/SPY-1 radar also supports both SM-2 and SM-3 engagements. The fielded radars are installed in guided missile cruisers and destroyers of the Atlantic and Pacific Fleets.

AN/TPY-2 Terminal Mode (TM) and Forward-Based Mode (FBM) Radars



The AN/TPY-2 radar is an X-band, phased-array radar (130-degree azimuth field of view) developed for the THAAD program. In TM, the radar is a part of the THAAD element, functioning as the primary sensor. In FBM, the radar has modified software to provide forward-based acquisition and tracking of ballistic missiles of all ranges in the boost phase through transition to the midcourse phase. In FBM, the radar relies on C2BMC to set search plans, prioritize, process, and distribute track data to other BMDS elements, including coalition partners. The AN/TPY-2 radar can be used in either TM or FBM, but not at the same time. Different software versions control the radar in different modes, and setup and calibration time is required to transition the radar between modes. Additionally, the different modes provide separate interfaces into the BMDS command and control architecture. In 2006, the MDA deployed the first AN/TPY-2 (FBM) to Shariki, Japan, and in 2008, the MDA sent a second AN/TPY-2 (FBM) to Israel. In 2011, the MDA delivered a third AN/TPY-2 (FBM) to Turkey as part of the EPAA Phase 1 architecture. Other AN/TPY-2 radars are currently slated for the first THAAD fire units, part of the THAAD ground and flight test programs, and in integration and test for advanced FBM capabilities.

Cobra Dane Radar

The Cobra Dane radar is an L-band, single-face (120-degree azimuth field of view) phased-array radar located at Shemya, Alaska, with hardware and software upgrades to support BMD. Cobra Dane is one of the principal radar sensors used to develop the GMD weapon task plan and in-flight target updates for North Korean IRBM and ICBM threats targeting Alaska and the continental United States. The U.S. Air Force operates the Cobra Dane radar.



Sea-Based X-Band (SBX) Radar

The SBX radar is an X-band, single-face, phased-array radar on a movable mount that can position through 270 degrees azimuth. It is installed on a twin-hulled, semi-submersible, self-propelled ocean-going platform and is designed to support operational and test missions throughout the Pacific Ocean. The SBX radar is intended to serve as a primary midcourse sensor for the BMDS performing high resolution cued search, acquisition, tracking, and target discrimination. Beginning in



FY13, the SBX will only be used for contingency operations and limited testing.

Space-Based Infrared System/Defense Support Program (SBIRS/DSP)

SBIRS/DSP is an infrared satellite sensor system consisting of a mix of geosynchronous earth orbit and legacy DSP satellites, payloads in highly elliptical earth orbit, and associated ground hardware and software that provide the BMDS with the initial notification of a ballistic missile launch and defended area threatened. The MDA declared a SBIRS/DSP active interface operational in February 2007, enabling C2BMC and the GMD Fire Control to receive early warning data directly from SBIRS/DSP instead of through the GMD communications network.



Upgraded Early Warning Radars (UEWR) – Beale, Fylingdales, and Thule



The UEWRs are ultra-high frequency fixed-site, fixed-orientation, phased-array radars located at Beale U.S. Air Force Base, California (two faces, 240-degree azimuth field of view); Fylingdales, United Kingdom (three faces, 360-degree azimuth field of view); and Thule, Greenland (two faces, 240-degree azimuth field of view). The radars are used to detect, track, and classify ballistic threats targeting the United States. The Beale, Fylingdales, and Thule UEWRs are designed to provide radar coverage for portions of the United States threatened by North Korean and Iranian threats. The radars perform both the BMD and legacy missile warning and space tracking missions.

Future Capability Development

The MDA plans to evolve the BMDS architecture through development of new capabilities in a phased approach in concert with projected threat development and deployment timelines and quantities. A primary objective of this capability development effort is to provide an early intercept capability to increase the flexibility of targeting opportunities by intercepting and destroying ballistic missiles early in flight. Developed systems might also enhance capabilities for intercept in the later stages of flight.

In consultation with Department of Defense leadership, the MDA intends to transition these future capabilities to the BMDS technical baseline. The current BMDS test program, as documented in the BMDS Integrated Master Test Plan, employs test beds for future capability technology demonstration and data gathering. Some of these future capabilities and associated test beds are described briefly below.²

² Ballistic Missile Defense System Integrated Master Test Plan (IMTP), Version 11.2, Missile Defense Agency, August 10, 2011.

Weapons

Aegis Ashore

Aegis Ashore is a future land-based Aegis BMD weapon system with associated AN/SPY-1 radar deckhouse, vertical launching system, and upgraded Aegis BMD combat system and SM-3 missiles. The MDA will incorporate Aegis BMD and SM-3 upgrades into both Aegis Ashore facilities and deployed Aegis BMD ships. The land-based system is designed to be transportable to support worldwide deployment.

The Aegis Ashore Test Center at the Pacific Missile Range Facility, Hawaii, will serve as the Aegis Ashore test bed. This test bed will be a land-based Aegis BMD element consisting of a four-faced AN/SPY-1 radar, SM-3 missile and launch system, satellite Link 16 communication equipment, and other necessary Aegis BMD combat system equipment and computer programs. The MDA plans for this test facility to be operational in 2014 to support development, integration, and test of the Aegis Ashore capability.

Aegis BMD Builds 5.1/5.1x

Future Aegis BMD capabilities are designed to provide midcourse defense against longer-range ballistic missiles and enhanced terminal defense against SRBMs and select MRBMs. Aegis BMD 5.1 will use the SM-3 Block IIA missile to enable midcourse engagement capability against SRBMs, MRBMs, and IRBMs. Aegis BMD 5.1x will use the SM-3 Block IIB missile to extend the Aegis BMD midcourse engagement capability to a broader range of IRBMs and ICBMs. These Block II missile variants will leverage the increased speed, maneuverability, and range of the SM-3 family of interceptors to facilitate an early intercept capability against MRBMs, IRBMs, and ICBMs. Aegis BMD 5.1 will also use the SM-6 interceptor to provide an enhanced sea-based terminal capability beyond the current near-term sea-based terminal (SM-2 Block IV based) capability.

Sensors

Airborne Infrared (ABIR) Sensors

The ABIR sensors effort is intended to use existing unmanned aerial vehicles, like the RQ-4 Global Hawk and the RQ-9 Reaper, modified to carry sensors to detect ballistic missiles in early stages of flight. Ground control stations will forward tasking to the aerial platforms and relay detection and tracking messages to C2BMC for engaging ballistic missile threats. In FY11, ABIR sensors collected data during five BMD flight test events. The MDA is currently reviewing the ABIR program for possible termination.

Precision Tracking Space System (PTSS)

PTSS is a planned low-Earth-orbit satellite constellation for visible and infrared tracking of ballistic missiles from post-boost through re-entry, including midcourse tracking in the long-wavelength infrared spectrum. It is intended to provide a space node to support tracking of MRBMs, IRBMs, and ICBMs, from post-boost through re-entry based on boosting tracks provided to PTSS by other space-based assets. PTSS will provide sensor track data to C2BMC for the generation of engagement quality tracks. Initially, PTSS will support SM-3 engagements, and the MDA will later develop the support for engagements using other interceptors.

The Space Tracking and Surveillance System (STSS) demonstrator program supports the development and fielding of PTSS. The two STSS satellites launched in FY09 provide a risk reduction test platform for PTSS for up to 4 years. In FY11, STSS collected data during five BMD flight test events.

Advanced C2BMC

Advanced C2BMC includes upgrades to integrate ABIR sensors and PTSS, advanced algorithms, and functionality for interceptor launch during threat missile boost phase and other early intercept enablers. In support of early intercept, the MDA plans to develop an Enhanced C2BMC test bed for algorithm testing. It will be used for off-line analysis of data gathered in test events and will support development of the Advanced C2BMC.

BMDS Development/Deployment Concept

Phased Adaptive Approach: European Defense

From March 2009 through January 2010, the Department of Defense conducted a comprehensive review of U.S. BMD policies, strategies, plans, and programs, as mandated by Congress and guided by Presidential directive. This 2010 Ballistic Missile Defense Review sought to align the U.S. missile defense posture with the near-term regional ballistic threat while sustaining and technically enhancing the U.S. ability to defend the homeland against a limited long-range attack. The Secretary of Defense delivered the 2010 Ballistic Missile Defense Review report to Congress on February 1, 2010. The report described the steps proposed by the Administration both to defend the homeland and to address threats to U.S. forces overseas, allies, and partners. To help facilitate regional integration, the report concluded that the United States should work with allies and partners to strengthen regional deterrence architectures; pursue a phased, adaptive approach to missile defense within each region that is tailored to the threats and circumstances unique to that region; and develop capabilities that are mobile and transportable.

The MDA has adopted the phased, adaptive approach for the development/deployment of the BMDS and chose Europe as its initial focus. For the defense of Europe, the MDA has adopted a four-phased, adaptive approach as outlined in the 2010 Ballistic Missile Defense Review report. While further technology advances or future changes in the threat could modify the details or timing of later phases, current plans, as documented in the BMDS Integrated Master Test Plan, call for the following:

- Phase 1 (2011 time frame): Deploy existing missile defense systems to defend against SRBMs and MRBMs. Phase 1 focuses on the protection of portions of southern Europe by utilizing the sea-based Aegis Weapon System 3.6.1, the SM-3 Block IA interceptor, C2BMC Spiral 6.4, and sensors such as AN/TPY-2 (FBM) to provide track data early in the engagement. Phase 1 also augments homeland defenses with the utilization of forward-based sensors and has THAAD available for deployment. Testing of Phase 1 regional defense capabilities against SRBMs and MRBMs was conducted in 2011. (See Appendix C for the DOT&E EPAA Phase 1 Operational Assessment.)

- Phase 2 (2015 time frame): Deploy the more capable SM-3 Block IB interceptor and make greater use of external sensors to expand the defended area against SRBMs and MRBMs. Phase 2 will include both sea- and land-based (Aegis Ashore) Aegis Weapon System 4.0.1/5.0 configurations, expanding coverage to additional North Atlantic Treaty Organization (NATO) allies. Phase 2 will support a more robust launch-on-remote sensor capability, improving defended area and capabilities against larger raid sizes.³ Phase 2 will culminate in an Operational Test and Evaluation of strategic and regional defense capabilities against SRBMs, MRBMs, and IRBMs.
- Phase 3 (2018 time frame): Deploy the more advanced SM-3 Block IIA variant, the Aegis Weapon System 5.1, and PTSS and ABIR sensors to enable engage-on-remote sensor capability to counter SRBMs, MRBMs, and IRBMs.⁴ Additionally, deploy a more advanced Aegis fire control system to optimize the SM-3 engagement space. Phase 3 will include an additional Aegis Ashore site to extend coverage to all NATO allies in Europe and to accommodate larger raid sizes. Phase 3 will culminate in an Operational Test and Evaluation of strategic and regional defense capabilities against SRBMs, MRBMs, IRBMs, and ICBMs.
- Phase 4 (2020 time frame): Deploy the more advanced SM-3 Block IIB and Aegis Weapon System 5.1x to better cope with MRBMs and IRBMs and the potential future ICBM threat from the Middle East to the United States. Phase 4 will culminate in an Operational Test and Evaluation of strategic and regional defense capabilities against SRBMs, MRBMs, IRBMs, and ICBMs.

All four phases will include upgrades to the missile defense command and control system. C2BMC will integrate with the existing combatant command architecture resulting in a progression from situational awareness and track forwarding to actual battle management.

U.S. Homeland Defense

Military operators for the U.S. Army Space and Missile Defense Command/U.S. Army Forces Strategic Command, which is the U.S. Army Service component to U.S. Strategic Command, can use the deployed GMD element to defend the U.S. Homeland against IRBM and ICBM attacks using the GBI to defeat threat missiles during the midcourse segment of flight. The EPAA Phase 4 architecture will augment GMD capabilities against ICBM threats from the Middle East to the U.S. Homeland.

³ Launch-on-remote refers to engagement operations that require weapon systems to use sensor data for launch that is not from their organic sensor(s).

⁴ Engage-on-remote refers to engagement operations that require weapon systems to use sensor data for launch or full engagement that is not from their organic sensor(s).

This page intentionally left blank.

Section Three

BMDS Progress Towards Threat Class Capabilities

The breadth of the BMDS mission and the varying levels of maturity for the individual BMDS elements are such that a single assessment of overall BMDS progress toward achieving an integrated layered ballistic missile defense is not possible at this time. To overcome this problem, the FY09 version of this report presented the BMDS mission in MDA-defined threat-based campaigns and assessed campaign-level progress. The FY10 version of this report rated the level of demonstrated progress against the threat classes, vice the FY09 MDA threat-based campaigns. The threat class-based approach is continued in this report. Progress is reported first, for the overall integrated layered BMDS, second, by individual weapon elements within each threat class, and third, by battle management.

Progress Demonstration Levels

The MDA defines its Effectiveness Metrics Standard in terms of the probability of engagement success, launch area denied, defended area, raid size capability, and operational area.⁵ The weapon elements (Aegis BMD, Ground-based Midcourse Defense (GMD), Patriot, and THAAD) are the only complete, integrated sets of BMDS subsystems measureable in terms of these performance metrics. The sensor components and battle management element (Command, Control, Communications, and Battle Management [C2BMC]), while important contributors to an overall defense, play an enabling role to the weapon elements. For this reason, progress for only the weapon elements is assessed in this section.

This report measures BMDS and threat-class defense progress in terms of six levels defined by the manner in which the capabilities against the threat classes have been demonstrated. Table 3-1 provides a summary of these progress demonstration levels from highest to lowest, as well as a color code for each demonstration level. The level definitions, as written, apply to both overall BMDS progress and threat-class defense progress, which are each treated separately in this report. Note that these levels, with the exception of the top level (Level 6), do not take into account inventory (number of interceptors, radars, etc.). Only the top level, as discussed below, requires sufficient inventory to provide a credible and sustained combat capability. Note also that achieving the two highest progress demonstration levels (Levels 5 and 6) does not imply that the BMDS/threat-class defense has achieved its performance or effectiveness goals. The discussion of BMDS/threat-class defense performance and effectiveness is provided in Section Five and classified Appendices A and B of this report. The remaining progress demonstration levels (Levels 1 through 4) address the types of BMDS/threat-class defense testing that have been performed, from least to most technically rigorous and operationally realistic. These four demonstration levels are partly defined by the type of testing accomplished, but they do not address the adequacy of this testing. The discussion of test adequacy is deferred to Section Four.

⁵ Ballistic Missile Defense System Effectiveness Metric Standard, April 6, 2009.

Table 3-1. BMDS/Threat-Class Defense Progress Demonstration Levels

Level	Description
6	BMDS/threat-class defense capability verified through integrated, operational flight testing, and independently accredited ground testing and/or models and simulations. The demonstrated capability fulfills the defined threat-class defense/weapon element requirements and is fully integrated into the BMDS/threat-class defense. Sufficient inventory is deployed to provide a credible and sustained combat capability.
5	Broad, but incomplete, demonstration of threat class-defense/weapon element capabilities through independently accredited ground testing and/or models and simulations. Accreditation is possible only if a sufficient quantity and quality of operational flight test data have been collected to support model verification and validation ⁶ . Limited combat operations are possible with existing inventories.
4	Specific/limited threat-class defense/weapon element capabilities demonstrated through operationally realistic intercept flight testing with the full set of operational components. Flight testing emphasizes operational objectives over developmental objectives. Ground testing and/or models and simulations need not be independently accredited and may be used for preliminary assessments. Emergency combat operations are possible with existing inventories.
3	Specific/limited threat-class defense/weapon element capabilities demonstrated through flight testing with key operational components. Flight testing emphasizes developmental objectives over operational objectives. Flight test data obtained are expected to contribute to independent accreditation of models and simulations used for assessing performance.
2	Specific threat-class defense/weapon element capabilities demonstrated through developmental flight testing with developmental or legacy system hardware/software. The flight test data obtained support the development of engineering versions of models and simulations.
1	Threat-class defense/weapon element concept defined with capabilities estimated through analysis, laboratory testing, and/or legacy system models and simulations.

In general, these progress levels address the quality of BMDS/threat-class defense testing. More detailed descriptions of the progress levels are provided below.

Level 1, the lowest level of threat-class defense/weapon element progress demonstration, is achieved through analysis, laboratory testing, and/or legacy system models and simulations. Such demonstrations provide a proof-of-concept that a desired threat-class defense/weapon element capability is possible.

Level 2, the next higher level of threat-class defense/weapon element progress demonstration, is achieved through flight testing with developmental or legacy system hardware/software. It includes flight testing incorporating only components or sub-systems of the BMDS/threat-class defense. A complete developmental system is not a prerequisite for achieving Level 2.

⁶ Accreditation is the official certification by an independent accrediting agency that a model or simulation is acceptable for a specific application or purpose. Verification is the process of determining that a model or simulation implementation accurately represents the developer's conceptual description and specifications. Validation is the process of determining the degree to which a model or simulation is an accurate representation of the real world from the perspective of the intended uses of the model.

Level 3, a higher level of threat-class defense/weapon element progress demonstration, exists when key components (e.g., the interceptor, sensor(s), and fire control software) under test are representative of the intended operational configuration. If the components under test are not representative of the intended operational configuration, the capability is not considered to be demonstrated at Level 3. Flight testing at this level incorporates developmental testing (DT) combined with operational testing (OT), or combined DT/OT. Flight testing can incorporate some operational objectives, but the emphasis and priority is on developmental objectives. At this level, limited inventories of hardware and software might be procured for additional testing, but their developmental nature will restrict their operational use. The three levels discussed thus far are insufficient to demonstrate that an operationally useful, threat-class defense capability exists.

Level 4 is a significant milestone in the development of a threat-class capability and consists of operationally realistic intercept flight testing with the intended operational components. This testing emphasizes and prioritizes operational objectives over developmental objectives. In addition, Level 4 includes ground tests and/or models and simulations to help assess the capability against the threat class. Because this level of demonstration occurs during the development phase, an independent agency such as the BMDS Operational Test Agency Team need not have accredited these ground tests and models and simulations for performance assessment purposes. Level 4 is the first level to demonstrate that an actual combat capability exists, although this capability might be rudimentary and is likely not very robust. Accordingly, only emergency combat operations could be attempted with this capability. Inventories are low, reliance on contractors is likely high, and deployability for extended periods of time is likely problematic. The suitability and survivability of this capability is probably unknown, and the effectiveness is likely estimated based on only a few flight tests. A threat-class defense/weapon element capability can be assessed at Level 4 for several years without connoting unsatisfactory progress, as the MDA collects verification and validation data to support accreditation of models and simulations by an independent agency. Such an accreditation is necessary for promotion to Level 5.

Level 5 is another significant milestone. It consists of a broad, but incomplete, demonstration of threat-class defense/weapon element capabilities using independently accredited ground tests and/or models and simulations. Such accreditations are possible only if a sufficient quantity and quality of flight test data have been collected to validate the models and simulations.⁷ These data are generally the result of operational testing but are supplemented with developmental testing. A credible threat-class-specific combat capability is demonstrated at this level, although it is likely somewhat limited. Estimates of effectiveness, suitability, and survivability can be expected at this level, although these estimates might be preliminary with correspondingly large uncertainties and therefore limited operational utility. The depth of the capability is not assessed here. That is, the necessary inventories might not be available for

⁷ Ground tests and models and simulations can be accredited for many purposes. Here, we mean that the ground tests and models and simulations have been accredited for performance assessment purposes.

sustained combat, or operationally useful capabilities for specific regions of the battlespace, defended area, or launch area denied might not be achievable with the currently demonstrated capability. However, for the parts of the battlespace, defended area, or launch area denied where the capability has been demonstrated, a moderately robust combat capability exists.

Level 6, the highest progress demonstration level, is a demonstration of integrated BMDS/threat-class defense capabilities through operational flight tests, independently accredited ground testing, and/or models and simulations across the entire battlespace. Sufficient inventory is deployed to provide a credible and sustained combat capability. Note that this level references BMDS/threat-class defense capabilities rather than individual weapon element capabilities. The weapon elements that contribute to overall BMDS/threat-class defense capabilities at this highest demonstration level, provide evidence that they do not degrade the capabilities of any other BMDS weapon element. For a weapon element to contribute to BMDS/threat-class defense capabilities at this level, integrated operational testing must demonstrate full integration with the BMDS/threat-class defense as well as the individual weapon element requirements.

Table 3-2 is a summary of the key characteristics of each progress demonstration level described in Table 3-1 and the preceding discussion. From the bottom at Level 1 to the top at Level 6, it depicts the deliberate increase in demonstrated performance and difficulty in achieving each level.

Table 3-2. Summary of Progress Demonstration Levels by Key Characteristics

Level	Accreditation of Models & Simulations	Demonstrated Capability	Hardware/Software Components	Fielding & Inventory	Testing
6	Independent Accreditation ⁸	Fulfills Defined Requirements	Full Operational Set with BMDS Integration	Sustainable Combat Operations	Integrated OT
5	Independent Accreditation ⁹	Broad but Incomplete	Full Operational Set	Limited Combat Operations	OT
4	Limited Accreditation	Specific/Limited/Operationally Realistic	Full Operational Set	Emergency Combat Operations	Combined dt/OT ¹⁰
3	No Accreditation Required	Specific/Limited	Key Operational Set	None	Combined DT/ot ¹¹
2	Engineering Models & Simulations	Specific	Developmental or Legacy	None	DT
1	Legacy Models & Simulations	Concept Only	Analysis, Labs, or Legacy	None	Lab

BMDS Progress

[Author note: Please refer to the foldout inside the back cover of this report for the remainder of Section Three.]

Table 3-3 shows the relationship between weapon elements under development, their designed intercept phase, and types of threats they will intercept in the specified phase of flight. In the case of Aegis BMD, the interceptor type is also shown.

⁸ Independent accreditation of integrated BMDS-level models is achieved at this level.

⁹ Independent accreditation of element-level models is achieved at this level. The element-level models need not be the same as the integrated BMDS-level models.

¹⁰ Testing emphasizes operational vice developmental test objectives, denoted as dt/OT.

¹¹ Testing emphasizes developmental vice operational test objectives, denoted as DT/ot.

Table 3-3. Element, Intercept Phase, and Threat Pairings

Element	Intercept Phase	Threat Type			
		SRBM	MRBM	IRBM	ICBM
GMD Fire Control (GFC) 6B	Midcourse			X	X
Aegis BMD 3.6.1	Midcourse (SM-3)	X	X	X	
	Terminal (SM-2)	X			
Aegis BMD 4.0.1	Midcourse (SM-3)	X	X	X	
	Terminal (SM-2/6)	X			
Aegis BMD 5.1/5.1x	Midcourse (SM-3)	X	X	X	X
THAAD Fire Control and Communications (TFCC) 5.2	Terminal	X	X		
Patriot Post Deployment Build (PDB) 6.5	Terminal	X	X		
Patriot PDB 7.0	Terminal	X	X		

Figure 3-1 compares the DOT&E assessment of demonstrated BMDS progress for FY10 with that of FY11. This figure is intended to show BMDS progress toward a demonstration of capability against the threat classes broken down by weapon element. The triangles represent the assessed threat-class status for SRBMs, MRBMs, IRBMs, and long-range or ICBM threats. For example, for Patriot, the highest level of demonstrated progress – Level 6 – has been achieved against short-range and medium-range threats that have been defined by requirements. The capabilities against each of the threat classes span several demonstration levels because the BMDS weapon elements providing these capabilities are at different levels of maturity.

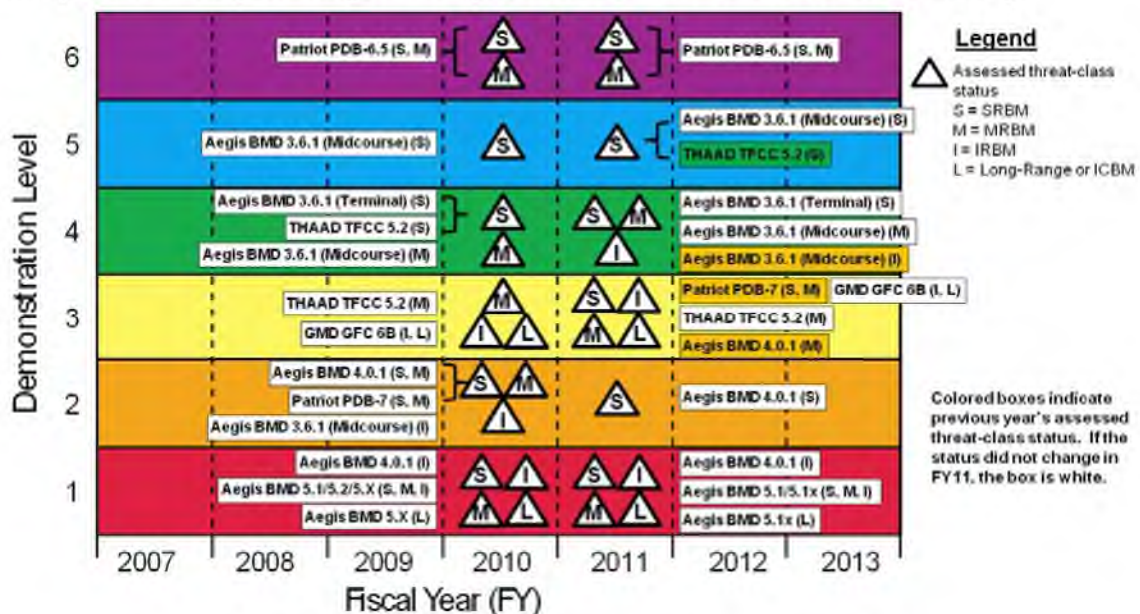


Figure 3-1. BMDS Progress Assessments for FY10 and FY11

The boxes containing the element names for the FY11 assessments are color-coded to indicate whether the assessed FY11 status has changed from FY10. White boxes indicate no change in assessed status, while colored boxes indicate that a change has occurred. The color of the box indicates the assessed progress demonstration level in FY10. For example, green filled boxes indicate that the element was assessed at the green (Level 4) level in FY10. Observe that in FY11, Aegis BMD 3.6.1 (Midcourse) and 4.0.1, THAAD TFCC 5.2, and Patriot PDB-7, all experienced increases in assessed status.

Aegis BMD 3.6.1 and Patriot PDB-6.5 are the currently deployed weapon elements providing BMDS capabilities against SRBMs and MRBMs. They are the most mature BMDS weapon elements and, accordingly, have demonstrated their capabilities against their assigned threat classes at Level 4 or higher. THAAD TFCC 5.2 is not currently deployed, although two fire units have been produced, and a materiel release decision is scheduled for February 2012. THAAD testing has primarily been against short-range threats, so its progress against SRBMs is higher than that against MRBMs. GMD is the least mature weapon element of the deployed BMDS and is assessed at a demonstrated progress level of 3. Elements rated at Levels 1 and 2 are mainly follow-on capabilities to existing BMDS weapon elements.

The GMD element does not strictly adhere to the progress level definitions given in Tables 3-1 and 3-2; the GMD element was deployed in 2004 as part of an Initial Defensive Operations concept capable of providing an emergency missile defense capability if needed. An inventory of GMD interceptors was purchased and deployed to provide this emergency capability before sufficient testing had been completed to quantitatively assess GMD effectiveness. To date, GMD testing has not demonstrated progress beyond Level 3 despite having a limited combat capability. Additional discussion of the GMD progress demonstration level is provided later in this section.

Threat-Class Defense Progress

Each of the demonstrated BMDS capabilities against the threat classes, as shown in Figure 3-1, is built primarily upon weapon element capabilities because only Level 6 requires the weapon elements to operate in a fully integrated fashion at the BMDS level. Although the MDA has made progress in integrating the BMDS weapon elements, most of the actual combat capability is still resident in the individual weapon elements, or perhaps in a loose federation of a few weapon elements. A fully integrated and coordinated BMDS combat capability that optimizes overall engagement planning and execution across all the threat classes in all phases of flight does not yet exist.

SRBM

Figure 3-2 shows the progress toward a demonstration of SRBM defense capability. Aegis BMD and THAAD provide short-range capabilities. Patriot also provides short-range capabilities, but because it is a U.S. Army program, rather than an MDA program, it is not included in Figure 3-2. It is discussed separately in this section. DOT&E first began assessing weapon element-level progress in terms of threat classes in FY09. The progress assessments

prior to FY09, shown as blue diamonds, represent DOT&E's retrospective assessment of assessed progress.

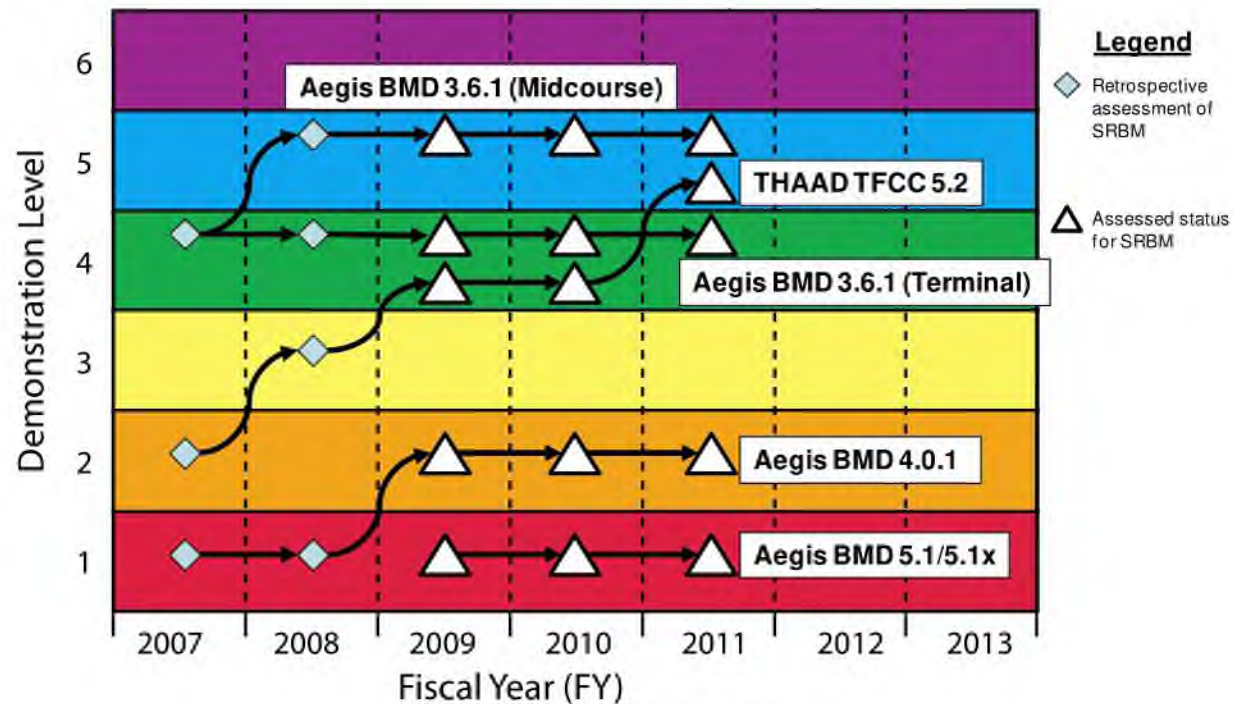


Figure 3-2. SRBM Progress

Aegis BMD 3.6.1 is the most mature deployed weapon element in Figure 3-2 at Level 5. THAAD has also demonstrated a Level 5 progress against SRBMs and completed an Initial Operational Test & Evaluation (IOT&E) flight test event in October 2011. Aegis BMD 3.6.1 includes midcourse-phase engagement capabilities with SM-3 Block IA interceptors and terminal-phase engagement capabilities with modified SM-2 Block IV interceptors. Aegis 4.0.1 is currently not deployed and provides no operational capability at this time. Aegis BMD 4.0.1 introduces enhanced midcourse-phase engagement capabilities with the addition of an advanced BMD signal processor and SM-3 Block IB interceptors. THAAD, which is designed to provide terminal-phase engagement capability, is currently not deployed. An Army Materiel Release decision for the first THAAD fire units is scheduled in February 2012, and if successful, will allow the first THAAD fire unit to be deployed. The following discussion focuses on the progress for each of the weapon elements (Aegis BMD, THAAD, and Patriot) that can provide defenses against SRBMs.

Aegis BMD Build 3.6.1

The MDA has demonstrated Aegis BMD 3.6.1 midcourse capabilities against SRBMs at Level 5, as shown in Figure 3-2. Level 6 is currently not warranted due to limited flight testing of SM-3 Block IA dual pulse mode of the third-stage rocket motor. Also, given the central role played by Aegis BMD 3.6.1 in the EPAA Phase 1 architecture, testing of Aegis BMD 3.6.1 capabilities at larger downrange and cross-range intercept locations is needed to verify the system's performance under all the operational scenarios that could arise in conducting European

missile defense. In addition, the SM-3 inventory continues to build up to sustainment levels. DT/OT testing of the Aegis BMD 3.6.1 midcourse capability is complete. The MDA has demonstrated Aegis BMD 3.6.1 sea-based terminal capabilities only at Level 4 because of limited flight testing and limited data available for a full accreditation of models and simulations. Unless additional Aegis BMD 3.6.1 terminal flight tests are performed and the associated models and simulations are accredited, the progress demonstration level of Aegis BMD 3.6.1 (terminal) will stay at Level 4.

Aegis BMD Build 4.0.1

Aegis BMD 4.0.1 is currently undergoing developmental testing and is not deployed. The Aegis BMD 4.0.1 system has not yet conducted a successful intercept flight test as part of DT, so it remains at a progress demonstration level of 2 in Figure 3-2. Level 2 is warranted due to participation in tracking events with simulated engagements against SRBM targets.

Aegis BMD Build 5.1/5.1x

Aegis BMD 5.1 and 5.1x, which both include the capability to engage SRBMs, are in early stages of development, and are thus assessed at Level 1 in Figure 3-2.

THAAD (TFCC 5.2)

The THAAD demonstration level against SRBMs progressed to Level 5, as shown in Figure 3-2. The THAAD program made progress toward SRBM defense in FY11 by completing Flight Test THAAD Interceptor-12 (FTT-12), which was designated an Operational Test. FTT-12 allowed THAAD to demonstrate new capabilities, but testing of some aspects of SRBM defense is still incomplete. A number of THAAD models and simulations achieved limited accreditation for performance against SRBMs from the U.S. Army Test and Evaluation Command. Production of THAAD components continued, and inventory levels are sufficient for limited combat operations.

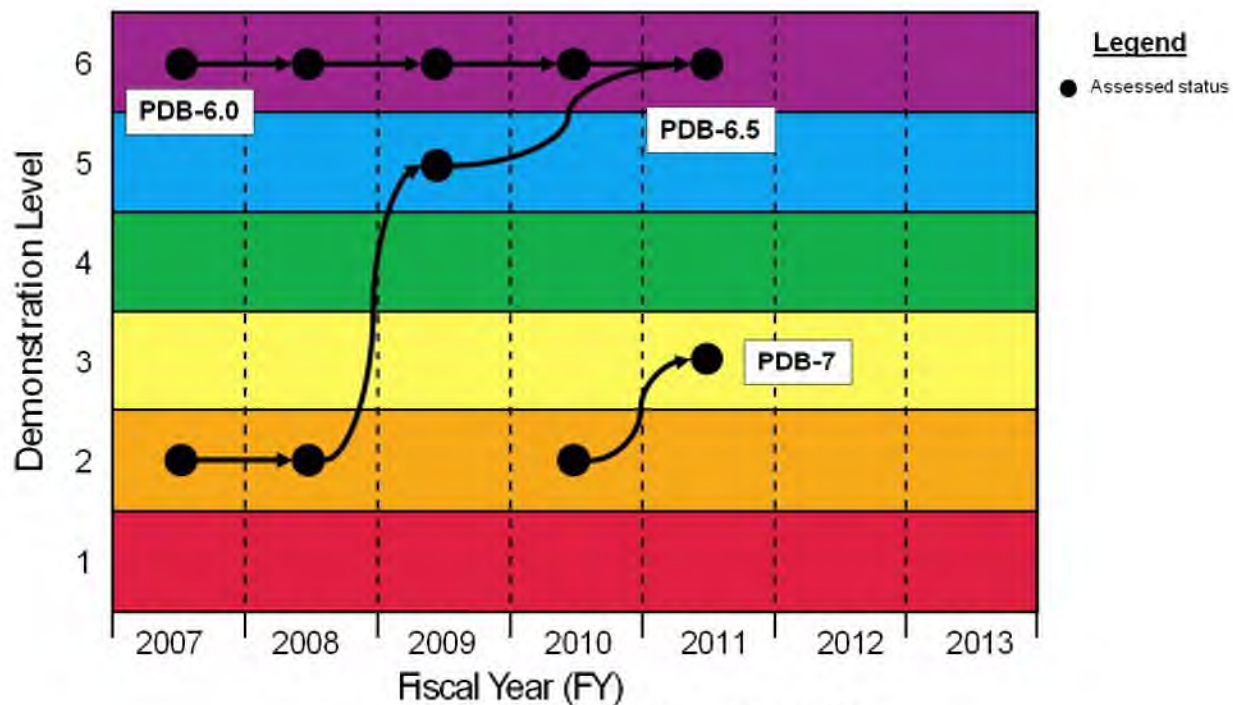


Figure 3-3. SRBM Progress for Patriot

Patriot (PDB 6.5)

Patriot was originally developed based on formal DoD operational requirements and is currently a fielded, operational system managed by the U.S. Army. The BMDS elements managed by the MDA are not currently subject to the formal DoD operational requirements management process. Since Patriot has been deployed for decades, its progress can be determined without resorting to retrospective analyses. The currently deployed version of Patriot is PDB-6.5, which has demonstrated progress at Level 6, as shown in Figure 3-3. PDB-7 is the follow-on build to PDB-6.5 and has demonstrated its capabilities at Level 3. This increase is due to PDB-7 developmental flight and ground testing conducted in 2011.

MRBM

Figure 3-4 shows the progress demonstrated against MRBMs for Aegis BMD and THAAD. Patriot also can engage MRBMs. However, Patriot's demonstrated progress against MRBMs is the same as for SRBMs (see Figure 3-3) and is not discussed further.

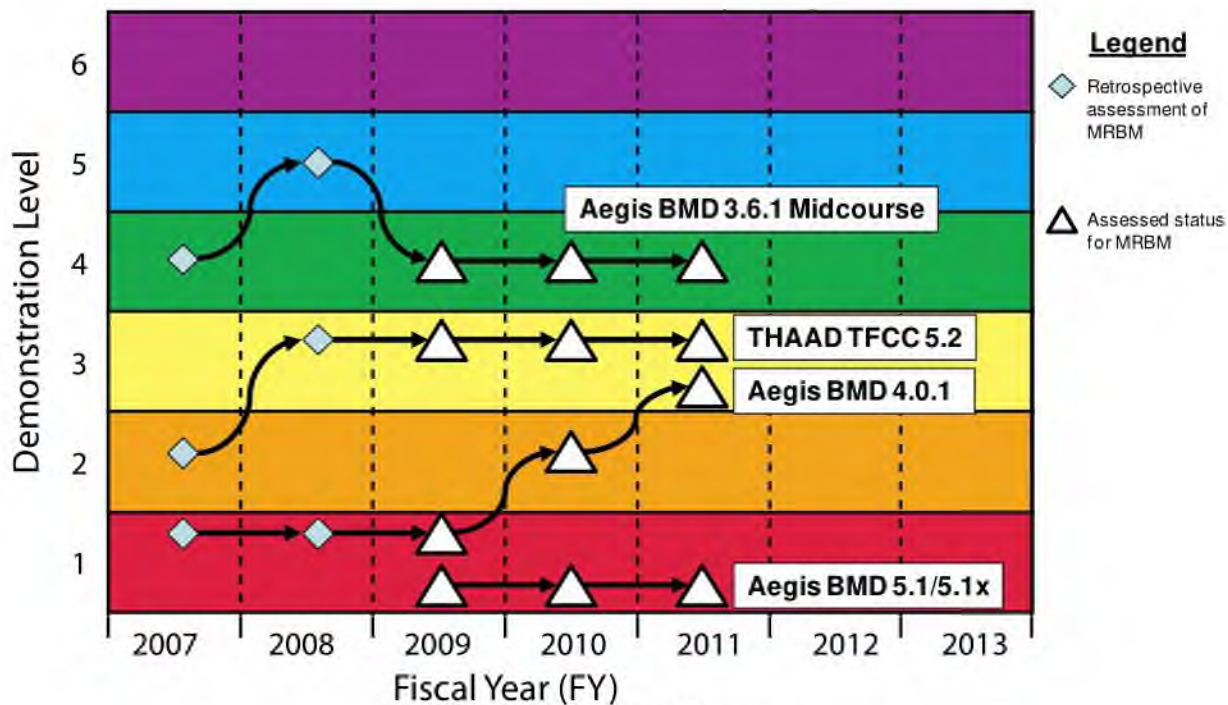


Figure 3-4. MRBM Progress

Aegis BMD Build 3.6.1

Figure 3-4 shows that the MDA has demonstrated Aegis BMD 3.6.1 midcourse capabilities at Level 4 against MRBM threats. Note that this demonstration of capability has been against targets flying maximum SRBM ranges with MRBM characteristics. However, Aegis BMD 3.6.1 has engaged an IRBM, as discussed subsequently. These targets are representative of those threats expected in the North Korean theater (with Aegis BMD operating primarily in the Sea of Japan) and the Middle Eastern theater (with Aegis BMD operating primarily in the Persian Gulf). Such threats represent only the lower-range threshold of MRBMs. In 2009, the EPAA introduced Iranian threats to the Aegis BMD 3.6.1 threat set as part of Phase 1. Prior to 2009, Aegis BMD 3.6.1 progress was measured against lower-range threshold MRBMs. Since the new EPAA architecture for European missile defense introduced Iranian threats to the Aegis BMD 3.6.1 threat set, the entire span of MRBM threat ranges must now be considered when assessing Aegis BMD demonstration of capabilities. Since the Aegis BMD program had not been flight tested against the upper-range threshold of MRBMs, the demonstration of progress for Aegis BMD 3.6.1 decreased from Level 5 to Level 4 in FY09. Since then, there have been no attempts to engage the upper range of MRBM threats in flight testing so the Aegis BMD 3.6.1 demonstrated progress remains at Level 4.

Aegis BMD Build 4.0.1

Aegis BMD 4.0.1 has participated in multiple tracking exercises and conducted simulated engagements against lower-range threshold MRBM-representative targets. Aegis BMD 4.0.1's participation in the FTM-16 Event 2 flight test resulted in its promotion to Level 3 in Figure 3-4. This promotion to Level 3 is based on the inclusion of key operational components, namely the

Aegis BMD 4.0.1 system (with a new BMD signal processor and system software) and SM-3 Block IB interceptor (with a new kinetic warhead divert system and seeker) in Event 2.

Aegis BMD Build 5.1/5.1x

Aegis BMD 5.1 and 5.1x, which both include the capability to engage MRBMs, are in the early stages of development and remain at Level 1 in Figure 3-4.

THAAD (TFCC 5.2)

THAAD progress against MRBMs remains at Level 3 in Figure 3-4 because the MDA has not flight tested THAAD against true MRBMs. Twice, THAAD has tested against a target with MRBM characteristics flying a maximum SRBM range. The MDA has scheduled a flight test providing information toward a true MRBM defense capability for FY12.

IRBM

Figure 3-5 shows the progress against IRBMs. GMD and Aegis BMD are the only two weapon elements that provide IRBM defenses. The FY09 version of this report included the THAAD weapon element as a participant in IRBM defense. In FY10, the MDA concluded that THAAD was not currently designed with the capability to intercept IRBMs and removed all THAAD flight tests against intermediate-range targets from the BMDS Integrated Master Test Plan. This report will therefore not track THAAD defense against IRBMs unless the MDA decides to reestablish testing of this capability.

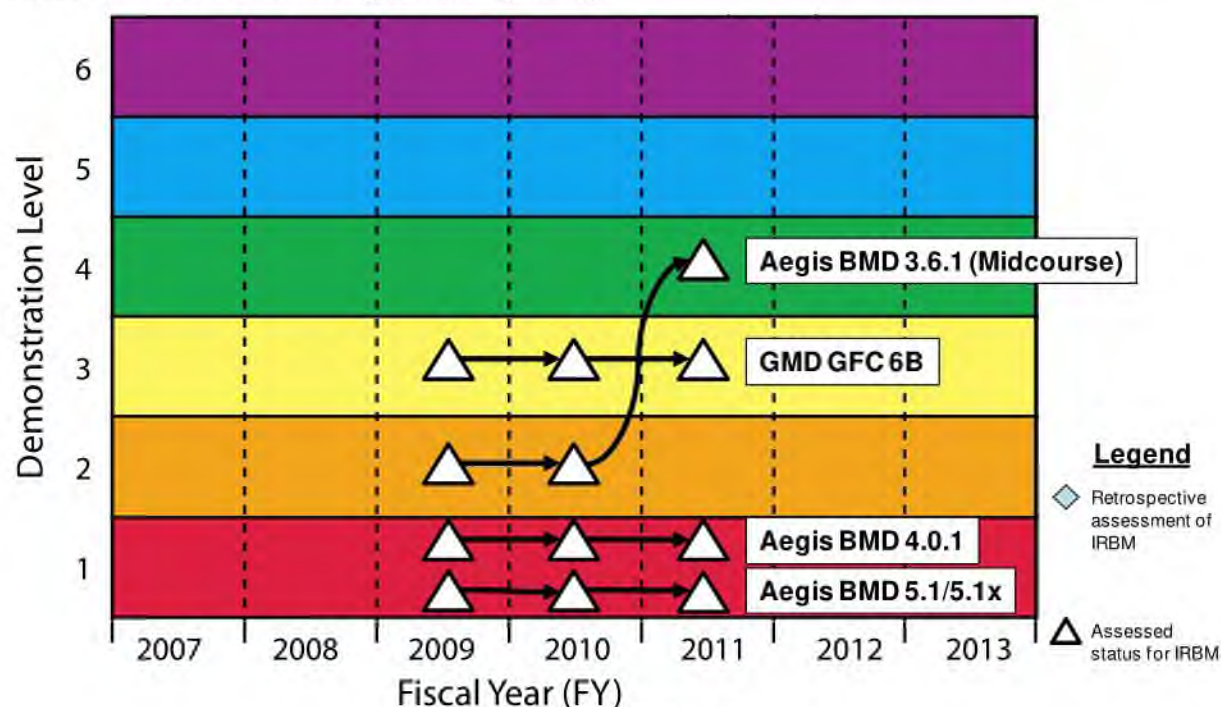


Figure 3-5. IRBM Progress

In FY11, a successful demonstration of defensive capability against IRBMs occurred with the Flight Test Standard Missile-15 (FTM-15) flight test of Aegis BMD 3.6.1. FTM-15 is Aegis BMD 3.6.1's only attempt to engage an IRBM target. The GMD program has demonstrated its IRBM capabilities three out of five times (the three successes were against an ICBM-like target launched at IRBM ranges), but since its interceptors are located at fixed sites, the number of IRBM threats it can operationally engage is extremely limited. Aegis BMD 3.6.1's mobility allows it to potentially engage a wider variety of threats.

The following discusses the capabilities GMD and Aegis BMD have demonstrated against IRBMs in greater detail. The current version of the GMD Fire Control (GFC) software is designated GFC 6B.

GMD (GFC 6B)

The GMD progress demonstration level against IRBMs remained unchanged (Level 3 in Figure 3-5) in FY11, primarily due to the nature of testing, which is mostly combined DT/ot. In FY10 and FY11, the MDA conducted two GMD intercept flight tests against IRBM targets.¹² Both tests employed advanced Capability Enhancement-II (CE-II) Exoatmospheric Kill Vehicles (EKVs). The first test resulted in a failure to intercept due to problems with both the SBX radar and the GBI. The second intercept flight test also resulted in a failure to intercept. The MDA convened a failure review board to determine the root cause. Results are discussed in Appendix A. The three prior GMD intercept flight tests using CE-I EKV's, which the MDA conducted for demonstration of a capability for defense of the United States against ICBMs, support the Level 3 assessment for GMD against IRBMs. The target ranges in these prior flight tests were representative of IRBM threat ranges, but the test scenario geometry, GBI flyout range, target suite, and sensor positioning for these flight tests were not representative of an IRBM threat engagement. Ground tests also support the Level 3 assessment for GMD against IRBMs; however, these ground tests employed models and simulations that were not accredited for performance assessment. Classified details are discussed in Appendix A.

Aegis BMD Build 3.6.1

With the addition of the European defense mission in 2009, a limited set of IRBMs is now a part of the Aegis BMD 3.6.1 threat set. Aegis BMD 3.6.1 demonstrated a capability against IRBMs in FTM-15, which was designated as an OT for Aegis BMD 3.6.1 (although it was not an OT for other FTM-15 participants).¹³ As a result, Aegis BMD 3.6.1 has been promoted to Level 4 in Figure 3-5.

¹² The target reentry vehicle emulated an ICBM threat reentry vehicle, but it was deployed from an IRBM.

¹³ FTM-15 used a subset of the assets (both sensors and shooters) expected in the EPAA Phase 1 architecture. Therefore, the complex interactions expected between the assets performing the European defense mission could not be fully tested in FTM-15. The progress assessment in Figure 3-5 refers to a more generic capability against IRBMs and not specifically to the European mission.

Aegis BMD Build 4.0.1

Aegis BMD 4.0.1 has conducted no testing against IRBM-class targets. Its progress demonstration level remains at Level 1 in Figure 3-5.

Aegis BMD Build 5.1/5.1x

Aegis BMD 5.1 and 5.1x, which include the capability to engage IRBMs, are in the early stages of development. This build continues to be assessed at Level 1 in Figure 3-5.

ICBM

Figure 3-6 shows the progress against ICBMs. GMD is the sole weapon element that currently provides any capability against ICBMs. Aegis BMD 5.1x is planned to engage ICBMs in the future.

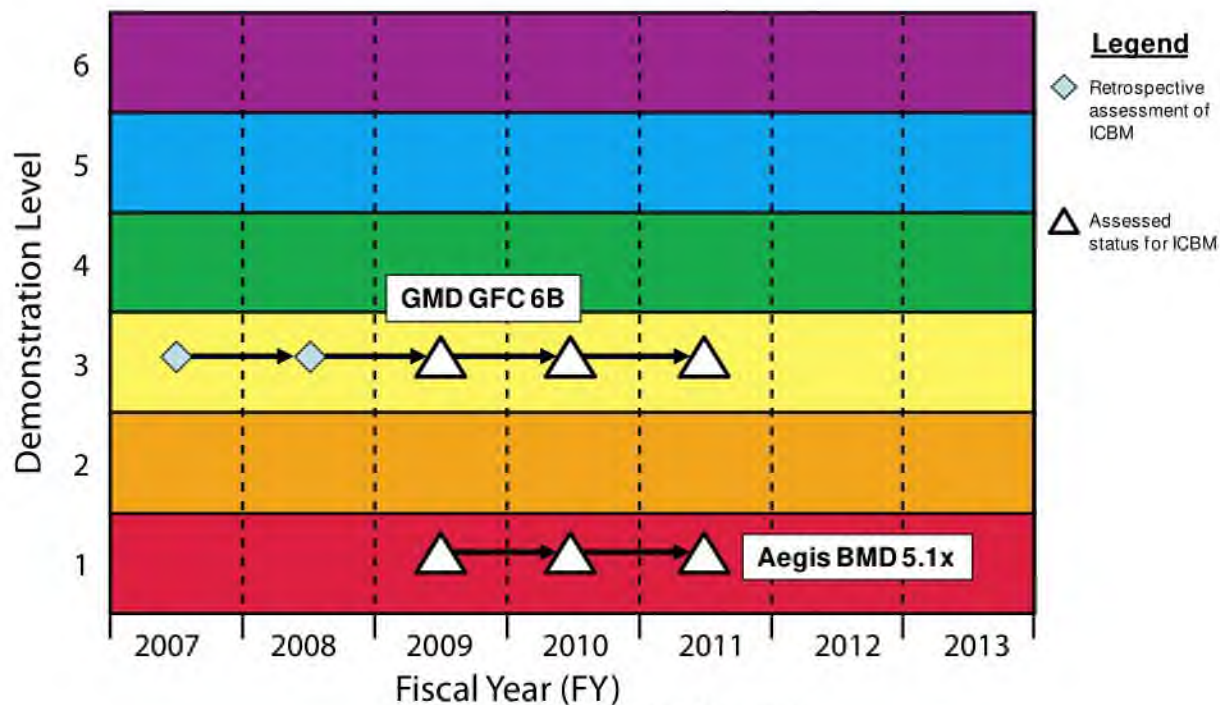


Figure 3-6. ICBM Progress

GMD (GFC 6B)

The GMD progress demonstration level against ICBMs remains unchanged (Level 3 in Figure 3-6) in FY11, primarily due to the nature of testing, which is mostly combined DT/ot. The MDA did not schedule an intercept flight test against an ICBM target in FY/CY11. In FY10 and FY11, the MDA conducted intercept flight tests against IRBM targets (replicating ICBM endgame performance characteristics), which would have supported a GMD capability demonstration assessment against ICBMs; however, both tests failed to intercept and failed to achieve their full set of test objectives. Both tests employed CE-II EKV. In the three prior flight tests against ICBM-class targets (FY06-09) using CE-I EKV, the MDA employed an

operationally representative Ground-Based Interceptor (GBI) and progressively increased operational realism in test.¹⁴ All three of these tests resulted in target intercepts. Ground tests also support the Level 3 assessment for GMD against ICBMs; however, these ground tests employed models and simulations that were not accredited for performance assessment.

Aegis BMD

Aegis BMD 5.1x is planned to have a capability to engage a set of ICBMs and is in the early development stage (Level 1 in Figure 3-6). Aegis BMD 5.1 (not shown), also in early development, might provide a potential capability against a limited set of ICBMs.

BMDS Battle Management Progress

Battle management functionality is essential for a fully integrated and coordinated BMDS engagement capability. While the MDA has made progress toward full integration, the engagement planning and execution capability across all threat classes and phases of flight does not yet exist. BMDS battle management includes engagement planning, sensor management, track forwarding, sensor-weapon system pairing, and BMDS engagement direction. C2BMC is the element that is planned to perform global battle management, while BMD weapon elements retain element-level battle management and fire control functionality. In June 2011, C2BMC Spiral 6.4 (S6.4) replaced Spiral 6.2 (S6.2) as the operational version of C2BMC software at U.S. Northern, Pacific, and Strategic Commands. In December 2011, S6.4 became the operational version of C2BMC at U.S. European Command as part of the EPAA Phase 1 deployment. The MDA will replace S6.2 at U.S. Central Command in 4QFY12.

Sensor Management

The Global Engagement Manager (GEM) is the component of C2BMC that performs sensor management functions, beginning with S6.4. Since the beginning of the Ground Test-04 (GT-04) campaign in FY10, GEM exercised in four integrated ground tests and one distributed ground test the capability to perform sensor management functions for two AN/TPY-2 (FBM) radars and track data fusion and AN/TPY-2 (FBM) track forwarding. GEM also performed sensor management functions for a single AN/TPY-2 (FBM) in two flight tests and three distributed ground tests in FY11.

Sensor-Weapon Pairing/Track Forwarding

Sensor-weapon system pairing allows BMDS weapon elements to increase their battlespace using sensor tracks from non-organic sensors.¹⁵ The ability to engage a threat using non-organic track data is crucial to defense of Europe. In the EPAA Phase 1 architecture, Aegis BMD relies on one AN/TPY-2 (FBM) radar to provide cues or launch-on-remote track data, but testing has shown that defense of Europe benefits from two AN/TPY-2 radars. Aegis BMD executed a launch-on-remote engagement of an IRBM target using AN/TPY-2 (FBM) tracks

¹⁴ In these flight tests, the targets exhibited ICBM-like characteristics but flew IRBM ranges.

¹⁵ Non-organic sensors are sensors not part of an original weapon system design.

forwarded by C2BMC S6.4 during FTM-15. Several ground tests in the GT-04 campaign tested launch-on-remote capability culminating in GTD-04d Part 3, which used assets that are part of the initial EPAA Phase 1 deployment.

S6.4 software demonstrated track forwarding of single AN/TPY-2 (FBM) tracks to Tactical Digital Information Link J (Link 16) users in multiple ground tests and one flight test in FY11. C2BMC also exercised the forwarding of track data from two AN/TPY-2(FBM) radars in two integrated and one distributed ground tests as part of the EPAA Phase 1 capability demonstration.

Engagement Direction/Situational Awareness

As a precursor to BMDS engagement direction functionality, providing situational awareness was the first incremental capability developed for C2BMC and is the most mature C2BMC capability today. C2BMC situational awareness depends upon the ability of C2BMC to receive sensor track data and weapon element status and deliver it to operators and decision-makers. To date, S6.4 software has demonstrated the ability to receive, forward, and display track and status information from the following weapon elements and sensors: Aegis BMD, GMD (including sensors), Patriot, THAAD, AN/TPY-2 (FBM), space-based sensors (SBIRS/DSP), and the Israeli Arrow Weapon System. In the past, ground test analysis mainly focused on ensuring the accuracy and timeliness of C2BMC situational awareness for strategic threats. The EPAA Phase 1 technical capability declaration in December 2011 has shifted the focus of ground test analysis to emphasize the accuracy of C2BMC situational awareness for theater engagements.

S6.4 software received engagement and status information from Aegis BMD, GMD (including sensors), Patriot, THAAD, AN/TPY-2 (FBM), and space-based sensors (SBIRS/DSP). and provided situational awareness in several GT-04 campaign tests. C2BMC S6.4 also participated in three flight tests in FY11. Interoperability between the Israeli Arrow Weapon System, Patriot, and C2BMC S6.4 via Link 16, was demonstrated during United States Flight Test-4. C2BMC also provided situational awareness during Flight Test GBI-06a (FTG-06a) and FTT-12. Follow-on versions to S6.4 will incorporate the theater-level engagement management (THAAD-to-Patriot and Aegis BMD-to-Aegis BMD) required for the European missile defense mission. Limited engagement coordination between THAAD and Patriot was demonstrated in two ground test campaigns (GT-03 and GT-04) to date.

Section Four

Assessment of BMDS Test Adequacy

This section assesses the test adequacy of the FY/CY11 BMDS test program with respect to the four threat classes defined in Section Two. Since battle management functionality is essential to the successful performance of an integrated, layered-engagement BMDS, this section concludes with an assessment of test adequacy as it relates to BMDS battle management.

BMDS Test Adequacy Assessment Methodology

Four areas were reviewed to assess the adequacy of the BMDS test program: test planning and execution; operational realism; modeling and simulation; verification, validation, and accreditation (VV&A); and target development. Each of these areas affects the characterization of BMDS capability, both positively and negatively. In this section, these areas are assessed relative to each of the four threat classes.

The planning and execution of ground and flight tests of the BMDS is a complex and dynamic process. The Missile Defense Agency (MDA) documents this process in its BMDS Integrated Master Test Plan, which establishes the schedule, flight, and ground test requirements for the BMDS technical baseline. In preparing this document, the MDA must de-conflict range, test resources for use by the various BMDS elements and other outside users, and integrate the BMDS elements possessing varying maturities into system-level, rather than element-level, tests. Test planning and execution is an important ingredient of the characterization process and is discussed first.

In FY05, both the MDA and DOT&E agreed to a set of criteria (Table 4-1) for including operational realism in flight testing. The MDA and DOT&E generated these criteria in response to the FY05 National Defense Authorization Act, which requires the MDA to conduct an “operationally realistic test” of the BMDS. In its FY06 through FY10 reports to Congress, DOT&E applied these criteria in assessing the adequacy and sufficiency of the BMDS flight test program. For the FY/CY11 BMDS flight test program, DOT&E applied the criteria outlined in Table 4-1 to the flight tests conducted in the preceding year. These results are discussed second.

Table 4-1. MDA/DOT&E Operational Realism Criteria for Flight Testing

MDA/DOT&E Operational Realism Criteria	Description
Operationally Representative Interceptor	Operationally representative interceptor modified to support mandatory flight safety and data collection requirements
Threat-Representative Target	Threat-representative target trajectories, signatures, and scenarios
Complex Countermeasures	Target dynamics and penetration aids
Operational Sensor(s)	Operationally representative sensor modified to meet mandatory range safety and truth data requirements
Operational Fire Control Software	Operationally representative fire control software, fully tested and certified through the formal software acceptance process
Tactics, Techniques, and Procedures	Operationally representative tactics, techniques, and procedures within test constraints
Warfighter Participation	Operationally realistic warfighter participation consistent with real-world scenarios
Unannounced Target Launch	Target launch time unknown to warfighters
End-to-End Test	Direct use of appropriate operational assets while minimizing the introduction of artificialities

As discussed in Section Three, to evaluate, or quantify, the operational effectiveness, operational suitability, and survivability of the BMDS, an adequate test program must include models and simulations that have been fully accredited for performance assessment purposes by an independent agency such as the BMDS Operational Test Agency Team. Ground tests and models and simulations can examine scenarios that flight tests cannot assess because of geographic and safety constraints. The OTA must accredit over 40 component, element, lethality, threat, and environmental models and well as over 50 simulations in order to use them to assess BMDS performance. When properly verified and validated, they provide realistic predictions of system performance. Based on these predictions, operationally realistic flight tests provide empirical data to confirm system performance and to refine and validate the ground tests and models and simulations. Given its importance to a comprehensive evaluation of system performance, the status of the modeling and simulation VV&A effort is discussed third.

In Table 4-1, “threat-representative targets” is cited as one of the operational realism criteria. Targets are an important developmental asset common to all flight test programs. The MDA is the Department of Defense agency responsible for designing, developing, producing, and procuring ballistic missile targets for testing the BMDS. Targets that represent the full spectrum of threat ballistic missile capabilities and ranges are fundamental to the operational realism of a flight test program. Therefore, in assessing the adequacy of the FY/CY11 BMDS test program, the target development and employment status is discussed fourth.

Threat-Class Defense Test Adequacy Assessment

SRBM

The MDA and the U.S. Army conducted testing in FY/CY11 toward assessing the performance of the BMDS against SRBMs.

Test Planning and Execution for FY/CY11 (SRBM)

Aegis BMD

Aegis BMD did not conduct intercept flight testing against SRBM-class targets in FY/CY11. Flight testing of the SRBM engagement capability of the currently fielded Aegis BMD 3.6.1 system was completed in FY09 during the early part of follow-on testing for the 3.6.1 system.

Flight testing of Aegis BMD 3.6.1 SRBM engagement capability has been adequate to show capability over much of the designed-to battlespace, though there are minor shortfalls in testing. Flight testing to date has not exercised the pulse 2 mode of the SM-3 solid-fuel divert and attitude control system.¹⁶ However, the program has executed seven ground tests to verify pulse 2 operation. These ground tests, combined with modeling and simulation results, suggest that the full range of pulse modes function correctly. In addition, the MDA has not tested the zero-pulse mode of the SM-3 third-stage rocket motor in a live intercept event.¹⁷ Zero-pulse functionality is applicable to only a small portion of the overall engagement battlespace and is nearly impossible to demonstrate safely during flight testing. Results from digital simulations and ground testing are encouraging with respect to the rocket motor's zero-pulse functionality.

Aegis BMD 3.6.1 follow-on testing included two flight test missions that exercised sea-based terminal capability with SM-2 Block IV interceptors, which, along with a developmental sea-based terminal test, provide only three data collection events for that capability. Additional flight testing of the sea-based terminal capability would allow for a characterization of effectiveness with higher certainty, but that might not be practical given the limited inventory of SM-2 Block IV interceptors, which are no longer in production.

Although no intercepts were attempted against SRBM targets in FY/CY11, Aegis BMD 3.6.1 did participate in a technology demonstration event involving an SRBM:

¹⁶ The SM-3 solid-fuel divert and attitude control system has two pulse modes of operation. The first, or pulse 1 mode, is used to divert the Kinetic Warhead to achieve a zero effort miss. (Zero effort miss is a term used to describe the miss distance of the kill vehicle/kinetic warhead if it were to coast for the remaining time of flight without firing its attitude control divert system.) It is also used for aimpoint selection if the divert maneuver does not consume the entire pulse duration. This is the normal mode of operation for most engagements. The second, or pulse 2 mode, is invoked for aimpoint selection only if pulse 1 is required to correct the zero effort miss. This pulse mode is not normally invoked and is considered margin in the system.

¹⁷ The zero-pulse mode of operation for the SM-3 third-stage rocket motor is invoked only if the target object flies nearly directly over the defending ship.

- Flight Test Other (FTX)-16 Event 1 – March 15, 2011. This event assessed the capability of Aegis BMD 3.6.1 to conduct a simulated engagement of an SRBM target using track data from the Space Tracking and Surveillance System.

Flight testing against SRBM-class targets has not yet taken place with the next generation Aegis BMD 4.0.1 system. However, the Aegis BMD 4.0.1 system did participate in a live-target mission relevant to SRBM engagement capability:

- Flight Test Standard Missile-16 (FTM-16) Event 1 – March 10, 2011. An Aegis BMD 4.0.1 (engineering load) cruiser conducted a simulated engagement against a complex separating SRBM target with an SM-3 Block IB simulated missile.

To date, the Aegis BMD 4.0.1 system has conducted four simulated engagements against SRBM targets (including FTM-16 Event 1). The MDA plans to conduct the first Aegis BMD 4.0.1 engagement against a complex separating SRBM target in 3QFY12.

THAAD

The U.S. Army Operational Test Agency and MDA conducted one THAAD operational intercept flight test in FY/CY11 relevant to SRBM threats:

- FTT-12 – October 4, 2011. FTT-12 was a successful multiple simultaneous engagement with nearly simultaneous intercepts of two short-range targets.¹⁸ This test was also an IOT&E supporting the upcoming THAAD materiel release and Beyond Low-Rate Initial Production decisions. A Minimum Engagement Package, which is a reduced configuration of a THAAD battery, performed battle planning, overseas deployment, emplacement, and operations, under operationally realistic conditions (within the constraints of test range safety). As part of the IOT&E, the battery demonstrated continuity of operations after the live event by engaging a raid of threats generated by the Simulation Over Live Driver after the live event.

In addition to flight tests, the THAAD government ground test qualification program completed missile safety testing after exposure to extreme temperature environments and rail impact testing for the launcher. The program also performed regression rail impact and dust testing for the battery support center, after the MDA modified several components because of previous test failures. Most THAAD ground qualification testing is now complete, but planning and testing will continue as redesigns, capability, obsolescence upgrades take place.

The MDA also conducted a Reliability Confidence Test in July 2011 at McGregor Range, New Mexico, to demonstrate reliability growth from the 2010 Reliability Demonstration and Limited User Test, in support of the U.S. Army conditional material release decision.

Throughout 2011, THAAD completed supplementary testing and analyses to support the THAAD lethality assessment.

¹⁸ One target was a non-separating SRBM, and the other target was a separating target that had MRBM characteristics but flew a short-range trajectory.

THAAD also participated in one Aegis BMD flight test, FTM-16 Event 2, in September 2011, while the Minimum Engagement Package was deployed for FTT-12. The THAAD radar observed the target, and THAAD Fire Control and Communications (TFCC) exchanged data with C2BMC and indirectly with the Aegis ship through the Space and Naval Warfare System Command. The program also performed mission scenarios using the Simulation Over Live Driver during the pre-test communication checks.

Patriot

The U.S. Army conducted the following Patriot developmental tests against SRBMs in FY/CY11:

- Flight Test Missile Segment Enhancement (MSE) 7-3 – March 2, 2011. During flight test MSE 7-3, Patriot fired two Patriot Advanced Capability (PAC) -3 MSE interceptors in a ripple fire engagement at a threat-representative Juno unitary SRBM target to demonstrate performance in the extended battlespace of the MSE interceptor. Interceptor performance was consistent with preflight predictions, with the first MSE interceptor achieving body-to-body impact with the SRBM target, resulting in target destruction. The second MSE interceptor then tracked and intercepted target debris resulting from the first MSE intercept.
- Flight Test P7-4 – November 1, 2011. Patriot fired two PAC-3 missiles in a ripple fire engagement against an SRBM target. Interceptor performance was consistent with preflight predictions, with the first PAC-3 interceptor achieving body-to-body impact with the SRBM target, resulting in target destruction. The second PAC-3 interceptor was command-destructed, as designed for this mission.
- Flight Test P7-3 – November 4, 2011. Patriot fired two Guidance Enhanced Missile (GEM)-T interceptors in a ripple fire engagement against an SRBM target. The first GEM-T intercepted the SRBM target, resulting in target destruction. The second GEM-T interceptor self-destructed, as designed for this mission.
- Flight Test P7-2 – November 9, 2011. Patriot fired GEM-T/GEM-C interceptors in ripple fire engagements against two SRBM targets. In the first SRBM engagement, the first GEM-T missile intercepted the target, resulting in target destruction; the GEM-C missile then tracked and intercepted a piece of target debris resulting from the GEM-T intercept of the first SRBM target. In the second SRBM engagement, the first GEM-T missile intercepted the target, resulting in target destruction; the GEM-C missile was tracking a piece of target debris from the GEM-T intercept of the second SRBM target when it was command-destructed, as designed for this mission.
- Post-Deployment Build-7 (PDB-7) Developmental Test and Evaluation (DT&E) ground testing – July to October 2011. The test collected data to characterize the ability of the PAC-3 system using PDB-7 software to meet established operational performance requirements against threat-representative simulated and live targets. Data analysis is ongoing. The Army conducted a PDB-7 Endurance Test in late January 2012. The Army has scheduled the last PDB-7 DT&E flight test mission (P7-1) for late February 2012 to

complete PDB-7 DT&E testing. The Army has scheduled PDB-7 operational testing (Limited User Test) to begin in April 2012.

Operational Realism Assessment (SRBM)

Table 4-2 provides the assessment of flight test operational realism for FY/CY11 flight tests in support of SRBM threat-class defense using the criteria in Table 4-1.

Table 4-2. Operational Realism Assessment for FY/CY11 Flight Tests in Support of SRBM Defense

MDA/DOT&E Operational Realism Criteria	FY/CY11 Flight Tests				
	THAAD	Patriot			
	FTT-12	7-3	P7-4	P7-3	P7-2
Operationally Representative Interceptor	A	A	A	A	A
Threat-Representative Target	A	A	A	A	A
Complex Countermeasures	NT	NT	NT	NT	NT
Operational Sensor(s)	A	A	A	A	A
Operational Fire Control Software	A	A	A	A	A
Tactics, Techniques, and Procedures	A	A	A	A	A
Warfighter Participation	A	A	A	A	A
Unannounced Target Launch	A	NT	NT	NT	NT
End-to-End Test	A	A	A	A	A
Key: A – Achieved, P – Partially Achieved, NT – Not Tested					

Aegis BMD

Aegis BMD did not conduct flight testing against SRBM targets during FY/CY11. However, previously throughout the Developmental Test/Operational Test (DT/OT) and follow-on testing phases, Aegis BMD 3.6 and 3.6.1 demonstrated a good degree of operational realism. The Aegis BMD 4.0.1 system underwent its first developmental flight test in FY11 but has not yet engaged an SRBM target with a live interceptor.

THAAD

In FY/CY11, the MDA conducted FTT-12, an IOT&E flight test, against two SRBM targets, meeting all of the operational realism criteria attempted during the test. All THAAD components used were the final major hardware and software builds for the initial materiel release, although additional materiel releases are planned for several upcoming THAAD Software Builds in FY12 and FY13, and one of the interceptors was a deployable unit from the production line. FTT-12 used two realistic targets; trained Soldiers operated the equipment using the most recent tactics, techniques and procedures; and THAAD communicated with the Pacific Air and Space Operations Center, the 94th Air and Missile Defense Command, and C2BMC during the test. Soldier pre-flight battle design, emplacement, and preparation activities, were representative of the build-up to combat operations.

Patriot

The four FY/CY11 Patriot flight tests met seven of the nine operational realism criteria. None of the FY/CY10 Patriot flight tests included complex countermeasures or unannounced target launch, so those operational realism criteria were not tested.

Modeling and Simulation VV&A Status (SRBM)

Aegis BMD

DT/OT flight testing (through FTM-13) for the Aegis BMD 3.6 system was adequate to demonstrate a broad range of system capabilities. In addition, it allowed the program office to perform a verification and validation assessment of the core Aegis BMD modeling and simulation suite in support of accreditation by the U.S. Navy Commander, Operational Test and Evaluation Force (COMOPTEVFOR) for operational testing. In CY08, COMOPTEVFOR accredited the modeling suite and performed runs-for-the-record to support their evaluation of the Aegis BMD 3.6 system as a lone shooter but not for BMDS-level venues. The upgrade to Aegis BMD 3.6.1 added the near-term sea-based terminal capability but did not alter the midcourse engagement capability. As a result, COMOPTEVFOR opted not to reaccredit the modeling suite for midcourse engagement.

For the sea-based terminal capability with modified Standard Missile (SM)-2 Block IV interceptors, COMOPTEVFOR performed a limited set of runs-for-the-record using models validated from flight test data. However, there is no plan to perform a full accreditation of the Aegis BMD 3.6.1 sea-based terminal suite of models. COMOPTEVFOR performed the limited set of runs-for-the-record to enhance their own assessment of the Aegis BMD 3.6.1 system, but the runs do not carry the same weight as those for the Aegis BMD 3.6 midcourse engagement capability. It is unclear whether there are enough data from the sea-based terminal flight testing to perform a full accreditation of the models.

There are currently no plans to re-visit the accreditation of the Aegis BMD 3.6.1 modeling and simulation suite to address Aegis BMD's role in the defense of Europe as part of the EPAA Phase 1 architecture. However, it is uncertain whether a new accreditation is necessary for SRBM engagements for the EPAA Phase 1 mission.

There has been no flight testing of the new Aegis BMD 4.0.1 system against SRBM-class targets, so no VV&A is yet possible. The Aegis BMD program office is currently writing a verification and validation plan for 4.0.1., and COMOPTEVFOR is drafting an accreditation plan. The two plans will likely be finalized in early CY12.

THAAD

The U.S. Army Test and Evaluation Command conducted an independent accreditation of some THAAD models and simulations before using the data in their Operational Test Agency Assessment Report in support of the fielding decision for the first two THAAD fire units. It accredited, with limitations, the Simulation Over Live Driver, Integrated Simulation and Tactical Software, THAAD Evaluation Center Hardware-in-the-Loop and Imaging Infrared Imaging Simulation, and Parametric Endo-/Exo-atmospheric Lethality Simulation. For BMDS-level venues, the BMDS Operational Test Agency Team has recommended limited accreditation of the

Integrated Simulation and Tactical Software model. All THAAD models and simulations used for performance assessment undergo verification and validation continuously as flight and ground testing progresses.

Patriot

The U.S. Army Test and Evaluation Command accredited the PDB-6.5 version of the Mobile Flight Mission Simulator hardware-in-the-loop system in November 2009, the Parametric Endo-/Exo-atmospheric Lethality Simulation and the Extended Range Interceptor Lethality Endgame Simulation in January 2010, and the Patriot Advanced Capability (PAC)-2 Simulation and PAC-3 Simulation in March 2010. The U.S. Army is drafting VV&A plans for the PDB-7 versions of these models and simulations. For BMDS-level venues, the BMDS Operational Test Agency Team has not recommended accreditation of the Patriot System Effectiveness Model and does not expect to do so until Phase 2 of the EPAA. The Flight Mission Simulator/Digital was used in BMDS-level integrated ground tests to test Patriot interoperability with other BMDS elements (not performance), but the simulator has not yet been accredited for use in BMDS-related events.

Target Development and Employment Status (SRBM)

Aegis BMD

Aegis BMD continues to use existing rocket technology to produce the inexpensive Aegis Readiness Assessment Vehicle-A (ARAV-A) targets for use in tracking and midcourse engagement missions requiring a non-separating SRBM target. ARAV-A targets are significantly cheaper to produce than the Test Target Vehicles (constructed from a Minuteman I missile second stage) used in early intercept missions.

For the expanded mission against more complicated SRBMs with Aegis BMD 4.0.1 and SM-3 Block IB interceptors, the program developed an ARAV-C target for use in both tracking and engagement missions. The FTM-16 Event 1 simulated engagement was the second simulated engagement against an ARAV-C target (the first was in FTX-06 Event 4).

THAAD

Progress was made in FY/CY11, when the short-range air-launched target that failed last year in FTT-11, returned to flight following a quality review. The target, which is necessary to test the radar advanced algorithms, which are described in Appendix A, is now scheduled for a THAAD flight test in FY14. The MDA had previously flown the two target types used in FTT-12.¹⁹

Patriot

After IOT&E in 2002, DOT&E required the U.S. Army to conduct flight tests against targets representing two particular threat SRBMs, prior to a Patriot full-rate production decision. The Army has assigned as tasks the deficiencies identified in 2002 and has scheduled one of

¹⁹ The MDA had planned FTT-11 to test the radar advanced algorithms before the materiel release decision. This capability will now be tested after the decision.

these tests for 2012. Requirement definition for the second threat continues as threat projection evolves.

MRBM

The MDA conducted testing in FY/CY11 toward assessing the performance of the BMDS against MRBMs.

Test Planning and Execution for FY/CY11 (MRBM)

Aegis BMD

The MDA conducted two Aegis BMD-related intercept flight tests against MRBM-class targets (at maximum SRBM ranges) in FY/CY11:

- Japan Flight Test Standard Missile-4 (JFTM-4) – October 29, 2010. A Japanese Aegis BMD destroyer using an SM-3 Block IA interceptor intercepted an MRBM-representative separating target. JFTM-4 was the third successful (out of four) engagement performed by a Japanese Aegis BMD destroyer.
- FTM-16 Event 2 – September 1, 2011. An Aegis BMD cruiser with 4.0.1 software failed to intercept a separating MRBM-like ballistic missile target with an SM-3 Block IB interceptor. FTM-16 Event 2 was the first intercept attempt for the new Aegis BMD 4.0.1 system with the SM-3 Block IB interceptors.

The targets the MDA flew in JFTM-4 and FTM-16 Event 2 possessed MRBM-like characteristics but flew less than 1,000 kilometers and were therefore SRBMs in terms of range. However, since the targets have characteristics similar to those of low-end MRBMs and only fall slightly short of true MRBM ranges, it is fair to treat them as surrogates for low-end MRBMs. Flight testing of Aegis BMD has been adequate to demonstrate the capability to conduct midcourse phase engagements against MRBMs at the lower threshold of the medium-range band. Testing of this capability included three Aegis DT/OT missions and one DT mission, and four Japanese Aegis BMD flight tests.

Prior to FY/CY11, the primary shortfall in testing Aegis BMD engagement capability against MRBMs had been the lack of flight testing against targets with ground ranges well into the medium-range band. Engagements against such threats became part of Aegis BMD's mission with the introduction of the EPAA Phase 1 architecture for missile defense in Europe. This shortfall was, to a degree, addressed by the engagement of an IRBM target during FTM-15 (see the IRBM discussion below). The characteristics of the engagement are similar and the ability to engage a longer-range target provided a demonstration of engagement capability against longer-range MRBM threats. Overall certainty in the system's ability to engage longer-range targets is limited, however, since only one engagement of that type has been performed.

A secondary shortfall is the aforementioned lack of flight testing of the SM-3 kinetic warhead's divert system's pulse 2 mode, though ground testing does mitigate this shortfall somewhat.

The Aegis BMD 4.0.1 system did not attempt any simulated engagements against live MRBM-class targets in FY/CY11. However, the 4.0.1 system has conducted seven simulated engagements against MRBM-class targets (at upper-end SRBM ranges) in testing to date.

THAAD

The FTT-12 IOT&E flight test discussed above for SRBMs has relevance to the MRBM mission because the separating target, although it flew a short range trajectory, had MRBM characteristics. While not an MRBM-representative trajectory, some data from the test may still be useful when THAAD MRBM performance is assessed. The Aegis BMD flight test event discussed above, FTM-16 Event 2, similarly has some relevance to the MRBM mission.

In addition, many aspects of the ground testing and lethality testing discussed for SRBMs are also relevant to MRBMs, since THAAD will use the same hardware and software for both short- and medium-range threats. BMDS-level ground tests also explored some characteristics of THAAD engagements against MRBMs.

Patriot

The U.S. Army did not conduct any Patriot flight tests against MRBM targets in FY/CY11. The PDB-7 Developmental Test and Evaluation (DT&E) hardware-in-the-loop testing did include simulated MRBM targets.

Operational Realism Assessment (MRBM)

Table 4-3 provides the assessment of flight test operational realism for FY/CY11 flight tests in support of MRBM threat-class defense using the criteria in Table 4-1.

Table 4-3. Operational Realism Assessment for FY/CY11 Flight Tests in Support of MRBM Defense

MDA/DOT&E Operational Realism Criteria	FY/CY11 Flight Tests
	Aegis BMD
	FTM-16 Event 2
Operationally Representative Interceptor	P
Threat-Representative Target	P
Complex Countermeasures	NT
Operational Sensor(s)	P
Operational Fire Control Software	P
Tactics, Techniques, and Procedures	P
Warfighter Participation	P
Unannounced Target Launch	NT
End-to-End Test	P
Key: A – Achieved, P – Partially Achieved, NT – Not Tested	

Aegis BMD

FTM-16 Event 2 was the lone FY/CY11 flight test against an MRBM-like target utilizing U.S. Aegis BMD assets (Japanese Aegis BMD flight tests are not assigned ratings for operational realism). FTM-16 Event 2 was the first developmental flight test of the next generation Aegis BMD 4.0.1 system with SM-3 Block IB interceptors. All hardware and software-related realism criteria are assigned a rating of “Partially Achieved,” since one or more aspects of the hardware or software are new in the Aegis BMD 4.0.1 system and SM-3 Block IB interceptors. For example, the SM-3 Block IB interceptor has a new kinetic warhead divert system and seeker, and the ship-board system has a new BMD signal processor and system software.

Other realism criteria also warrant a “Partially Achieved” rating since the test was developmental in nature. The participating ship did have warfighters on-station, but there was a much greater contractor presence than in a DT/OT or OT mission. In addition, the end user did not certify the tactics, techniques, and procedures used in the test.

THAAD

Although THAAD completed no flight tests against true MRBM targets in FY/CY11, FTT-12, discussed previously for SRBMs, provides some data on performance against MRBMs. In addition to the MRBM characteristics of one of the targets, the test employed the same communication structures and tactics, techniques, and procedures used for MRBMs.

Patriot

The U.S. Army did not conduct any Patriot flight tests against MRBM targets in FY/CY11. Consequently, no flight tests are assessed here for operational realism.

Modeling and Simulation VV&A Status (MRBM)

Aegis BMD

DT/OT flight testing for the Aegis BMD 3.6 system was sufficient to perform a verification and validation assessment of the midcourse-phase modeling and simulation suite in support of the CY08 accreditation by COMOPTEVFOR for operational testing. COMOPTEVFOR accredited the modeling suite and performed a set of runs-for-record to support their evaluation of Aegis BMD 3.6 system performance against short-range MRBM-like threats.

However, after announcement of the expanded EPAA mission for Aegis BMD, the validity of the models used for the BMD 3.6 runs-for-record was called into question for threats with ranges well beyond those tested during DT/OT (i.e., short-range MRBM-like threats). In light of this, COMOPTEVFOR limited the accreditation to threats with a range of less than 1,000 kilometers.²⁰

There has been only one developmental flight test of the Aegis BMD 4.0.1 system, so VV&A is not yet possible. As mentioned under the discussion for SRBMs, a VV&A plan is being developed, and will likely be available by early CY12.

THAAD

As discussed previously for SRBMs, verification and validation is ongoing for the primary THAAD models and simulations as flight and ground testing progresses. Since no true medium-range flight tests have taken place, the U.S. Army's current accreditation for the Simulation Over Live Driver, Integrated Simulation and Tactical Software, THAAD Evaluation Center Hardware-in-the-Loop and Imaging Infrared Imaging Simulation, and Parametric Endo-/Exo-atmospheric Lethality Simulation, does not include THAAD performance against MRBMs. Some information is attainable from FTT-09 and FTT-12, for which the targets flew short-range trajectories but exhibited primarily medium-range target characteristics, but not enough for a complete accreditation using medium-range flight characteristics. The U.S. Army plans additional assessments as more capabilities are tested and fielded.

Patriot

The U.S. Army Test and Evaluation Command accredited the PDB-6.5 version of the Mobile Flight Mission Simulator hardware-in-the-loop system in November 2009, the Parametric Endo-/Exo-atmospheric Lethality Simulation and Extended Range Interceptor Lethality Endgame Simulation in January 2010, and the PAC-2 Simulation and PAC-3 Simulation in March 2010. The U.S. Army is drafting VV&A plans for the PDB-7 versions of these models and simulations. For BMDS-level venues, the BMDS Operational Test Agency Team has not recommended accreditation of the Patriot System Effectiveness Model and does not expect to do so until Phase 2 of the EPAA. The Flight Mission Simulator/Digital was used in

²⁰ This was documented in a memorandum to DOT&E and MDA from W.J. McCarthy, Deputy, COMOPTEVFOR, February 9, 2010.

BMDS-level integrated ground tests to test Patriot interoperability with other BMDS elements (not performance), but the simulator has not yet been accredited for use in BMDS-related events.

Target Development and Employment Status (MRBM)

Aegis BMD

For MRBM targets, Aegis BMD continues to use the Medium Range Target (MRT) for engagement missions. MRTs are essentially SRBMs (in terms of range) with MRBM characteristics. JFTM-4 flight tested with an MRT and was the seventh MRT used in an Aegis BMD-related flight test.

Until recently, the MDA did not intend to utilize an ARAV variant for use in engagement missions against MRBM-like targets. The FTM-16 Event 2 engagement was the first intercept mission utilizing a simple separating variant of the ARAV (the ARAV-B). Prior to this test, the ARAV-B had only been used for tracking exercises and simulated engagements. Although the ARAV-B was engaged in FTM-16 Event 2 (which was a developmental test), COMOPTEVFOR has not yet certified the ARAV-B for use in DT/OT or OT engagement missions.

The MDA has begun the process of developing new MRBM-class targets for use in upcoming Aegis BMD (and other element) flight missions. Its aim is to develop a set of targets based on common, cost-effective, and flexible components, wherein a standard set of targets can be used to meet specific threat requirements.

THAAD

Starting in FY12, THAAD plans to use true medium-range targets, rather than the targets used to date, which have medium-range characteristics but fly short-range. Development and production of these targets are still underway. The target type is planned for use in the next flight test, Flight Test Integrated-01, and currently has a production schedule with little margin.

Patriot

DOT&E has proposed that the MDA develop a target to represent a particular MRBM threat for Patriot to engage in Flight Test Operational-02 in FY15. This is discussed in Appendix C. However, the MDA currently plans to use an SRBM target instead.

IRBM

The MDA conducted testing in FY/CY11 toward assessing the performance of the BMDS against IRBMs.

Test Planning and Execution for FY/CY11 (IRBM)

Ground-based Midcourse Defense (GMD)

In FY/CY11, the MDA conducted one GMD intercept flight test intended to address GMD capability to defend the U.S. Homeland against IRBMs:

- Flight Test GBI-06a (FTG-06a) – December 15, 2010. FTG-06a was a re-test of the unsuccessful FTG-06 intercept attempt in January 2010. The GMD element attempted to intercept an IRBM-class target using the new Capability Enhancement-II (CE-II) Exo-atmospheric Kill Vehicle (EKV). AN/TPY-2 (FBM) and Sea-Based X-Band (SBX)

radars provided target acquisition, track, and discrimination data to GMD. Space-Based Infrared System/Defense Support Program (SBIRS/DSP) also participated in the test. The GMD interceptor flew to its designated point and deployed its EKV. The EKV acquired the target complex, but failed to intercept the target reentry vehicle.

During FTG-06a, the MDA collected data on multiple critical engagement conditions; however, FTG-06a test objectives related to EKV performance were not achieved. The intercept failure precluded acquisition of EKV performance data that could support validation and accreditation of models and simulations of EKV performance. A failure review board investigated the cause of the failure; results are discussed in Appendix A. The test was adequate to support limited characterization of GMD ground system performance and interceptor launch and flyout performances. In addition, the MDA succeeded in verifying the effectiveness of software fixes that were made to the SBX radar in response to its undesirable performances in FTG-06. FTG-06a demonstrated a capability of the SBX radar to provide track data that supported GMD engagement planning against an IRBM target.

Aegis BMD

The MDA conducted one Aegis BMD 3.6.1 end-to-end flight test against an IRBM target in FY/CY11:

- FTM-15 – April 15, 2011. An Aegis BMD 3.6.1 destroyer, set up with remote engagements authorized, intercepted a separating IRBM target with an SM-3 Block IA interceptor using up-range track data from an AN/TPY-2 (FBM) radar.²¹

The FTM-15 engagement was the first intercept of an IRBM with an SM-3 Block IA interceptor, and the first intercept attempt with an Aegis BMD ship set up with remote engagements authorized. The FTM-15 demonstration of Aegis BMD 3.6.1 engagement capability against longer-ranged targets provided a needed proof-of-concept for a type of engagement expected for the EPAA Phase 1 architecture for missile defense in Europe. However, the overall certainty in that capability is limited because there has been only one flight test of this capability.

Aegis BMD also participated in a GMD intercept mission to exercise the IRBM engagement capability with the system set up with remote engagements authorized:

- FTG-06a – December 15, 2010. Aegis BMD assessed launch-on-remote capability (with the ship set up with remote engagements authorized) by conducting a simulated engagement of an IRBM target using a surrogate destroyer with 3.6.1.2 software based on live AN/TPY-2 (FBM) track data.

²¹ Having remote engagements authorized means that the Aegis BMD ship will use non-organic radar tracking data, either to cue the ship to acquire and then engage the threat (a cued engagement), or, if the data quality is adequate, to launch an interceptor before the radar on the Aegis BMD ship acquires the threat (a launch on remote engagement).

Current plans call for the Aegis BMD 4.0.1 system to be flight tested against IRBM-class targets in FY15 with SM-3 Block IB interceptors as part of the Flight Test Operational-02 system test.

Operational Realism Assessment (IRBM)

Table 4-4 provides the assessment of flight test operational realism for FY/CY11 flight tests in support of IRBM threat-class defense using the criteria in Table 4-1.

Table 4-4. Operational Realism Assessment for FY/CY11 Flight Tests in Support of IRBM Defense

MDA/DOT&E Operational Realism Criteria	FY/CY11 Flight Tests	
	GMD	Aegis BMD
	FTG-06a	FTM-15
Operationally Representative Interceptor	A	A
Threat-Representative Target	DT	A
Complex Countermeasures	NT	NT
Operational Sensor(s)	P	A
Operational Fire Control Software	A	A
Tactics, Techniques, and Procedures	DT	P
Warfighter Participation	A	A
Unannounced Target Launch	A	A
End-to-End Test	DT	A
Key: A – Achieved, P – Partially Achieved, DT – Developmental Testing, NT – Not Tested		

GMD

In FY/CY11, the MDA conducted one GMD intercept flight test, FTG-06a, which addressed GMD capability to defend against IRBMs. Specific to the operational realism criteria, this flight test featured the following:

- The GMD interceptor met operational realism criteria and was operationally representative of emplaced interceptors that incorporate CE-II EKV's.
- Aspects of the target were threat-representative, but the target trajectory was shaped to achieve developmental test objectives and the target reentry vehicle emulated an ICBM threat reentry vehicle. In addition, the MDA chose the target deployment vehicle, the target deployment vehicle maneuvering, and the countermeasure deployments to achieve developmental test objectives.
- The MDA did not include complex countermeasures in this test.
- The employed sensors partially met operational realism criteria. The SBX radar was located in the test geometry in an operationally representative location and was cued by an operationally representative AN/TPY-2 (FBM) radar. The MDA, however, employed

the SBX radar in a manner that departed from full operational realism in order to achieve specific developmental test objectives and to reduce risk to the achievement of primary test objectives. Due to this departure from operational realism, MDA precluded the SBX radar from supporting GMD engagement of the target through intercept. The fire control software, warfighter participation, and unannounced target launch, met operational realism criteria.

- The MDA tailored the Soldier's tactics, techniques, and procedures, in order to support the flight test timeline and did not meet operational realism criteria.
- Specific test parameters, such as the scenario geometry, engagement timeline, and operational sensor employment, were not representative of an operationally realistic end-to-end test.

Aegis BMD

FTM-15, which was designated as an OT for Aegis BMD 3.6.1 and a combined DT/OT at the system level, included many aspects of operational realism, motivating the assignment of "Achieved" for most of the realism criteria. Fielded Aegis BMD 3.6.1 hardware and software was used in the test, as was an operational SM-3 Block IA interceptor. The AN/TPY-2 (FBM) radar and C2BMC used in the test were configured as they will be when deployed as part of Phase 1 of the EPAA architecture. Although the types and versions of hardware/software planned for the EPAA Phase 1 architecture were tested in FTM-15, they were not present in the number and configurations expected for European defense.

Tactics, techniques, and procedures are assigned a rating of "Partially Achieved" because FTM-15 was conducted before certified tactics, techniques, and procedures for EPAA Phase 1 were established. It is also worth noting that many of the warfighters who participated in FTM-15 were not the end-users for EPAA Phase 1 (from U.S. European Command), but they were rather assigned from U.S. Pacific Command. Nonetheless, a rating of "Achieved" is assigned for Warfighter Participation with the assumption that operators from the two warfighter communities are similarly trained and would have operated the system in a similar manner.

Modeling and Simulation VV&A Status (IRBM)

GMD

In FY09, the MDA identified 12 GMD engagement parameters that required data acquisition to support GMD model and simulation VV&A and revised the GMD test program plan to support acquisition of this data. The MDA needs several successful intercept flight tests for accreditation of models and simulations over a limited portion of the GMD engagement battlespace. As testing proceeds according to the GMD test plan, the GMD models and simulations would accrue accreditation over increasing portions of the expected engagement battlespace. The MDA currently plans 13 future intercept flight tests to support model and simulation accreditation over the complete IRBM and ICBM engagement battlespace. The slow pace of flight testing limits the pace of progress toward VV&A of models and simulations. Intercept flight test FTG-06a was inserted into the BMDS Integrated Master Test Plan as a re-test

of the failed FTG-06. FTG-06a did not achieve all of its test objectives, and it failed to provide data to support VV&A of the interceptor EKV performances.

In FY/CY11, the MDA made progress toward the VV&A of models and simulations, but the progress was inadequate to support accreditation of the models and simulations for performance assessment in end-to-end ground testing. VV&A of supplemental, non-GMD models and simulations are also needed for performance assessment of the GMD element in end-to-end simulations. These non-GMD models and simulations include IRBM and ICBM threat models, sensor models, and environmental models. In FY/CY11, the MDA did not achieve accreditation for any IRBM or ICBM threat model. The Cobra Dane radar model was not accredited for performance assessment. The Upgraded Early Warning Radar (UEWR) and Sea-Based X-Band (SBX) radar models achieved limited accreditation. For environmental models, 3 achieved accreditation, 18 achieved limited accreditation, and 9 achieved no accreditation.

Aegis BMD

There has been only one flight test against IRBM targets with Aegis BMD as the shooter (FTM-15). Since COMOPTEVFOR has not yet accredited the core modeling and simulation suite for midcourse engagements, no runs-for-record were performed.

Target Development and Employment Status (IRBM)

GMD

The MDA developed the Launch Vehicle-2 as a boost vehicle for IRBM targets. In FTG-06 and FTG-06a, the target consisted of a Launch Vehicle-2, a Matching Ballistic Reentry Vehicle-2, and countermeasures. The target performed successfully in both flight tests. The MDA plans to employ the Launch Vehicle-2 and Matching Ballistic Reentry Vehicle-2 in two future GMD intercept flight tests. In FY/CY11, the MDA awarded a new contract for development of an air-launched IRBM target.

Aegis BMD

The MDA used a Launch Vehicle-2 target in FTM-15. The Launch Vehicle-2 is expected to be used in future Aegis BMD flight missions involving IRBM-class targets. New IRBM targets such as the air-launched IRBM targets might be used in the future, but such targets have yet to be built or flight tested. The next Aegis BMD test, including the engagement of an IRBM, is planned for FY15.

ICBM

The MDA conducted testing in FY/CY11 toward assessing the performance of the BMDS against ICBMs.

Test Planning and Execution for FY/CY11 (ICBM)

GMD

In FY/CY11, the MDA conducted a GMD intercept flight test, FTG-06a, against an IRBM target. Details of this test are discussed above in the IRBM section. Specific data, such as GMD ground system performance, operator performance, and interceptor launch and flyout

performances, are directly relevant to GMD performance against ICBM threats. The failure to intercept precluded acquisition of EKV performance data that could support VV&A of models and simulations of EKV performance.

Aegis BMD

Aegis BMD 5.1x, which is planned to include a capability to engage a set of ICBMs, is in an early stage of concept development. The Aegis BMD 5.1 system, which is also in an early stage of development, might provide a potential capability against a limited set of ICBMs. The MDA currently has no plans to conduct a flight test with any of these builds until FY18 at the earliest. No assessment of flight test operational realism can be provided.

Operational Realism Assessment (ICBM)

GMD

The operational realism of FTG-06a as a test against an IRBM target is discussed above in the IRBM section. Since the test was designed and executed as an intercept test against an IRBM, the operational realism of this test is not rated in this section.

Aegis BMD

Aegis BMD did not conduct a flight test against ICBM targets. Consequently, no operational realism assessment is given.

Modeling and Simulation VV&A Status (ICBM)

GMD

The GMD modeling and simulation VV&A status is discussed above in the IRBM section.

Aegis BMD

The Aegis BMD 5.1 and 5.1x systems are in the early stages of development, so the modeling and simulation tools are immature. Until flight testing provides data for anchoring the models and simulations, no VV&A is possible.

Target Development and Employment Status (ICBM)

GMD

In FY/CY11, the MDA continued planning activity for future development of an ICBM target. The first GMD intercept flight test against the new ICBM target is planned for 4QFY15.

Aegis BMD

The Aegis BMD 5.1 and 5.1x systems are not likely to test against ICBM-class targets until FY18 at the earliest. Any ICBM-class targets used for Aegis BMD testing will probably be identical to those used for GMD flight testing, and they will be developed as part of MDA's new common and flexible component approach to target design.

BMDS Battle Management Test Adequacy Assessment

In FY/CY11, Aegis BMD, GMD, Patriot, THAAD, and C2BMC all participated in BMDS-level (multi-element) ground tests. These tests were not accredited for performance assessment as endgame performance was not modeled, and specific models (threat, environmental, sensor) that were used in the tests were not accredited for performance. However, these ground tests were adequate to support a limited characterization of BMDS-level battle management functionality. BMDS-level ground tests and flight tests conducted in FY/CY11 relevant to the battle management aspect of the BMDS include the following:

- Fast Eagle – October 2010. The purpose of this hardware-in-the-loop test was to demonstrate the integration of AN/TPY-2 (FBM), C2BMC S6.2, SBIRS/DSP, Aegis BMD, and Patriot for U.S. Central Command defense.
- Assured Response-04X (AR-04X) – October 2010. C2BMC S6.4 participated in the global U.S. Strategic Command exercise, AR-04X. The exercise used both strategic- and theater-level scenarios in the hardware-in-the-loop configuration. C2BMC provided situational awareness for strategic and EPAA Phase 1 scenarios. The U.S. European Command sensor managers from the 357th Air and Missile Defense Detachment (AMD-D) used GEM to control two simulated AN/TPY-2 (FBM) radars.
- Assured Response-04D (AR-04D) – March 2011. This distributed U.S. Strategic Command exercise focused on the EPAA Phase 1 architecture and scenarios. C2BMC S6.2 and S6.4 provided situational awareness to the U.S. Central Command and U.S. European Command crews, respectively. The U.S. European Command sensor managers from the 357th AMD-D, again concurrently controlled two simulated AN/TPY-2 (FBM) radars.
- FTG-06a – December 15, 2010. FTG-06a was an attempted GMD intercept of an IRBM target. C2BMC S6.4 received AN/TPY-2 (FBM) tracks, forwarded the tracks to GMD, and provided situational awareness in multiple locations. C2BMC received and displayed AN/TPY-2 (FBM), SBX, and GMD summary data and collected data to support the FTM-15 risk reduction analysis. SBIRS/DSP also participated in the test.
- United States Flight Test-4 (USFT-4) – February 22, 2011. This flight test demonstrated interoperability between the Israeli Arrow Weapon System and BMDS elements. C2BMC S6.4 exchanged messages with Patriot and Israeli Arrow and provided situational awareness. The test revealed interoperability and situational awareness problems.
- Ground Test Distributed-04b (GTD-04b) – February/March 2011. GTD-04b was a distributed test of the entire BMDS focused on the defense of the continental United States from North Korean threats. The MDA collected data in support of the S6.4 fielding decision. The U.S. Pacific Command sensor managers from the 94th Army Air and Missile Defense Command (AAMDC) used the Global Engagement Manager (GEM) to command and control a single AN/TPY-2 (FBM). C2BMC provided situational

awareness and track forwarding functionality and demonstrated the integration of the new AN/TPY-2 software with S6.4.

- FTM-15 – April 15, 2011. FTM-15 was the first launch-on-remote engagement of an IRBM target with Aegis BMD. The U.S. Pacific Command sensor managers from the 94th AAMDC controlled one AN/TPY-2 (FBM) radar. C2BMC received AN/TPY-2 (FBM) tracks, reported the tracks to the firing Aegis BMD ship, and provided situational awareness to the U.S. Pacific Command crew. The ship launched an interceptor based on the track information received from C2BMC.
- Technical Assessment 04 (TA-04) – July-Sept 2011. The MDA conducted TA-04, a fully digital simulation, to assess the status of BMDS element-level digital simulations and BMDS-level integration of those simulations. TA-04 provides risk reduction for Performance Assessment 04, which is planned for the 4QFY13. Multiple simulated threat scenarios stimulated digital representations of the BMDS and its elements within the defined TA-04 architecture.
- Ground Test Integrated-04d (GTI-04d) Part 1 – July 2011. This test was a theater-level hardware-in-the-loop event intended to support the EPAA Phase 1 assessment. The members of the 357th AMD-D controlled two simulated AN/TPY-2 (FBM) radars using two GEM terminals. C2BMC provided situational awareness for defense of Europe and Israel. Aegis BMD, Patriot, THAAD, Israeli Arrow, and SBIRS/DSP also participated.
- GTD-04d Part 1 – September 2011. GTD-04d Part 1 was a theater-level distributed event intended to support the EPAA Phase 1 and NATO Active Layered Theater Ballistic Missile Defense (ALTBMD) Interim Capability assessments. GTD-04d Part 1 tested C2BMC S6.4 and AN/TPY-2 (FBM) software upgrades at U.S. European Command. The members of the 357th AMD-D controlled one AN/TPY-2 (FBM) radar. Aegis BMD, SBIRS/DSP, and Israeli Arrow also participated. In addition, the interoperability between EUCOM C2BMC S6.4, AN/TPY-2 (FBM), SBIRS, Aegis BMD and NATO ALTBMd, a German Patriot Unit, a Dutch Patriot Unit and Shared Early Warning was tested for the first time in a distributed environment.
- Global Defender Exercise-04d (GDEx-04d) – September 2011. C2BMC S6.4 participated in the global BMDS exercise GDEx-04d. The exercise included both strategic and regional scenarios and provided a training opportunity for the warfighters.
- FTT-12 – October 5, 2011. FTT-12 demonstrated a near-simultaneous engagement of an SRBM and an MRBM-class target flown at a maximum SRBM range. The test also demonstrated limited THAAD and C2BMC S6.4 interoperability over Link 16. C2BMC provided situational awareness and status of the BMDS under test to the 94th AAMDC warfighters.
- GTI-04d Part 2 – October 2011. This test was a follow-on test for GTI-04d Part 1. It included updated scenarios and radar location. The 10th AAMDC (formerly 357th AMD-D) warfighters controlled two simulated AN/TPY-2 (FBM) radars. C2BMC provided

situational awareness for defense of Europe and Israel. Aegis BMD, Patriot, Israeli Arrow, and SBIRS/DSP also participated.

- GTI-04 Israel (ISR) – November 2011. This integrated test demonstrated a combined U.S.-Israeli capability to defend Israel against theater threats. C2BMC S6.4, AN/TPY-2 (FBM), SBIRS/DSP, Aegis BMD, Patriot, THAAD, and Israeli Arrow, participated in GTI-04 ISR.
- GTD-04d Part 2 – December 2011. Part 2 of GTD-04d was a theater-level distributed event supporting the fielding of the new EUCOM AN/TPY-2 (FBM) and the EPAA Phase 1 technical capability declaration. A single AN/TPY-2 (FBM) radar was represented in the test architecture in addition to C2BMC S6.4, Aegis BMD, and SBIRS/DSP.
- GTD-04d Part 3 – December 2011. The MDA conducted a distributed test GTD-04d Part 3 in support of the EPAA Phase 1 assessment. The sensor managers from the 10th AAMDC used C2BMC S6.4 to command and control two AN/TPY-2 (FBM) radars for the first time in a distributed ground test. Aegis BMD and SBIRS/DSP also participated.

C2BMC S6.4 functions, (situational awareness, launch-on-remote, and interoperability) with other BMDS elements, were demonstrated in several flight tests in FY/CY11. The MDA conducted FTM-15 to demonstrate launch-on-remote capability using AN/TPY-2 (FBM) tracking data forwarded by S6.4. Launch-on-remote using EPAA Phase 1 assets was also demonstrated in several ground tests using the initial Phase 1 architecture. C2BMC S6.4 provided situational awareness in USFT-4, FTG-06a, FTM-15, FTT-12, and all ground tests, but the warfighter participation in flight tests was not always fully operationally realistic.

In the past, ground test analysis of C2BMC capabilities focused on strategic situational awareness. The MDA recently shifted the focus to C2BMC capabilities for theater-level engagements. Initially, theater situational awareness, support for Aegis BMD launch-on-remote engagements, and management of multiple AN/TPY-2 (FBM) radars will be the most important C2BMC functions for defense of Europe and Israel. The implementation of the EPAA Phase 1 architecture has not been consistent in recent GT-04 ground tests. No flight tests and only one distributed ground test demonstrated management of two AN/TPY-2 (FBM) radars.

The MDA will incrementally implement battle engagement direction functionality, which is an important part of system-level tests, over several future C2BMC versions. The ground and flight tests above provided opportunities to exercise system-level battle management and to make modifications and improvements based on the interoperability problems encountered. The MDA will need to conduct additional weapon element flight tests and system-level flight tests with multiple weapon element participation to allow for a characterization of the battle management of the integrated BMDS in a realistic environment.

This page intentionally left blank.

Section Five

Characterization of BMDS Operational Effectiveness, Suitability, and Survivability

This section, together with Appendices A and B (both classified), characterizes the operational effectiveness, suitability, and survivability of the BMDS and its weapon elements that have been fielded or tested before the end of FY/CY11. The characterization is relative to each of the four threat classes defined in Section Two.

BMDS Performance Characterization Methodology

In the FY07 DOT&E report to Congress assessing the BMDS, DOT&E identified a set of Critical Operational Issues (COIs) used to characterize the operational effectiveness, suitability, and survivability of the BMDS. Key COIs from the FY07 report include the following:

- **Effectiveness:** Is the BMDS operationally effective against strategic/theater threat ballistic missiles?
 - *Detect and Track:* Can the BMDS detect the threat and, given detect, track the threat?
 - *Assess, Classify, and Discriminate:* Can the BMDS perform threat assessment (threat to defended area), threat classification (threat or non-threat), and, if applicable, discriminate the lethal threat object from decoys, countermeasures, and other objects, given track?
 - *Engage and Intercept:* Can the BMDS engage and intercept the threat with a missile, given track and threat classification?
 - *Lethality:* Can the BMDS kill the strategic threat under the expected intercept conditions, given intercept?
 - *Battle Management:* Does the BMDS successfully manage information between sensors and weapon elements to contribute to strategic/theater mission success?
 - *Kill Assessment:* Can the BMDS accurately determine if the system successfully negated the threat object?
- **Suitability:** Is the BMDS suitable for global (strategic and theater) missile defense operations?
 - *Interoperability:* Are the missile defense elements, sensors, and components interoperable with each other?
 - *Reliability:* Are the BMDS elements, sensors, and components sufficiently reliable to provide a credible defense?
 - *Availability:* Are the BMDS elements, sensors, and components sufficiently available for operations to provide a credible defense?

- *Maintainability*: Are the BMDS elements, sensors, and components sufficiently maintainable so that the system downtime is short enough to maintain a credible 24/7 defensive posture?
- **Survivability**: Is the BMDS survivable against enemy attack or in its intended operating environment?
 - *Conventional Attack*: Is the BMDS survivable against or vulnerable to conventional enemy attack?
 - *Intended Operating Environment*: Are the BMDS elements, sensors, and components survivable in their intended operating environments?

Like the previous FY08-10 DOT&E reports, the COIs in the FY07 report are considered here to characterize the current performance of the BMDS. The COIs are applied to each of the BMDS threat classes. The characterization adopts categories of “Good,” “Fair,” “Limited,” and “Not Characterized” (see Appendix A for the category definitions). Using these categories, Appendix A provides the classified characterization of the COIs for each of the four threat classes. For Patriot, however, the characterization categories of “Requirements Met,” “Requirements Partially Met,” and “Requirements Not Met” are used, since test results can be directly compared to the requirements found in the U.S. Army Patriot Operational Requirements Document. Data sources considered in the characterization include flight tests, ground tests, wargames/capability demonstrations, models and simulations, and real-world events that employed the threat-class defense elements and components.

Confidence intervals are provided wherever sufficient data are available to derive a point estimate of capability and to bound the range of uncertainty. Where test data are insufficient to quantify capability using numerical statistics, the use of this term is avoided.

The FY10 version of this report described a method DOT&E developed for estimating the probability of engagement success for the BMDS weapon elements for which sufficient data have been collected to perform a more quantitative assessment. Weapon elements that have collected sufficient data to perform a quantitative assessment have generally achieved a progress demonstration level of at least 5 (see Section Three for progress demonstration level definitions). This methodology was applied to Aegis BMD 3.6.1 in the FY10 report. During FY11, enhancements were made to this methodology to incorporate additional mathematical and statistical rigor into the estimation of the probability of engagement success and to produce less conservative, though still accurate, confidence intervals in most cases.

The enhanced methodology continues to incorporate end-to-end flight test data, ground test data, and component tests such as tracking exercises and interceptor-only flight tests to the maximum extent possible. The probability of engagement success estimates generated by the enhanced methodology continues to be applicable only to the portion of the BMDS weapon element battlespace that has been sampled through flight, ground, and component testing. Thus, DOT&E’s estimates are referred to as the probability of engagement success for the tested battlespace (PES-TB). Estimates of PES-TB do not obviate the need for robust operational testing, models and simulations accredited for performance assessment, or probability of

engagement success estimates from other organizations such as the Missile Defense Agency (MDA) or the BMDS Operational Test Agency Team. DOT&E's PES-TB estimates are independent inputs to the on-going process of determining the current probability of engagement success throughout the entire BMDS weapon element battlespace as each of the weapon elements matures through its life cycle.

DOT&E's methodology starts by defining PES-TB as the ratio of the number of reentry vehicles killed during test events to the total number of reentry vehicles presented to the system during testing. This ratio definition does not provide a means to incorporate component-level testing, so DOT&E replaced the single ratio estimate with the product of multiple ratios corresponding to critical steps in a missile defense engagement. This product of multiple ratios reduces to the single ratio definition of PES-TB when the test program consists entirely of end-to-end flight test data. In FY10, missile defense engagements were broken down into 10 critical steps. The FY11 enhancements to the PES-TB methodology now allow for different numbers of critical steps for each weapon element, or the number of critical steps can be tailored specifically for a portion of the weapon element's battlespace.

The estimate for PES-TB is computed by first estimating the value of the ratios for the critical engagement steps based on the available end-to-end and partial flight and ground test data. The process for estimating these ratios improved during FY11. In FY10, the ratios were estimated using a subset of the available data to preserve any correlations between successive engagement steps. Now the ratios are computed using all the available data through a modified version of the Horvitz-Thompson estimator commonly used in simple random survey sampling. This modified version of the Horvitz-Thompson estimator uses inverse probability weighting to account for the different amounts of correlated test data available for each ratio and then corrects the estimate based on the remaining uncorrelated test data. The estimate for PES-TB is computed by multiplying the values of each ratio together. Confidence intervals for the PES-TB estimate are computed based on the number of end-to-end flight tests. They are the limiting factor for several of the ratios, which make them the primary contributor to the uncertainty in the PES-TB estimate. The enhanced PES-TB methodology is described in more detail in classified Appendix B.

The following discussion provides an unclassified summary of the characterization of threat-class defense performance with specific examples of demonstrated capabilities. The Aegis BMD 5.1/5.1x systems are in the early stages of development. Thus, no characterizations for these builds are possible. Aegis BMD 5.1/5.1x will not be discussed.

Threat-Class Defense Performance Characterization

SRBM

Aegis BMD (SRBM)

Build 3.6.1

Aegis BMD 3.6.1 has demonstrated a capability to engage non-separating SRBM threats in the midcourse phase of flight using SM-3 Block IA interceptors and non-separating SRBMs in

the terminal phase of flight using modified SM-2 Block IV interceptors. An earlier variant, Aegis BMD 3.6, had the same midcourse phase capability as the Aegis BMD 3.6.1 build, but lacked the terminal phase capability. Aegis 3.6.1 is the currently deployed build.

The characterization of Aegis BMD SRBM engagement capability is based primarily on results from three of the six test missions that comprised the combined Developmental Test/Operational Test (DT/OT) phase for Aegis BMD 3.6 and on three follow-on test and evaluation (FOT&E) missions for Aegis BMD 3.6.1. DT/OT included a maintenance demonstration and other in-port and at-sea opportunities to collect data on reliability, maintainability, availability, and other suitability measures. FOT&E for Aegis BMD 3.6.1 also provided opportunities to collect data on system suitability and survivability. Results from six DT flight tests before combined DT/OT, a U.S. Navy Fleet exercise, and other applicable test data are all considered as appropriate.

Effectiveness

Aegis BMD has demonstrated the capability to detect, track, and engage non-separating SRBMs in the midcourse phase of flight. In total, Aegis BMD ships intercepted 10 out of 13 non-separating SRBMs (two of which were engaged simultaneously) in the midcourse phase. Five of the 13 midcourse-phase engagements were attempted with SM-3 Block IA interceptors fired from Aegis BMD 3.6 or 3.6.1 ships. The Navy Commander Operational Test and Evaluation Force (COMOPTEVFOR), in its DT/OT operational assessment report, determined that these interceptors, along with Aegis BMD 3.6, are operationally effective for the SRBM mission.²² The sole FOT&E mission against a non-separating SRBM target was successful, confirming SRBM mission capability after the 3.6.1 upgrade. COMOPTEVFOR, in its follow-on evaluation report, declared the Aegis BMD 3.6.1 SRBM engagement capability to be operationally effective.²³ Appendix B includes DOT&E's estimate for the Aegis BMD PES-TB for SRBM threats engaged in the midcourse phase of flight.

For the first of the failed intercept attempts, a kinetic warhead divert valve malfunctioned. Following this failure, the program replaced the old divert valve with one incorporating a new design. The MDA attributed the failure during the second failed flight test to incorrect fire control input parameters set by the operators. The U.S. Navy implemented subsequent training and software changes intended to prevent this from occurring in the future. The MDA attributed the third failure, which took place during a recent U.S. Navy Fleet exercise, to manufacturing procedures applicable to the Block I missile that do not apply to current Block IA interceptors.

For the terminal phase mission, flight testing during Aegis BMD 3.6.1 FOT&E demonstrated Aegis BMD's capability to engage non-separating SRBMs in the terminal phase

²² Aegis Ballistic Missile Defense (BMD) Operational Test Agency Evaluation Report, Block 04 3.6 System Final Report to the Chief of Naval Operations, COMOPTEVFOR, October 27, 2008.

²³ Aegis Ballistic Missile Defense (BMD) 3.6.1 System Operational Test Agency Follow-on Evaluation Report to the Chief of Naval Operations, COMOPTEVFOR, December 20, 2011.

with modified Standard Missile (SM)-2 Block IV interceptors. Aegis BMD ships intercepted all (two out of two) non-separating SRBMs in the terminal phase during FOT&E missions. An early developmental flight test demonstration of the sea-based terminal capability with modified SM-2 Block IV interceptors adds further certainty in the capability. Additional flight testing of the sea-based terminal capability would allow for a better characterization of effectiveness, but that might not be practical given the limited inventory of SM-2 Block IV interceptors, which are no longer in production.

Suitability

Analyses of data obtained during DT/OT and FOT&E flight missions, at-sea events, and the maintenance demonstration suggest that the Aegis BMD 3.6.1 system is suitable to meet operational availability specifications. Operational testers observed numerous software critical failures during Aegis BMD 3.6 DT/OT and BMD 3.6.1 FOT&E testing, especially in relation to command, control, communications, computers, and intelligence (C4I) systems, but the system still meets the U.S. Navy's availability needs. In its CY08 Aegis BMD 3.6 operational assessment, COMOPTEVFOR declared the system to be operationally suitable for its mission to engage SRBMs. The update to Aegis BMD 3.6.1 corrected a number of the suitability issues found during Aegis BMD 3.6 DT/OT testing, though the overall suitability measure of performance for the mean time between computer program mission critical events still does not meet the U. S. Navy requirement (due in large part to the C4I system). COMOPTEVFOR's follow-on evaluation report assesses the 3.6.1 system as operationally suitable for SRBM engagements.

Survivability

Although not stressing, multi-warfare exercises during DT/OT (midcourse missions) and FOT&E (terminal missions) demonstrated a capability to perform simultaneous anti-air warfare ship self-defense and BMD functionality. Exercises during DT/OT and FOT&E also demonstrated the retention of legacy Aegis ship missions such as Tomahawk strike (via simulation) and undersea warfare engagement.

Testing to date occurred during available weather conditions, which in most cases did not reach stressing levels of rain, sea state, or other environmental conditions. As a result, characterizing survivability under extreme environmental conditions is not possible. Aegis BMD obtained some experience in system survivability at high sea states during one of the recent sea-based terminal engagement missions. Other environmental testing shortfalls that limit an assessment of overall system survivability include tests to determine the effects of nuclear, biological, and chemical environments, as well as realistic testing conducted in a Global Positioning System-denied environment.

Aegis BMD has performed sufficient information assurance testing at the developmental level for the system to be granted an authority to operate. However, the MDA has not yet conducted important penetration and exploitation testing. This and more testing is necessary to characterize the information assurance survivability of the system with certainty.

Build 4.0.1

Aegis BMD 4.0.1 introduces the capability to engage more complicated SRBM threats in the midcourse phase of flight using SM-3 Block IB interceptors. It is worth noting here that the Aegis BMD 4.0.1 system will eventually be converted to an open architecture; this version, Aegis BMD 5.0, will have the same midcourse BMD capabilities as build 4.0.1. Build 5.0 will also include the sea-based terminal capability resident in build 3.6.1 and is planned to include the first increment of an enhanced sea-based terminal capability with SM-6 interceptors.

Effectiveness

Aegis BMD 4.0.1 capabilities that further enhance SRBM engagements are still in the early stages of developmental testing; thus, a characterization of effectiveness cannot be made. During recent test events, the MDA has conducted at-sea tracking exercises and simulated engagements of simple and complex SRBM targets in the midcourse phase using an engineering load of the Aegis BMD 4.0.1 system. Preliminary results are encouraging.

Aegis BMD 5.0 sea-based terminal capabilities are in the early stages of development and cannot be characterized at this time.

Suitability

The Aegis BMD 4.0.1 system is in the early stages of developmental testing. No statements are possible regarding overall operational suitability of this system.

Survivability

The Aegis BMD 4.0.1 system is in the early stages of developmental testing. No statements are possible regarding overall operational survivability of this system.

THAAD (TFCC 5.2) (SRBM)

An U.S. Army materiel release decision for the first two THAAD fire units is scheduled for February 2012. These first fire units are designed to have capability against SRBMs and MRBMs in the late midcourse and terminal phases of flight. For these first two units, each battery is comprised of 24 interceptors, three mobile launchers capable of holding eight interceptors each, a radar, a fire control unit, and battery support equipment. Follow-on batteries are planned for fielding starting in FY15, and these batteries are planned to have six launchers each with the corresponding 48 missiles. The first two batteries will eventually be backfilled with the additional launchers and missiles as well. Fielding of the first batteries in FY12 will support MDA's Partial Capability Delivery status for THAAD. In the interim, the U. S. Army has declared a THAAD Minimum Engagement Package available for emergency activation if requested by the Combatant Commanders.

This report characterizes THAAD capability against SRBMs using primarily intercept flight tests against threat-representative targets, currently seven flight tests (FTT-06 through FTT-10a, FTT-12, and FTT-14). FTT-10a was a DT/OT flight test and FTT-12 was an IOT&E. All of these flight tests were against short-range targets, although two targets exhibited medium-range target characteristics. This report also considers data from other tests, such as early

THAAD flight tests, live fire test and evaluation, ground qualification testing, and track exchange exercises with Aegis BMD.

Effectiveness

Currently, THAAD has demonstrated the capability to detect, track, and engage short-range non-separating and short-range simple separating targets. In seven flight tests, THAAD intercepted six of six short-range non-separating ballistic missiles and three of three short-range simple separating ballistic missiles. One flight test (FTT-10) demonstrated a salvo engagement of two THAAD interceptors against a single target, which is consistent with some tactical operations. Another flight test (FTT-12) demonstrated a multiple simultaneous engagement of two THAAD interceptors against two targets. THAAD has also demonstrated a capability to intercept threat missiles both inside and outside the atmosphere, the only BMDS weapon element specifically designed with this capability.

FTT-12, the IOT&E flight test, used field-representative hardware and software in an operationally realistic manner. However, the MDA has not invoked the advanced radar algorithms required for full discrimination capability during an intercept flight test, because the target types flown to date have not required them. A test that is expected to invoke the algorithms is scheduled for FY14.

In FY/CY11, the THAAD battlespace that has been explored in testing expanded. FTT-12 provided information about multiple simultaneous engagements and intercepts occurring far off the radar boresight. A full characterization of effectiveness against SRBMs, however, will require flight tests using the radar advanced algorithms against more complex SRBMs.

Appendix B includes DOT&E's estimate for the probability of engagement success for simple SRBM threats engaged by THAAD.

Suitability

Analyses of data obtained during testing, including the Reliability Confidence Test and FTT-12, suggest that the system components generally have adequate mean time between essential function failures and mean time to repair values. Additional classified metrics are provided in Appendix A. A number of shortfalls that affect sustainability, however, were identified in the documentation (manuals and users guides), and the built-in-test capability has a high false failure rate. The division of labor between Soldiers, contractor support, and reach-back contractor support is also heavily skewed toward reach-back contractor support. The procedures and triggers for this support are not clearly defined. FTT-12 demonstrated that the spares transport shelter is not large enough to support the amount of spares required for deployment.

Mobility and transportability testing were largely successful, and march order times were reasonable, indicating that the system is generally capable of movement and maneuver. Demonstrated timelines for site selection and emplacement, however, were excessively long because of a lack of proper tools and procedures.

The reporting of the operational capability of the system components to the fire control officer is insufficient to assess the status of the equipment. Specific instances of incorrect and inconsistent reporting were observed during testing. Some critical faults were not relayed through the system at all. The user interface on the radar operator screens is also insufficient to prevent accidental system shutdown.

Few health and safety concerns were uncovered in testing, suggesting the system is generally safe to operate and presents little undue health hazard.

The current THAAD personnel structure is not adequate to assure timely and sufficient deployment and operation of a THAAD battery because of the lack of a battalion support structure, forcing Soldiers to assume battalion duties without formal training. Training is also lacking at both the THAAD battery level and at command levels above THAAD. Some training aids and devices are also not available and not currently resourced.

Natural environments testing subjected THAAD to temperature extremes, temperature shock, humidity, rain, ice, snow, sand, dust, and wind. The MDA found deficiencies in all areas except for wind, resulting in many redesign recommendations. Until the MDA implements redesigns, the system may experience excessive faults and repairs in inclement weather.

Additional details on these issues and an assessment of THAAD interoperability with other BMDS elements are discussed in Appendix A.

Survivability

THAAD has completed testing and analysis to determine survivability to hostile environments, including exposure to chemical, biological, and radiological exposure and electromagnetic environmental effects; and to a direct information assurance attack, including insider and outsider computer network attacks and computer network exploitation. Testing has not been performed in an electronic countermeasure environment.

Subject matter experts from the U.S. Army West Desert Test Center determined that the THAAD system can be decontaminated from exposure to chemical, biological, and radiological elements within the U.S. Army-approved contamination criteria timeline, as long as separate teams work on each major component simultaneously. The THAAD system is also expected to meet the materiel hardness criterion and the compatibility criterion that specified minimum degradation of crew performance while wearing protective gear.

THAAD underwent sufficient information assurance testing for the system to be granted an interim authority to operate. The MDA Chief Information Officer has granted individual Authorities to Operate for the THAAD launcher, radar, fire control unit, and battery support center. The results of the information assurance testing, as well as the electromagnetic environmental effects testing, are included in Appendix A.

Patriot (Post Deployment Build (PDB)-6.5) (SRBM)

The Patriot configuration characterized in this report uses PDB-6.5 system software. The characterization is based primarily on Patriot performance against tactical ballistic missiles during the PDB-6.5 Limited User Test, conducted between November 2009 and July 2010.

Effectiveness

Patriot met the Operational Requirements Document system effectiveness and defended area Key Performance Parameter requirements against some tactical ballistic missiles but failed to meet the requirements against others (see Appendix A for classified details).

Suitability

Patriot did not meet its operational requirements for reliability or availability during the PDB-6.5 Limited User Test. The U.S. Army did not test Patriot maintainability during the PDB 6.5 Limited User Test and the system did not meet the requirement in this area during the PDB-6 Limited User Test. Patriot supportability and transportability were satisfied through testing prior to the IOT&E in 2002.

Patriot met some of its manpower, personnel, and means of employment requirements. However, PDB-6.5 software increases operator workload and requires additional manpower. The Limited User Test highlighted the growing complexity of the Patriot system, which requires a higher level of operator expertise that exceeds the current U.S. Army training standard.

Survivability

The assessment of Patriot survivability against anti-radiation missiles is contained in Appendix A. The U.S. Army did not test counter-reconnaissance, surveillance, and target acquisition, electronic countermeasure environments, or ballistic threats, during the PDB 6.5 Limited User Test. Therefore, DOT&E cannot characterize Patriot survivability in these areas.

Although Patriot information assurance infrastructure and management improved between PDB-6 and PDB-6.5 testing, these areas require further improvement. The Patriot System does not meet certain electromagnetic environments added after the Army designed and tested the Patriot System. The Army added new specifications to the Patriot system specification. The Patriot System does not comply with certain BMDS nuclear, biological, and chemical environmental requirements that differ from the Army requirements. Patriot, being a legacy system, did not meet the BMDS or certain US Army Nuclear and Chemical Agency (USANCA) requirements. The Army granted a waiver for the deficient requirements. The USANCA supported that waiver.

MRBM

Aegis BMD (MRBM)

Build 3.6.1

Aegis BMD 3.6.1 has demonstrated a capability to engage simple separating MRBM threats in the midcourse phase of flight using SM-3 Block IA interceptors. The Aegis 3.6.1 terminal phase engagement capability does not address MRBM threats.

The characterization of Aegis BMD MRBM engagement capabilities is based primarily on results from three of the six test events that composed the combined DT/OT phase for Aegis BMD 3.6, on an FOT&E multi-target tracking event, and on a system-level IRBM intercept mission including Aegis BMD 3.6.1. Aegis BMD 3.6 DT/OT and Aegis BMD 3.6.1 FOT&E included a maintenance demonstration and other opportunities to collect data on reliability,

maintainability, availability, and other suitability measures that are also applicable to an MRBM characterization. Results from Japanese Aegis BMD tests and one developmental flight test before the combined DT/OT phase are considered when appropriate, as are results from other target-of-opportunity flight tests and a recent Aegis BMD 4.0.1 developmental test (considering common components only).

Effectiveness

Aegis BMD has demonstrated the capability to detect, track, and engage simple separating ballistic missile threats in the midcourse phase of flight at the lower threshold of the medium-range band. In total, U.S. Navy Aegis BMD ships intercepted three out of three simple separating ballistic missile targets with ranges just below 1,000 kilometers, and one out of one MRBM targets presenting an unintentionally complex scene. Three of the four engagements were made with SM-3 Block IA interceptors. Using SM-3 Block IA interceptors, Japanese Aegis BMD ships intercepted three out of four simple separating ballistic missile targets identical to those used for U.S. Aegis BMD flight tests.²⁴ COMOPTEVFOR declared the engagement capability against threats similar to the targets tested against to be operationally effective in its CY08 DT/OT and CY11 Follow-on Operational Test and Evaluation assessment reports.

It is worth noting that the sub-1,000 kilometer threat surrogates used in testing, while SRBMs in terms of range, are essentially SRBMs with MRBM characteristics. The surrogates' characteristics and ranges are not significantly different from those of the 1,000- to 1,300-kilometer range threats, expected in the real-world defense scenarios that the Aegis BMD element was designed to counter. As such, it is reasonable to extrapolate performance into the lower end of the medium-range band.

The new EPAA Phase 1 architecture for missile defense in Europe will include Aegis BMD 3.6.1 ships in defense of locations that could require external sensor-to-ship coordinated engagements of threats with ranges well into the medium-range band. In FY11, the MDA conducted a flight test against an IRBM target that demonstrated this type of engagement capability. Although the test was conducted against an IRBM target, the results have application to MRBM threats at the upper threshold of the medium-range band. Overall certainty in this type of engagement capability is limited, however, because only one intercept mission against upper threshold MRBM or IRBM targets has been attempted.

Appendix B includes DOT&E's estimate for the Aegis BMD PES-TB for lower-range threshold MRBMs engaged in the midcourse phase of flight. Appendix C characterizes European Phased Adaptive Approach (EPAA) Phase 1 capability and includes a PES-TB estimate for upper-range threshold MRBM engagements like those expected in defense of Europe.

²⁴ The lone failure seen during Japanese Aegis BMD flight test was due to a malfunctioning valve in the SM-3 Block IA kinetic warhead divert system.

Suitability

The discussion of suitability given for the 3.6.1 system for SRBM engagements also applies to MRBM engagements when considering an Aegis BMD ship's ability to conduct an engagement. However, engagements against longer-ranged MRBMs would typically take place with a more complicated architecture (possibly with multiple sensors). Although one flight test and a number of ground tests have demonstrated the ability of the elements and sensors needed for such an engagement to interoperate, testing showed that improvements need to be made concerning interoperability.

Survivability

The discussion of survivability given for the 3.6.1 system for SRBMs also applies to MRBMs.

Build 4.0.1

Aegis BMD 4.0.1 (and 5.0 with the switch to an open architecture) introduces the capability to engage more complicated MRBM threats in the midcourse phase of flight using SM-3 Block IB interceptors. The first increment of the enhanced sea-based terminal capability with SM-6 interceptors adds the capability to engage a limited set of MRBM threats.

Effectiveness

Aegis BMD 4.0.1 capabilities that further enhance MRBM engagements are still in the early stages of developmental testing. As a result, a characterization of effectiveness cannot be made at this time.

There has been only one intercept test with the BMD 4.0.1 system, during which the SM-3 Block IB interceptor failed to intercept an SRBM-ranged target with MRBM-like characteristics. Although the primary objective of the mission was not met, many of the new capabilities of the Aegis BMD 4.0.1 system and SM-3 Block IB interceptor performed well. The performance of the new BMD 4.0.1 software during the intercept mission continued the good performance observed during a number of recent at-sea tracking exercises and simulated engagements against MRBM-like targets.

It should be noted that the failure in the recent Aegis BMD 4.0.1 developmental flight test slightly lowers overall certainty in the midcourse engagement capability of Aegis BMD 3.6.1 due to fact that the failure in the test is related to a component that both systems share in common. The MDA is currently investigating the root cause of the failure.

Suitability

The Aegis BMD 4.0.1 system is in the early stages of developmental testing. No statements are possible regarding overall operational suitability of the system. However, it should be noted that the failure in the recent intercept test with the 4.0.1 system and SM-3 Block IB interceptor might be related to a suitability issue. The MDA is currently investigating root cause of the failure.

Survivability

Aegis BMD 4.0.1 is in the early stages of developmental testing. No statements are possible regarding overall operational survivability of the system.

THAAD (TFCC 5.2) (MRBM)

As mentioned above, the THAAD batteries planned for materiel release in February 2012 are designed to have capability against both SRBMs and MRBMs. This report characterizes THAAD capability against MRBMs using primarily FTT-09 and FTT-12, although all intercept flight tests against threat-representative targets are relevant. The targets in FTT-09 and FTT-12 flew short-range trajectories, but each had a target that exhibited primarily medium-range target characteristics. Where applicable, this assessment also considers data from other tests, such as early THAAD flight tests, ground qualification testing, and track exchange exercises with Aegis BMD.

Effectiveness

THAAD has demonstrated the ability to detect, track, and engage two short-range simple separating targets replicating some medium-range target endgame performance characteristics. THAAD demonstrated this capability with two intercepts inside the atmosphere. This test, along with aspects of the other THAAD flight tests, point toward an initial capability against MRBMs for THAAD, but the MDA needs to complete more testing for a comprehensive characterization.

As for SRBMs, the use of field-representative hardware and software in an operationally realistic manner in FTT-12 provided additional battlespace information that also has relevance for MRBMs. A characterization of effectiveness against MRBMs, however, will need to include longer-range and more complex targets, and exploration of parts of the battlespace particularly relevant to these longer, faster threats.

Suitability

The section on the THAAD suitability characterization for SRBMs is equally applicable to MRBMs, since the system is designed for both short- and medium-range threats.

Survivability

The section on the THAAD survivability characterization for SRBMs is equally applicable to MRBMs, since the system is designed for both short- and medium-range threats.

Patriot (PDB-6.5) (MRBM)

The Patriot MRBM categorization is identical to the Patriot SRBM characterization. Therefore, it is not repeated here.

IRBM

GMD (GFC 6B) (IRBM)

GMD has demonstrated a limited capability to defend western Alaska, including the Aleutian Islands, against small numbers of simple IRBM threats.

The characterization of GMD IRBM engagement capabilities is based primarily on the engagement planning and interceptor launch and flyouts in FTG-06 and FTG-06a; GMD flight tests in FY06-09; and prior ground tests including GTD-04b within a small set of IRBM threat scenarios. The suitability characterization is based on data acquired during developmental and operational tests, operational exercises, and real-time operations. Currently, a limited quantity of suitability data exists. The survivability characterization suffers from significant data gaps that are identified in the BMDS Integrated Master Test Plan. The MDA plans to acquire additional survivability data, mostly from component level tests.

Effectiveness

The GMD element achieved intercepts in three of the five most recent intercept flight test attempts to date against IRBM range targets.²⁵ The three successful tests occurred first and employed interceptors equipped with Capability Enhancement-I (CE-I) Exoatmospheric Kills Vehicles (CE-I EKV). The two more recent tests failed; these tests employed interceptors equipped with the CE-II EKVs. Failure investigation teams were convened after each failure. The first investigation team concluded that a quality control process failure in the manufacture of the test EKV caused the first failure. The results of the second are discussed in Appendix A.

A quantitative assessment of the operational effectiveness of GMD against IRBM threats is currently not possible. As discussed previously, additional flight tests are needed to provide data for verification, validation, and accreditation (VV&A) of models and simulations. Greater operational realism in the intercept flight tests is also needed. Ground tests did not investigate a wide range of unfavorable adversarial tactics and threat countermeasures or the range of possible unfavorable threat missile behaviors and phenomenology. More fundamentally, the models and simulations employed in ground tests lacked accreditation for performance assessment.

A GMD defense capability against IRBMs is limited to threat missiles launched from North Korea. Figure 5-1 shows the maximum defined IRBM range of 5,500 kilometers for missiles launched from North Korea and Iran.²⁶ Maximum-range IRBMs from North Korea could reach western Alaska, including the Aleutian Islands, and several U.S. territories in the Pacific Ocean, including Guam. The GMD element can provide a defense of western Alaska, including the Aleutian Islands, but since the U.S. territories in the Pacific Ocean are closer to North Korea than they are to either of the GMD missile fields, these U.S. territories would need to be defended by other means. Aegis BMD, because it is a mobile asset, is the only element that can provide defense against IRBMs for the rest of the world (limited by its operating area). Therefore, in the characterization in Appendix A of BMDS defensive capability against IRBMs, the GMD IRBM characterization is specific to the defense of western Alaska, including the

²⁵ The prior set of intercept flight test attempts achieved five intercepts in ten attempts. Although these tests employed prototype EKVs and exercised portions of the GMD infrastructure, the tests employed surrogate interceptor boost vehicles and did not employ operationally-representative midcourse sensors.

²⁶ An arbitrary launch point was selected within each country for (unclassified) illustration purposes. Defense Intelligence estimates of specific IRBM range capabilities of North Korea and Iran might be shorter than the maximum defined IRBM range.

Aleutian Islands, and the Aegis BMD IRBM characterization covers the defense of all other areas.

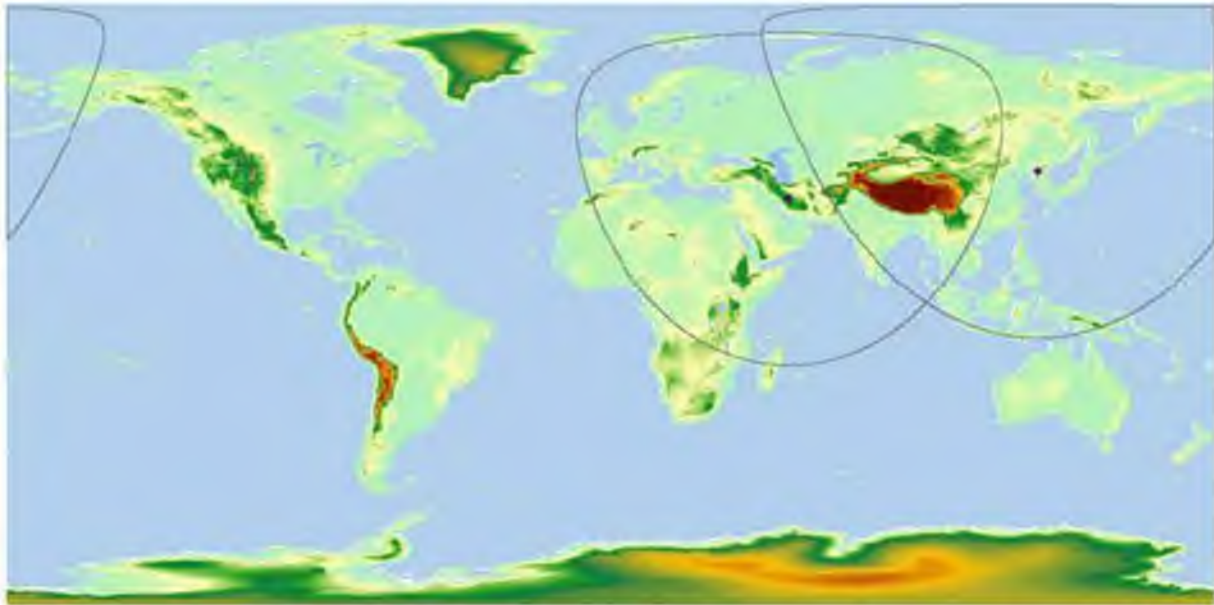


Figure 5-1. The Maximum Defined IRBM Range of 5,500 Kilometers for Missiles Launched from North Korea and Iran

Suitability

GMD element interoperability with BMDS sensors, C2BMC, and Aegis BMD and interoperability between the Ground-Based Interceptor (GBI) missile fields and GFC are good based on the data acquired in ground tests and intercept flight tests. These tests exercised the GMD communications network, portions of which are exercised on a daily basis.

GMD reliability and availability are limited but are adequate to engage a small number of threat missiles. The MDA has delivered and fielded GBIs concurrent with flight testing. GBI configuration changes based on flight test discovery have occurred “on-the-fly,” so that many fielded GBIs incorporate hardware variations. The MDA has continued its GBI refurbishment effort and plans to standardize the configurations of the fielded GBIs over a period of years.

GMD maintainability is limited. Discoveries during recent flight testing will likely require refurbishment of emplaced interceptors. It is unclear at this time whether the refurbishment can be accomplished at the missile field, or whether the missiles will need to be shipped elsewhere for refurbishment. Sea-Based X-band (SBX) radar and platform maintainability are also limited. Maintenance requirements can result in the non-availability of the SBX radar for time periods of several months. The SBX radar and platform underwent a 6-month maintenance period in 2009 and a 3-month maintenance period in 2011. The MDA currently operates the SBX radar and platform; transition to the Navy is scheduled to occur in 2012.

Survivability

Survivability data on many GMD element components and supporting BMDS assets in chemical, nuclear, and biological environments are unavailable or only partially available. Tests, demonstrations, and exercises to acquire survivability data are being planned and included in the BMDS Integrated Master Test Plan.

Information assurance is limited primarily due to the lack of independent penetration testing. The GMD element has performed sufficient information assurance testing at the developmental level for the system to be granted an authority to operate. Initial penetration and exploitation testing of the system has been conducted.

The MDA is addressing GMD survivability assessment in a new solicitation for a GMD Development and Sustainment Contract. The recently awarded contract includes a requirement for a Survivability Assessment Report that would include a review of system threats, system performance issues, and system degradation or shortfalls. The MDA awarded this contract in December 2011.

Aegis BMD (IRBM)

Build 3.6.1

Aegis BMD 3.6.1 includes an initial capability to engage IRBM threats with SM-3 Block IA interceptors if an up-range radar is available and the ship is set up with remote engagements authorized. Primary data in support of a characterization of Aegis BMD 3.6.1 engagement capability against IRBMs comes from one system-level flight test and three simulated engagements against IRBM targets. Supporting data comes from ground test engagements.

Effectiveness

The MDA demonstrated Aegis BMD 3.6.1 initial launch-on-remote capability against IRBMs in an intercept test in FY11. The flight test was an important demonstration of missile defense capabilities needed for EPAA Phase 1 missile defense in Europe. As mentioned under the MRBM discussion above, overall certainty in the use of Aegis BMD 3.6.1 for long-range engagements is limited, however, because only one intercept engagement of that type has been attempted. See classified Appendix C for an assessment of EPAA Phase 1.

Suitability

The discussion regarding Aegis BMD 3.6.1 suitability for SRBM and MRBM engagements also applies to IRBM engagements.

Survivability

The discussion of survivability given for the 3.6.1 system for SRBMs and MRBMs also applies to IRBMs.

Build 4.0.1

Aegis BMD 4.0.1 (and 5.0 with the switch to open architecture) introduces an enhanced capability to engage a limited set of IRBM threats in the midcourse phase of flight using SM-3 Block IB interceptors.

Effectiveness

Aegis BMD 4.0.1 capabilities that further enhance IRBM engagements are still in the early stages of developmental testing, and no flight tests exercising this capability have yet taken place. As a result, a characterization of effectiveness cannot be made.

Suitability

The Aegis BMD 4.0.1 system is in the early stages of developmental testing. No statements are possible regarding overall operational suitability of the system.

Survivability

Aegis BMD 4.0.1 is in the early stages of developmental testing. No statements are possible regarding overall operational survivability of the system.

ICBM

GMD (GFC 6B) (ICBM)

The GMD element is the sole weapon system that currently provides a capability to defend the U.S. Homeland against ICBMs. GMD has demonstrated a limited capability for defense of the U.S. Homeland against small numbers of simple ICBMs launched from North Korea and Iran.

The characterization of GMD ICBM engagement capabilities is based primarily on the engagement planning and interceptor launch and flyouts in FTG-06 and FTG-06a; GMD flight tests in FY06-09; and prior ground tests and GTD-04b, within a small set of ICBM threat scenarios.

Effectiveness

The discussion presented in the IRBM section above is relevant here as well. The two most recent intercept flight tests were failures, which is an undesirable trend. A quantitative assessment of the effectiveness of the GMD element against ICBM threats is currently not possible for the reasons presented above in the IRBM section.

Suitability

GMD suitability for defense against ICBMs is the same as described previously in the IRBM section.

Survivability

GMD survivability for defense against ICBMs is the same as described previously in the IRBM section.

BMDS Battle Management Performance Characterization

Results from ground and flight testing to date indicate that C2BMC S6.4 has the ability to manage, in some cases, one or two AN/TPY-2 (FBM) radars by issuing sensor task plans and managing the utilization of sensor resources. Since the beginning of GT-04 campaign in FY10, the new S6.4 sensor management software, GEM, exercised the capability to control two

AN/TPY-2 (FBM) radars in several integrated and one distributed ground tests. GTD-04d Part 3 was the first attempt by C2BMC to manage multiple radars in a distributed test environment. However, the MDA has not demonstrated S6.4 sensor management functions in a flight test with multiple AN/TPY-2 (FBM) radars. Results from two flight tests and three distributed ground tests confirm the ability of S6.4 to manage a single AN/TPY-2 (FBM) radar.

The new EPAA Phase 1 architecture includes use of Aegis BMD launch-on-remote capabilities. Aegis BMD performed a launch-on-remote engagement against an IRBM-class target during FTM-15, in which an Aegis BMD 3.6.1 ship launched an interceptor based on a track from AN/TPY-2 (FBM) forwarded by C2BMC. Since FTM-15, several ground tests with varying representations of the EPAA Phase 1 architecture demonstrated this capability. There has been no demonstration of this capability using the full Phase 1 architecture with multiple AN/TPY-2 (FBM) radars and Aegis BMD ships in a flight test. THAAD does not currently have a launch-on-remote capability. Launch-on-remote will require modifications to the THAAD fire control software. Flight testing is not scheduled until FY14.

While the MDA has taken the first step toward system integration by providing situational awareness capability implemented as part of C2BMC software for the whole BMDS, there have been no flight tests to date to address BMDS battle management. In FY/CY11, C2BMC S6.4 demonstrated in ground and flight testing the ability to provide situational awareness and exchange track and status information with Aegis BMD, GMD, Patriot, THAAD, and Israeli Arrow Weapon System. S6.4 incorporates situational awareness improvements, including new logic for track correlation, fusion, and association with launch events. Additional testing using S6.4 software is needed to ensure that all participants exchange accurate and timely information. The validity of the weapon element models that provide input to C2BMC limit the testing of C2BMC situational awareness. Engagement direction capabilities of S6.4 software are rudimentary and will increase gradually over future software builds. Results from the last two ground test campaigns and FTT-14 indicate that peer-to-peer engagement coordination between THAAD and Patriot with C2BMC monitoring might be possible, but more flight and ground testing is needed as the MDA implements fixes and improvements.

Aegis BMD, GMD, Patriot, THAAD, Israeli Arrow, and C2BMC continue to assess the systems' interoperability in support of BMDS integration. The programs have addressed early shortfalls in the quality and formatting of target track and element status data, but new issues have emerged since the EPAA Phase 1 ground testing started. These issues are discussed in Appendix A.

This page intentionally left blank

Director, Operational Test and Evaluation
2011 Assessment of the Ballistic Missile Defense System (BMDS)

Classified Appendix A

Characterization of Operational Effectiveness, Suitability, and Survivability

Provided Under Separate Cover

This page intentionally left blank.

Director, Operational Test and Evaluation
Director, Operational Test and Evaluation
2011 Assessment of the Ballistic Missile Defense System (BMDS)

Classified Appendix B
Estimating the Probability of Engagement Success (PES)
for Aegis BMD and THAAD

Provided Under Separate Cover

This page intentionally left blank.

Director, Operational Test and Evaluation
2011 Assessment of the Ballistic Missile Defense System (BMDS)

Classified Appendix C

Operational Assessment of the European Phased Adaptive Approach (EPAA)
Phase I Architecture

Provided Under Separate Cover

This page intentionally left blank.





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

FEB 9 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

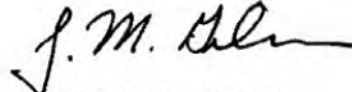
I have enclosed the 2011 Assessment of the Ballistic Missile Defense System (BMDS) required by the National Defense Authorization Act for Fiscal Year 2002, Section 232 (h), as amended by subsequent Acts. In the report, I conclude:

- Aegis BMD and Terminal High Altitude Area Defense (THAAD) demonstrated progress toward intermediate range and short range ballistic missile threat class capability, respectively. THAAD successfully completed an initial operational test and evaluation on which I will publish a separate report. However, Ground-based Midcourse Defense suffered a second consecutive flight test failure and did not demonstrate any progress toward intermediate range or intercontinental ballistic missile threat class capability. Command, Control, Battle Management, and Communications, for the first time, demonstrated the capability to control two operationally-deployed AN/TPY-2 radars in forward-based modes, using operational communications architectures, personnel, and tactics, techniques, and procedures.
- The testing conducted thus far on Phase 1 of the European Phased Adaptive Approach (EPAA) supports an assessment of capability demonstrated in a limited region of the EPAA's overall potential battlespace. I provide my assessment in Appendix C of this report.
- The MDA and the BMDS Operational Test Agency have now collected sufficient data to perform more quantitative assessments of Aegis BMD and THAAD. This report includes in, Appendix B, estimates of the probability of engagement success for the tested battlespace of these two weapon systems.
- Complete quantitative assessments of BMDS capability are still a number of years in the future. This is because it will take several more years to collect the test data needed to adequately verify, validate, and accredit the BMDS models and simulations required to perform such assessments. As data are collected, assessments will incrementally become more quantitative. In this report, Aegis BMD and THAAD reflect this progression

[REDACTED]

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Vice Chairman of the Joint Chiefs of Staff; the Director, Missile Defense Agency; and the Chairmen and Ranking Members of the Congressional defense committees.

This report is unclassified. Supporting information is contained in three classified appendices to this report.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable Adam Smith
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

FEB 9 2012

The Honorable C. W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

Dear Mr. Chairman:

I have enclosed the 2011 Assessment of the Ballistic Missile Defense System (BMDS) required by the National Defense Authorization Act for Fiscal Year 2002, Section 232 (h), as amended by subsequent Acts. In the report, I conclude:

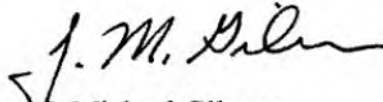
- Aegis BMD and Terminal High Altitude Area Defense (THAAD) demonstrated progress toward intermediate range and short range ballistic missile threat class capability, respectively. THAAD successfully completed an initial operational test and evaluation on which I will publish a separate report. However, Ground-based Midcourse Defense suffered a second consecutive flight test failure and did not demonstrate any progress toward intermediate range or intercontinental ballistic missile threat class capability. Command, Control, Battle Management, and Communications, for the first time, demonstrated the capability to control two operationally-deployed AN/TPY-2 radars in forward-based modes, using operational communications architectures, personnel, and tactics, techniques, and procedures.
- The testing conducted thus far on Phase 1 of the European Phased Adaptive Approach (EPAA) supports an assessment of capability demonstrated in a limited region of the EPAA's overall potential battlespace. I provide my assessment in Appendix C of this report.
- The MDA and the BMDS Operational Test Agency have now collected sufficient data to perform more quantitative assessments of Aegis BMD and THAAD. This report includes, in Appendix B, estimates of the probability of engagement success for the tested battlespace of these two weapon systems.
- Complete quantitative assessments of BMDS capability are still a number of years in the future. This is because it will take several more years to collect the test data needed to adequately verify, validate, and accredit the BMDS models and simulations required to perform such assessments. As data are collected, assessments will incrementally become more quantitative. In this report, Aegis BMD and THAAD reflect this progression.



[REDACTED]

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Vice Chairman of the Joint Chiefs of Staff; the Director, Missile Defense Agency; and the Chairmen and Ranking Members of the Congressional defense committees.

This report is unclassified. Supporting information is contained in three classified appendices to this report.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable Norman D. Dicks
Ranking Member



OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

FEB 9 2012

**OPERATIONAL TEST
AND EVALUATION**

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

Dear Mr. Chairman:

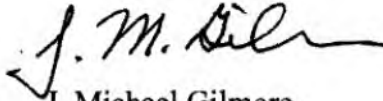
I have enclosed the 2011 Assessment of the Ballistic Missile Defense System (BMDS) required by the National Defense Authorization Act for Fiscal Year 2002, Section 232 (h), as amended by subsequent Acts. In the report, I conclude:

- Aegis BMD and Terminal High Altitude Area Defense (THAAD) demonstrated progress toward intermediate range and short range ballistic missile threat class capability, respectively. THAAD successfully completed an initial operational test and evaluation on which I will publish a separate report. However, Ground-based Midcourse Defense suffered a second consecutive flight test failure and did not demonstrate any progress toward intermediate range or intercontinental ballistic missile threat class capability. Command, Control, Battle Management, and Communications, for the first time, demonstrated the capability to control two operationally-deployed AN/TPY-2 radars in forward-based modes, using operational communications architectures, personnel, and tactics, techniques, and procedures.
- The testing conducted thus far on Phase 1 of the European Phased Adaptive Approach (EPAA) supports an assessment of capability demonstrated in a limited region of the EPAA's overall potential battlespace. I provide my assessment in Appendix C of this report.
- The MDA and the BMDS Operational Test Agency have now collected sufficient data to perform more quantitative assessments of Aegis BMD and THAAD. This report includes, in Appendix B, estimates of the probability of engagement success for the tested battlespace of these two weapon systems.
- Complete quantitative assessments of BMDS capability are still a number of years in the future. This is because it will take several more years to collect the test data needed to adequately verify, validate, and accredit the BMDS models and simulations required to perform such assessments. As data are collected, assessments will incrementally become more quantitative. In this report, Aegis BMD and THAAD reflect this progression.

[REDACTED]

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Vice Chairman of the Joint Chiefs of Staff; the Director, the Director, Missile Defense Agency; and the Chairmen and Ranking Members of the Congressional defense committees.

This report is unclassified. Supporting information is contained in three classified appendices to this report.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable John McCain
Ranking Member



OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

FEB 9 2012

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6025

Dear Mr. Chairman:

I have enclosed the 2011 Assessment of the Ballistic Missile Defense System (BMDS) required by the National Defense Authorization Act for Fiscal Year 2002, Section 232 (h), as amended by subsequent Acts. In the report, I conclude:

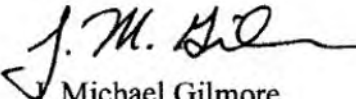
- Aegis BMD and Terminal High Altitude Area Defense (THAAD) demonstrated progress toward intermediate range and short range ballistic missile threat class capability, respectively. THAAD successfully completed an initial operational test and evaluation on which I will publish a separate report. However, Ground-based Midcourse Defense suffered a second consecutive flight test failure and did not demonstrate any progress toward intermediate range or intercontinental ballistic missile threat class capability. Command, Control, Battle Management, and Communications, for the first time, demonstrated the capability to control two operationally-deployed AN/TPY-2 radars in forward-based modes, using operational communications architectures, personnel, and tactics, techniques, and procedures.
- The testing conducted thus far on Phase 1 of the European Phased Adaptive Approach (EPAA) supports an assessment of capability demonstrated in a limited region of the EPAA's overall potential battlespace. I provide my assessment in Appendix C of this report.
- The MDA and the BMDS Operational Test Agency have now collected sufficient data to perform more quantitative assessments of Aegis BMD and THAAD. This report includes, in Appendix B, estimates of the probability of engagement success for the tested battlespace of these two weapon systems.
- Complete quantitative assessments of BMDS capability are still a number of years in the future. This is because it will take several more years to collect the test data needed to adequately verify, validate, and accredit the BMDS models and simulations required to perform such assessments. As data are collected, assessments will incrementally become more quantitative. In this report, Aegis BMD and THAAD reflect this progression.



[REDACTED]

Section 2399 provides that the Secretary of Defense may submit separate comments on my report, if he so desires. I have sent copies to him; the Under Secretary of Defense for Acquisition, Technology and Logistics; the Vice Chairman of the Joint Chiefs of Staff; the Director, Missile Defense Agency; and the Chairmen and Ranking Members of the Congressional defense committees.

This report is unclassified. Supporting information is contained in three classified appendices to this report.


J. Michael Gilmore
Director

Enclosure:
As stated

cc: The Honorable Thad Cochran
Ranking Member



OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 10 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Adam Smith
Ranking Member





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 10 2012

OPERATIONAL TEST
AND EVALUATION

The Honorable C.W. Bill Young
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6015

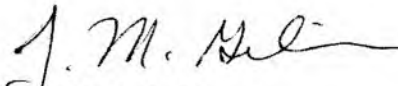
Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 10 2012

OPERATIONAL TEST
AND EVALUATION

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

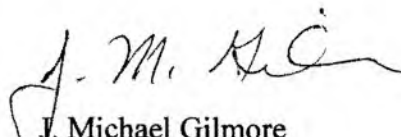
Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable John McCain
Ranking Member





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 10 2012

The Honorable Daniel K. Inouye
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6025

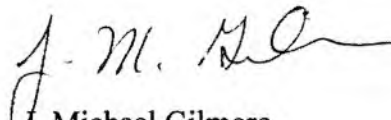
Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated

cc:
The Honorable Thad Cochran
Ranking Member





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Robert A. Brady
United States House of Representatives
102 Cannon House Office Building
Washington, DC 20515

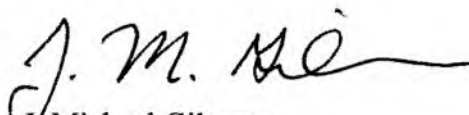
Dear Representative Brady:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Rick Larsen
United States House of Representatives
108 Cannon House Office Building
Washington, DC 20515

Dear Representative Larsen:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable James R. Langevin
United States House of Representatives
109 Cannon House Office Building
Washington, DC 20515

Dear Representative Langevin:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable W. Todd Akin
Chairman, Subcommittee on Seapower and Projection Forces
Committee on Armed Services
United States House of Representatives
117 Cannon House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

OPERATIONAL TEST
AND EVALUATION

The Honorable Joe Heck
United States House of Representatives
132 Cannon House Office Building
Washington, DC 20515

Dear Representative Heck:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

OPERATIONAL TEST
AND EVALUATION

The Honorable Mike Rogers
Chairman
Permanent Select Committee on Intelligence
United States House of Representatives
133 Cannon House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

OPERATIONAL TEST
AND EVALUATION

The Honorable Bill Shuster
United States House of Representatives
204 Cannon House Office Building
Washington, DC 20515

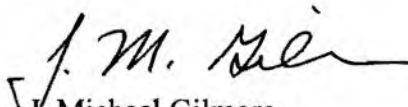
Dear Representative Shuster:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Joe Courtney
United States House of Representatives
215 Cannon House Office Building
Washington, DC 20515

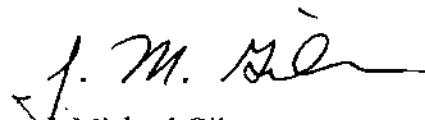
Dear Representative Courtney:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable Duncan Hunter
United States House of Representatives
223 Cannon House Office Building
Washington, DC 20515

Dear Representative Hunter:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

OPERATIONAL TEST
AND EVALUATION

The Honorable John Garamendi
United States House of Representatives
228 Cannon House Office Building
Washington, DC 20515

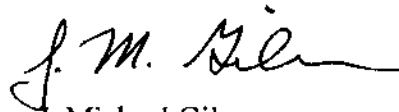
Dear Representative Garamendi:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

OPERATIONAL TEST
AND EVALUATION

The Honorable Nancy Pelosi
Minority Leader
United States House of Representatives
235 Cannon House Office Building
Washington, DC 20515

Dear Madam Minority Leader:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

OPERATIONAL TEST
AND EVALUATION

The Honorable Colleen Hanabusa
United States House of Representatives
238 Cannon House Office Building
Washington, DC 20515

Dear Representative Hanabusa:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Eric Cantor
Majority Leader
United States House of Representatives
303 Cannon House Office Building
Washington, DC 20515

Dear Mr. Majority Leader:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Kay Granger
United States House of Representatives
320 Cannon House Office Building
Washington, DC 20515

Dear Representative Granger:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Mike Rogers
United States House of Representatives
324 Cannon House Office Building
Washington, DC 20515

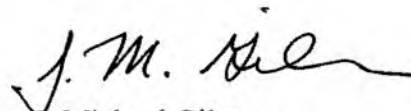
Dear Representative Rogers:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Scott Rigell
United States House of Representatives
327 Cannon House Office Building
Washington, DC 20515

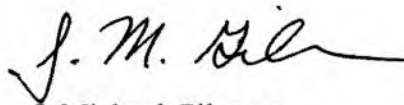
Dear Representative Rigell:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Steve Palazzo
United States House of Representatives
331 Cannon House Office Building
Washington, DC 20515

Dear Representative Palazzo:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Martin Heinrich
United States House of Representatives
336 Cannon House Office Building
Washington, DC 20515

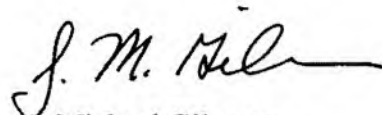
Dear Representative Heinrich:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Peter T. King
Chairman
Committee on Homeland Security
United States House of Representatives
339 Cannon House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Martha Roby
United States House of Representatives
414 Cannon House Office Building
Washington, DC 20515

Dear Representative Roby:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable John C. Fleming
United States House of Representatives
416 Cannon House Office Building
Washington, DC 20515

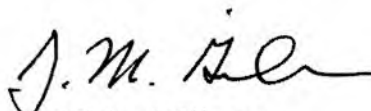
Dear Representative Fleming:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable William L. Owens
United States House of Representatives
431 Cannon House Office Building
Washington, DC 20515

Dear Representative Owens:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Doug Lamborn
United States House of Representatives
437 Cannon House Office Building
Washington, DC 20515

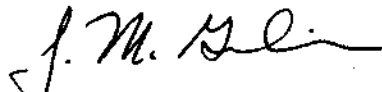
Dear Representative Lamborn:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Ander Crenshaw
United States House of Representatives
440 Cannon House Office Building
Washington, DC 20515

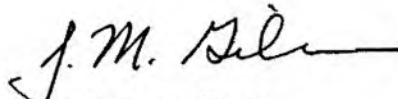
Dear Representative Crenshaw:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Chris Gibson
United States House of Representatives
502 Cannon House Office Building
Washington, DC 20515

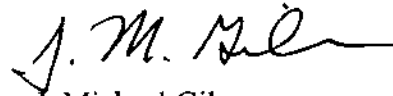
Dear Representative Gibson:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Bobby Schilling
United States House of Representatives
507 Cannon House Office Building
Washington, DC 20515

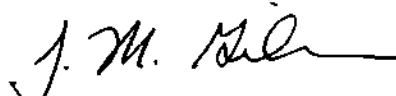
Dear Representative Schilling:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Austin Scott
United States House of Representatives
516 Cannon House Office Building
Washington, DC 20515

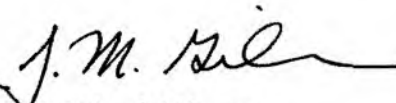
Dear Representative Scott:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Joseph R. Biden, Jr.
President of the Senate
United States Senate
S-212 Capitol Senate Office Building
Washington, DC 20510

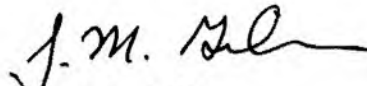
Dear Mr. President:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Scott Brown
Ranking Member, Subcommittee on Airland
Committee on Armed Services
United States Senate
359 Dirksen Senate Office Building
Washington, DC 20510

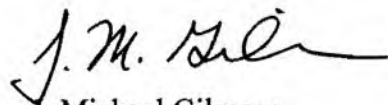
Dear Senator Brown:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate
413 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Collins:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Lamar Alexander
United States Senate
455 Dirksen Senate Office Building
Washington, DC 20510

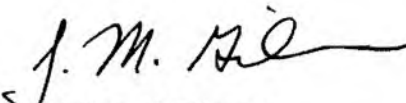
Dear Senator Alexander:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Kay R. Hagan
Chairman, Subcommittee on Emerging Threats and Capabilities
Committee on Armed Services
United States Senate
521 Dirksen Senate Office Building
Washington, DC 20510

Dear Madam Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable Roger F. Wicker
Ranking Member, Subcommittee on Seapower
Committee on Armed Services
United States Senate
555 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Wicker:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Mark Udall
United States Senate
110 Hart Senate Office Building
Washington, DC 20510

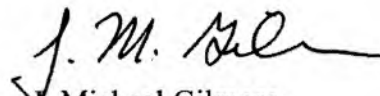
Dear Senator Udall:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable Tim Johnson
Chairman, Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Committee on Appropriations
United States Senate
136 Hart Senate Office Building
Washington, DC 20510

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Daniel K. Akaka
United States Senate
141 Hart Senate Office Building
Washington, DC 20510

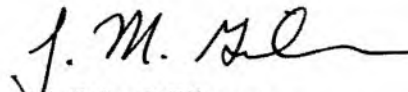
Dear Senator Akaka:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Joe Manchin III
United States Senate
303 Hart Senate Office Building
Washington, DC 20510

Dear Senator Manchin:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Richard G. Lugar
Ranking Member
Committee on Foreign Relations
United States Senate
306 Hart Senate Office Building
Washington, DC 20510

Dear Senator Lugar:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Herb Kohl
United States Senate
330 Hart Senate Office Building
Washington, DC 20510

Dear Senator Kohl:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Dianne Feinstein
Chairman
Select Committee on Intelligence
United States Senate
331 Hart Senate Office Building
Washington, DC 20510

Dear Madam Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Barbara Mikulski
United States Senate
503 Hart Senate Office Building
Washington, DC 20510

Dear Senator Mikulski:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable Claire McCaskill
United States Senate
506 Hart Senate Office Building
Washington, DC 20510

Dear Senator McCaskill:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable David Vitter
United States Senate
516 Hart Senate Office Building
Washington, DC 20510

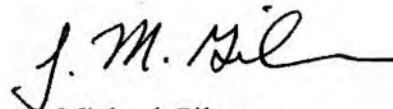
Dear Senator Vitter:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable John Cornyn
United States Senate
517 Hart Senate Office Building
Washington, DC 20510

Dear Senator Cornyn:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Jeanne Shaheen
United States Senate
520 Hart Senate Office Building
Washington, DC 20510

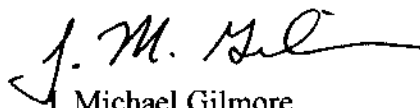
Dear Senator Shaheen:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable Harry Reid
Majority Leader
United States Senate
522 Hart Senate Office Building
Washington, DC 20510

Dear Mr. Majority Leader:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Mark Kirk
Ranking Member, Subcommittee on Military Construction, Veterans Affairs, and Related
Agencies
Committee on Appropriations
United States House of Representatives
524 Hart House Office Building
Washington, DC 20515

Dear Representative Kirk:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable Richard Blumenthal
United States Senate
702 Hart Senate Office Building
Washington, DC 20510

Dear Senator Blumenthal:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
706 Hart Senate Office Building
Washington, DC 20510

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Lisa Murkowski
United States Senate
709 Hart Senate Office Building
Washington, DC 20510

Dear Senator Murkowski:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Richard Durbin
United States Senate
711 Hart Senate Office Building
Washington, DC 20510

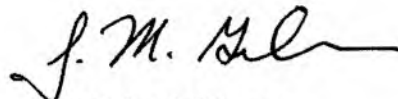
Dear Senator Durbin:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable Ben Nelson
Chairman, Subcommittee on Strategic Forces
Committee on Armed Services
United States Senate
720 Hart Senate Office Building
Washington, DC 20510

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Jack Reed
Chairman, Subcommittee on Seapower
Committee on Armed Services
United States Senate
728 Hart Senate Office Building
Washington, DC 20510

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Tom Harkin
United States Senate
731 Hart Senate Office Building
Washington, DC 20510

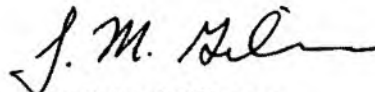
Dear Senator Harkin:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable John Boehner
Speaker of the House
United States House of Representatives
1011 Longworth House Office Building
Washington, DC 20515

Dear Mr. Speaker:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable Mark Critz
United States House of Representatives
1022 Longworth House Office Building
Washington, DC 20515

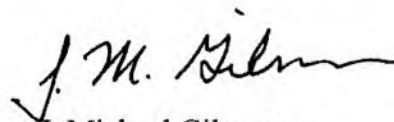
Dear Representative Critz:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable Vicky Hartzler
United States House of Representatives
1023 Longworth House Office Building
Washington, DC 20515

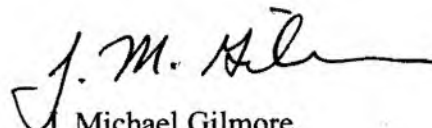
Dear Representative Hartzler:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Gabrielle Giffords
United States House of Representatives
1030 Longworth House Office Building
Washington, DC 20515

Dear Representative Giffords:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Loretta Sanchez
United States House of Representatives
1114 Longworth House Office Building
Washington, DC 20515

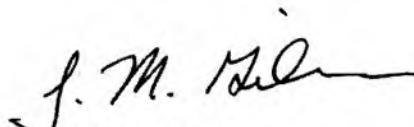
Dear Representative Sanchez:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,



J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Mike Coffman
United States House of Representatives
1222 Longworth House Office Building
Washington, DC 20515

Dear Representative Coffman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Tim Griffin
United States House of Representatives
1232 Longworth House Office Building
Washington, DC 20515

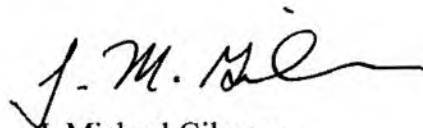
Dear Representative Griffin:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Jon Runyan
United States House of Representatives
1239 Longworth House Office Building
Washington, DC 20515

Dear Representative Runyan:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Rob Wittman
Chairman, Subcommittee on Oversight and Investigations
Committee on Armed Services
United States House of Representatives
1317 Longworth House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Chellie Pingree
United States House of Representatives
1318 Longworth House Office Building
Washington, DC 20515

Dear Representative Pingree:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Tim Ryan
United States House of Representatives
1421 Longworth House Office Building
Washington, DC 20515

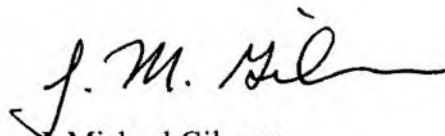
Dear Representative Ryan:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Hank Johnson
United States House of Representatives
1427 Longworth House Office Building
Washington, DC 20515

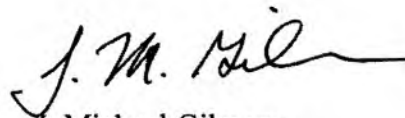
Dear Representative Johnson:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Betty Sutton
United States House of Representatives
1519 Longworth House Office Building
Washington, DC 20515

Dear Representative Sutton:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Susan A. Davis
Ranking Member, Subcommittee on Military Personnel
Committee on Armed Services
United States House of Representatives
1526 Longworth House Office Building
Washington, DC 20515

Dear Representative Davis:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable David Loebsack
United States House of Representatives
1527 Longworth House Office Building
Washington, DC 20515

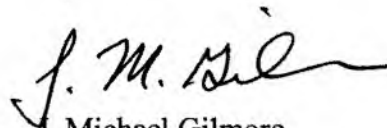
Dear Representative Loebsack:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Thomas J. Rooney
United States House of Representatives
1529 Longworth House Office Building
Washington, DC 20515

Dear Representative Rooney:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Jim Cooper
Ranking Member, Subcommittee on Oversight and Investigations
Committee on Armed Services
United States House of Representatives
1536 Longworth House Office Building
Washington, DC 20515

Dear Representative Cooper:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Niki Tsongas
United States House of Representatives
1607 Longworth House Office Building
Washington, DC 20515

Dear Representative Tsongas:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Larry Kissell
United States House of Representatives
1632 Longworth House Office Building
Washington, DC 20515

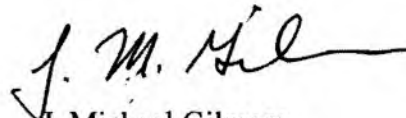
Dear Representative Kissell:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Mo Brooks
United States House of Representatives
1641 Longworth House Office Building
Washington, DC 20515

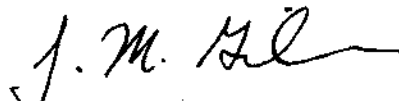
Dear Representative Brooks:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Allen West
United States House of Representatives
1708 Longworth House Office Building
Washington, DC 20515

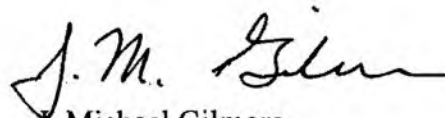
Dear Representative West:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Todd Young
United States House of Representatives
1721 Longworth House Office Building
Washington, DC 20515

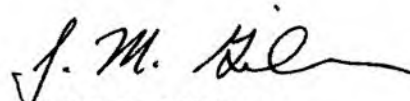
Dear Representative Young:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Jerry Lewis
United States House of Representatives
2112 Rayburn House Office Building
Washington, DC 20515

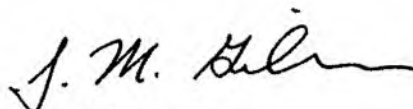
Dear Representative Lewis:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Mike McIntyre
Ranking Member, Subcommittee on Seapower and Projection Forces
Committee on Armed Services
United States House of Representatives
2133 Rayburn House Office Building
Washington, DC 20515

Dear Representative McIntyre:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Marcy Kaptur
United States House of Representatives
2186 Rayburn House Office Building
Washington, DC 20515

Dear Representative Kaptur:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Ileana Ros-Lehtinen
Chairman
Committee on Foreign Affairs
United States House of Representatives
2206 Rayburn House Office Building
Washington, DC 20515

Dear Madam Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Mac Thornberry
Chairman, Subcommittee on Emerging Threats and Capabilities
Committee on Armed Services
United States House of Representatives
2209 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Silvestre Reyes
Ranking Member, Subcommittee on Tactical Air & Land Forces
Committee on Armed Services
United States House of Representatives
2210 Rayburn House Office Building
Washington, DC 20515

Dear Representative Reyes:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Howard L. Berman
Ranking Member
Committee on Foreign Affairs
United States House of Representatives
2221 Rayburn House Office Building
Washington, DC 20515

Dear Representative Berman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Joe Wilson
Chairman, Subcommittee on Military Personnel
Committee on Armed Services
United States House of Representatives
2229 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
United States House of Representatives
2235 Rayburn House Office Building
Washington, DC 20515

Dear Representative Cummings:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Jo Bonner
United States House of Representatives
2236 Rayburn House Office Building
Washington, DC 20515

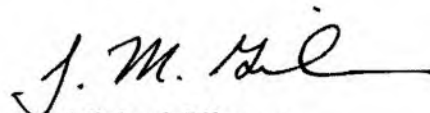
Dear Representative Bonner:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable James Moran
United States House of Representatives
2239 Rayburn House Office Building
Washington, DC 20515

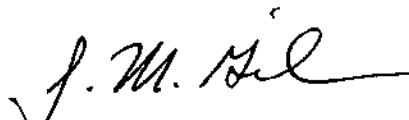
Dear Representative Moran:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Peter Visclosky
United States House of Representatives
2256 Rayburn House Office Building
Washington, DC 20515

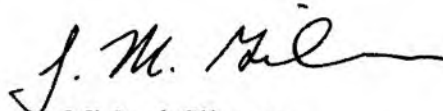
Dear Representative Visclosky:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Rob Andrews
United States House of Representatives
2265 Rayburn House Office Building
Washington, DC 20515

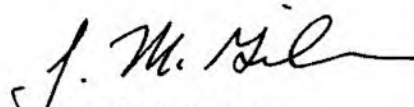
Dear Representative Andrews:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Ken Calvert
United States House of Representatives
2269 Rayburn House Office Building
Washington, DC 20515

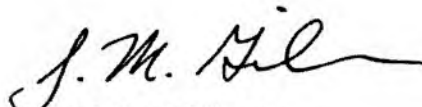
Dear Representative Calvert:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Steven Rothman
United States House of Representatives
2303 Rayburn House Office Building
Washington, DC 20515

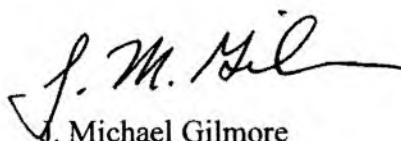
Dear Representative Rothman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Walter B. Jones
United States House of Representatives
2333 Rayburn House Office Building
Washington, DC 20515

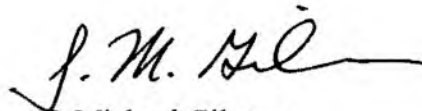
Dear Representative Jones:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Darrell E. Issa
Chairman
Committee on Oversight and Government Reform
United States House of Representatives
2347 Rayburn House Office Building
Washington, DC 20515

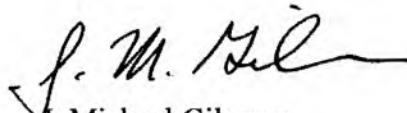
Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable John Culberson
Chairman, Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Committee on Appropriations
United States House of Representatives
2352 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Rodney Frelinghuysen
United States House of Representatives
2369 Rayburn House Office Building
Washington, DC 20515

Dear Representative Frelinghuysen:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Jack Kingston
United States House of Representatives
2372 Rayburn House Office Building
Washington, DC 20515

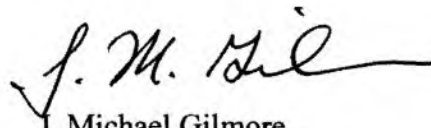
Dear Representative Kingston:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Harold Rogers
Chairman
Committee on Appropriations
United States House of Representatives
2406 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Roscoe G. Bartlett
Chairman, Subcommittee on Tactical Air & Land Forces
Committee on Armed Services
United States House of Representatives
2412 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Jeff Miller
Chairman
Committee on Veterans' Affairs
United States House of Representatives
2416 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Frank A. LoBiondo
United States House of Representatives
2427 Rayburn House Office Building
Washington, DC 20515

Dear Representative LoBiondo:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Bob Filner
Ranking Member
Committee on Veterans' Affairs
United States House of Representatives
2428 Rayburn House Office Building
Washington, DC 20515

Dear Representative Filner:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 11 2012

The Honorable Sanford Bishop
Ranking Member
Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Committee on Appropriations
United States House of Representatives
2429 Rayburn House Office Building
Washington, DC 20515

Dear Representative Bishop:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable K. Michael Conaway
United States House of Representatives
2430 Rayburn House Office Building
Washington, DC 20515

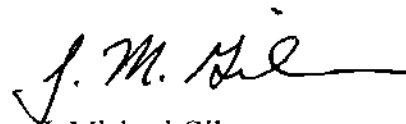
Dear Representative Conaway:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Maurice Hinchey
United States House of Representatives
2431 Rayburn House Office Building
Washington, DC 20515

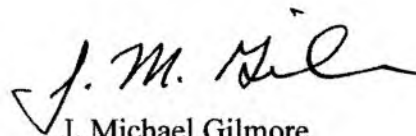
Dear Representative Hinchey:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Trent Franks
United States House of Representatives
2435 Rayburn House Office Building
Washington, DC 20515

Dear Representative Franks:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable John Kline
United States House of Representatives
2439 Rayburn House Office Building
Washington, DC 20515

Dear Representative Kline:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Madeleine Z. Bordallo
Ranking Member, Subcommittee on Readiness
Committee on Armed Services
United States House of Representatives
2441 Rayburn House Office Building
Washington, DC 20515

Dear Representative Bordallo:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable C.A. Dutch Ruppertsberger
Ranking Member
Permanent Select Committee on Intelligence
United States House of Representatives
2453 Rayburn House Office Building
Washington, DC 20515

Dear Representative Ruppertsberger:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Todd Russell Platts
United States House of Representatives
2455 Rayburn House Office Building
Washington, DC 20515

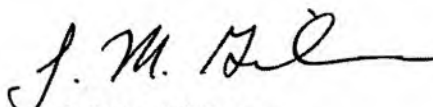
Dear Representative Platts:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable Tom Cole
United States House of Representatives
2458 Rayburn House Office Building
Washington, DC 20515

Dear Representative Cole:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
United States House of Representatives
2466 Rayburn House Office Building
Washington, DC 20515

Dear Representative Thompson:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable J. Randy Forbes
Chairman, Subcommittee on Readiness
Committee on Armed Services
United States House of Representatives
2438 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Mark Begich
United States Senate
111 Russell Senate Office Building
Washington, DC 20510

Dear Senator Begich:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Kelly Ayotte
United States Senate
144 Russell Senate Office Building
Washington, DC 20510

Dear Senator Ayotte:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable James M. Inhofe
United States Senate
205 Russell Senate Office Building
Washington, DC 20510

Dear Senator Inhofe:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Richard Burr
Ranking Member
Committee on Veterans' Affairs
United States Senate
217 Russell Senate Office Building
Washington, DC 20510

Dear Senator Burr:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable John F. Kerry
Chairman
Committee on Foreign Relations
United States Senate
218 Russell Senate Office Building
Washington, DC 20510

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Jim Webb
Chairman, Subcommittee on Personnel
Committee on Armed Services
United States Senate
248 Russell Senate Office Building
Washington, DC 20510

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Kay Bailey Hutchison
United States Senate
284 Russell Senate Office Building
Washington, DC 20510

Dear Senator Hutchison:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Lindsey Graham
Ranking Member, Subcommittee on Personnel
Committee on Armed Services
United States Senate
290 Russell Senate Office Building
Washington, DC 20510

Dear Senator Graham:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Richard Shelby
United States Senate
304 Russell Senate Office Building
Washington, DC 20510

Dear Senator Shelby:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Mitch McConnell
Minority Leader
United States Senate
317 Russell Senate Office Building
Washington, DC 20510

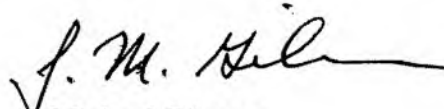
Dear Mr. Minority Leader:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Jeff Sessions
Ranking Member, Subcommittee on Strategic Forces
Committee on Armed Services
United States Senate
326 Russell Senate Office Building
Washington, DC 20510

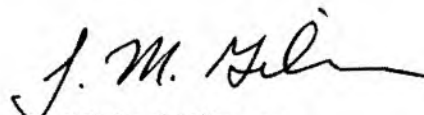
Dear Senator Sessions:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Rob Portman
United States Senate
338 Russell Senate Office Building
Washington, DC 20510

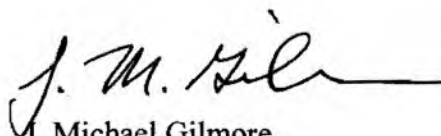
Dear Senator Portman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Michael Turner
Chairman, Subcommittee on Strategic Forces
Committee on Armed Services
United States House of Representatives
2454 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

JAN 12 2012

The Honorable Saxby Chambliss
Vice Chairman
Select Committee on Intelligence
United States Senate
416 Russell Senate Office Building
Washington, DC 20510

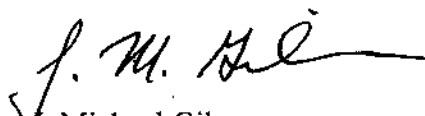
Dear Mr. Vice Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable Patrick Leahy
United States Senate
437 Russell Senate Office Building
Washington, DC 20510

Dear Senator Leahy:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OPERATIONAL TEST
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

JAN 12 2012

The Honorable Patty Murray
Chairman
Committee on Veterans' Affairs
United States Senate
448 Russell Senate Office Building
Washington, DC 20510

Dear Madam Chairman:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

The Honorable Kirsten Gillibrand
United States Senate
478 Russell Senate Office Building
Washington, DC 20510

Dear Senator Gillibrand:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,

J. Michael Gilmore
Director

Enclosure:
As stated





OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

OPERATIONAL TEST
AND EVALUATION

148 10 102

The Honorable Dan Coates
United States Senate
493 Russell Senate Office Building
Washington, DC 20510

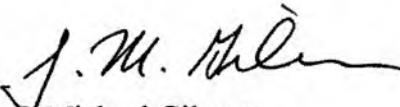
Dear Senator Coates:

I am pleased to enclose a copy of the Director, Operational Test and Evaluation (DOT&E) 2011 Annual Report for your information and use. This report provides my assessment of programs under operational and live fire testing oversight in Fiscal Year (FY) 2011 as required by section 139 of title 10, United States Code.

Of the 311 programs currently under operational and live fire testing oversight, this report contains 92 individual articles on programs that underwent testing in FY11. The remaining programs did not have significant operational test activity in FY11. The report also includes special sections that may be of interest to you or your staff.

My staff and I would be pleased to answer any specific questions you may have. I can be reached at (703) 697-3655.

Sincerely,


J. Michael Gilmore
Director

Enclosure:
As stated

