DOT&E Activity and Oversight

DOD Programs

Army Programs

Navy Programs

Air Force Programs

Ballistic Missile Defense Programs

Army Programs

Army Programs

Army Network Modernization

The FY16 National Defense Authorization Act directed the DOD to conduct a comprehensive assessment of the current and future capabilities and requirements of the Army's air-land, mobile tactical communications and data networks, including technological feasibility, suitability, and survivability. The study encompasses all Army air and land tactical communication systems; developments to date, planned enhancements (primarily programs of record), and potential future developments. Army programs of record include: Warfighter Information Network – Tactical (WIN-T); Mid-Tier Networking Vehicular Radio (MNVR); Handheld, Manpack, Small Form Fit (HMS) Rifleman Radio; HMS Manpack Radio; and Small Airborne Networking Radio (SANR). This report includes initial findings from the assessment to include:

- Capabilities of the currently fielded mobile tactical network
- Current and future operational needs that are not met by the existing capabilities
- Challenges in the Army's network modernization plans with an emphasis on the software-defined radio programs (HMS Rifleman Radio, HMS Manpack Radio, MNVR, and SANR)
- Analysis of software and hardware design concepts to understand root causes of these challenges

The final report is expected to be complete in March 2017. It will include an assessment of which challenges can improve with the current systems, which would require significant redesign of the network or individual systems, whether or not solutions, including technology alternatives, exist.

The Army's goal for its tactical network is to provide higher data rates to the individual user, to transfer voice and data simultaneously, and in the case of WIN-T Increment 1, replace multiple stove-piped systems to allow for a network with open communication within and beyond theater. Demonstrated performance to date of the mobile line-of-sight (LOS) tactical network indicates that it will not meet the Army's operational needs. The software-defined radio programs of record with their Mobile Ad hoc Network (MANET) design have struggled to meet requirements for range, power consumption, and message completion rate (MCR). The network as a whole is limited to between 30 and 40 nodes per channel and therefore requires complex planning and management and restricts unit task reorganization. The network has demonstrated poor survivability in contested electronic warfare environments, which is the primary driver for the Army's network modernization.

Performance shortfalls and the disconnect between the Army's Network Modernization plan and its operational priorities stem from multiple gaps in requirements, software (networking waveforms, network management), and the isolated hardware acquisition strategy. The bandwidth requirements, as defined in the radio requirements documents, are not driven by mission command network priorities, but rather by what the network can supply. Certain shortfalls such as the electromagnetic signature susceptibility are trade-offs in network design that are expected when the choice is the MANET. In that case, the capability to operate stealthily was not an operational priority when the Army originally conceived the network modernization plan. Other performance gaps, like high power consumption and network management complexity, are intrinsic to MANET waveforms. The expectation was that as technology evolved these gaps would narrow and the software-defined radios would ultimately outperform their legacy counterparts. In the meantime, the Army has tied requirements of future networking radios to existing waveforms, which are limited by the performance shortfalls intrinsic to those waveforms.

The hardware acquisition approach is such that the Army retains ownership and responsibility for the waveforms and the radio developers retain the rights to the hardware. Industry competitors who supply radio hardware cannot dictate the optimal implementation of the software; instead, they are expected to compete with the minimal possible technology solution that is the lowest cost and simplest to interoperate with other vendors in the multiple source non-developmental item (NDI) selection. They are continuing to build individual software-defined radios, rather than a functioning, integrated network. The effect on the Army's network is that the current path (future radio requirements, capabilities, and acquisition strategies) will not mitigate the performance shortfalls demonstrated to date. The Army should consider not specifying the waveform in requirements documents but rather allowing industry to compete with integrated end-to-end solutions consisting of the waveform and the radio hardware that are based on realistic threat and mission command data needs.

There is opportunity for the Army to recover performance trade-offs, re-align requirements with operational needs, and pursue technology solutions that could more effectively mitigate these shortfalls. Frequent program restructuring and acquisition delays over the past decade have translated into very few radios fielded to date. Three major tactical radio programs, MNVR, HMS Manpack Radio, and HMS Rifleman Radio, have re-entered source selection to allow for full and open competition. SANR is not scheduled for full-rate production until FY23. WIN-T Increment 2 began full-rate production in 2015, but heavy brigades cannot begin fielding until Armored Multi-purpose Vehicle production in 2021. The notable exception is WIN-T Increment 1, which completed fielding, but is still undergoing product improvements.

PERFORMANCE SHORTFALLS

As implemented, the Army's mobile LOS tactical network design diverges from the original MANET architecture. The original design had an ad hoc number of nodes on a single subnet. The idealized MANET architecture was self-healing and self-forming. The ad hoc features allowed a node to seamlessly self-organize into geographically advantageous partitions within the context of the larger, simpler, inclusive network. MANET waveforms include Soldier Radio Waveform (SRW), Wideband Networking Waveform (WNW), and Highband Networking Waveform (HNW). This architecture has been replaced by multiple defined subnets. The effect of breaking the network into a number of small subnets places an increased burden on network planners who must manually configure each user device to constrain communication to a specific set of nodes. Units are dependent on contractors to design and configure this complex network.

Electromagnetic Signature Vulnerability
In comparison to legacy systems, the Army's networking radios are more susceptible to electronic surveillance. Legacy push-to-talk radios limit their electromagnetic expression to those instances when user data need to be transmitted. Networking radios are constantly emitting in order to discover neighbors, maintain connectivity, and evaluate link conditions. Reducing the signal strength to mitigate this vulnerability requires reducing the transmit power of the signal, while to improve the LOS range requires increasing the power. Given that the Capabilities Production Documents (CPDs) for the software-defined radios currently require the radios to operate MANET waveforms, programs as currently defined cannot expect to produce systems with a reduction in electromagnetic signature.

Shorter Line-of-sight (LOS) Range than Legacy Radios
Range expectations for tactical networking radios are that they meet or exceed those set by their legacy counterparts. Reductions in range would require the Army to reconsider how they conduct tactical combat operations. Progress in radio frequency technology has not translated into better range performance for networking radios. This can be attributed to the constraints under which software-defined radios running SRW or WNW are operating relative to a straightforward Single Channel Ground Air Radio System (SINCGARS) implementation. SRW and WNW operate at higher frequencies than SINCGARS. The higher operating frequencies are more susceptible to range-limiting losses in even benign terrain conditions.

The exchange of information over a MANET is dependent on the health of the direct link between two nodes, the distance between them, and the complex process by which the two communicate. A node must take the time to "join" the network, be recognized by other members, and participate in extensive routing optimization and maintenance before actual data are transmitted or received. Since the nodes are mobile, network formation is an ongoing process, rather than a problem solved at the outset of a mission. As a result, the effective range of a node in a network is limited by a number of factors, (and very difficult to quantify in dynamic conditions). MCR is tied to the node's dynamic membership in the network, rather than the instantaneous condition of a link at the time a message is sent.

Network Complexity
The network is difficult to establish and maintain. Network components, including mission command systems, network manager and the radios, are challenging to use. The value added in having an integrated network to enhance mission command is diminished due to pervasive task complexity. Additionally, the Army is challenged to achieve and maintain user proficiency. Units are dependent upon contractors to plan and support the integrated network. Thus, the Army has implemented the MANET waveforms (WNW, SRW, and HNW) as pre-configured and rigid networks. This architecture has resulted in increased time and complexity required to execute task reorganization, when a unit is attached to a new headquarters. Presently, when unit task reorganization is required, a new network plan has to be created and loaded on to the radios.

High Power Consumption
The Army's software-defined radios have not benefited from technology innovations with respect to power consumption. The fields of battery technology, software-defined power management, improved circuit design, and microfabrication techniques have led to significantly less power needed to operate hardware. Soldiers are burdened with carrying and charging batteries to support dismounted radios. Mounted radios require vehicles to operate more hours per day than legacy radios, precluding the ability to perform silent watch missions and increasing the logistics support burden with increased fuel and vehicular maintenance requirements.

The root cause of the discrepancy can be traced to the design of the MANET radios themselves. Unlike legacy systems that only expend power when the warfighter is communicating, the software-defined radios are operating at near-maximum energy all the time because they must be constantly transmitting and receiving in order to maintain the network, and their presence on it, even when there is no need to transmit any voice or data messages. In the current designs, the best way to minimize the power expended during operation is to leave the network by turning off the radio. In the case of the dismounted HMS Manpack radio, soldiers observed high external temperatures during FOT&E — a common outcome of prolonged operation of high-power devices.

Low Message Completion Rate (MCR)
MCR is a measure of both the functionality of the networking software (i.e., its ability to correctly transmit, route, and parse messages), and the radio frequency connectivity of the underlying

links. The current software-defined radios have not demonstrated their requirements for MCR. The demonstrated MCR for situational awareness messages is lower than for command and control messages. Situational awareness messages consist of position location information and other messages related to battlefield entities, e.g. hazard and obstacle map icons that are automatically generated by Joint Battle Command – Platform (JBC-P). Situational awareness messages are transmitted once, and if they do not reach their destination, are dropped. Command and control messages, because of their higher priority, are programmed to keep retransmitting until the sender receives an acknowledgement of receipt.

The low MCR for situational awareness messages can be attributed to the design of the network. In moving away from the original MANET construct into multiple small subnets, the network lost its resiliency of allowing messages to make multiple hops through any node in its immediate proximity. To avoid consuming the available bandwidth, the number of nodes that a message can hop through is limited to those on its subnet even when there may be other nodes in LOS range. Not able to find a route through the network, it drops the situational awareness message causing the blue picture to be stale or inaccurate.

Absence of Anti-Jamming Capability

Two of the Army's principal LOS networking waveforms, SRW and WNW, have not demonstrated their effectiveness against a jamming threat. Anti-jamming techniques involve sophisticated algorithms that consume more bandwidth and produce reduced data rates in return. This would further reduce connectivity and MCRs for waveforms that cannot meet requirements under more benign conditions (open terrain and no jamming). The SRW and WNW standard modes of operation are not intended for a contested electronic environment. SRW's electronic warfare mode offers some jamming resistance but only at reduced data rates. The Army does not intend to use the electronic warfare mode. WNW has an anti-jam mode of operation intended to provide a more robust signal, albeit at lower data rates. Neither the SRW electronic warfare mode nor the WNW anti-jam mode has been demonstrated in an operational test environment. Given the poor performance in benign conditions, the additional constraints added by anti-jam algorithms may make an anti-jam mode not viable without re-investment in the design of the network approach as a whole.

Limited Scalability

To work effectively, the current networking waveforms limit the network to 30-40 nodes per channel. To operate the network with more than 40 nodes requires the MANET to use all the overhead bandwidth establishing and maintaining connectivity among nodes rather than sending and receiving voice or data communications. As currently configured, the radios continue to run software with ad hoc routing algorithms, but the Army has planned and configured the network to prevent ad hoc connectivity by restricting the number of nodes on a particular subnet, and in some cases, constraining exactly which nodes the data could hop through and which other nodes are retransmission vehicles.

REQUIREMENTS AND ACQUISITION APPROACH

The Army has tied the software-defined radio requirements to the existing waveforms for MNVR, HMS Manpack Radio, HMS Rifleman Radio, and SANR. Through this approach, the Army hoped to enhance competition among hardware developers and ensure waveform interoperability across different host systems. Radio capabilities will be limited by the electromagnetic signature susceptibility, high power consumption, low MCR, and network complexity, which are all performance shortfalls intrinsic to the MANET waveforms.

The network requirements are not consistent with the Army's operational needs. The bandwidth requirements, as defined in the radio CPDs, are not driven by mission command network priorities. They are based on what the network can supply rather than how much data are needed at each echelon. The data requirements drive the requirement to operate in higher operating frequencies and are a trade-off with LOS range performance.

The Army's requirements for its tactical networks do not take into account the evolving threat capable of advanced electronic warfare. While the requirements remain rooted in MANET waveforms as currently implemented, the networking solutions will continue to lack sufficient anti-jamming features to mitigate against the effects of electronic attack and remain effective. Direction-finding systems will threaten the survivability of soldiers and host platforms.

The current acquisition approach for HMS Rifleman, HMS Manpack, MNVR, and SANR is a modified NDI in which the Army is retaining ownership and responsibility for the waveform and network manager, and the radio developer is retaining rights to the hardware. Hardware and software developers lack the design control necessary to implement new technology solutions. Hardware contractors have no financial incentive to integrate new technology if the Army's requirements force them to run waveforms that cannot take advantage of those capabilities. In some cases, the contractor may already have its own commercial off-the-shelf waveform optimized for its advanced hardware platform, but may instead opt to deliver a less capable hardware system that better suffices the Army's waveform requirement

Though the government-run reference integration labs continue to make incremental improvements to the Army's networking waveforms, the fundamental design of these waveforms remains rooted in the MANET protocols and hardware functionality of the early 2000s. Since the waveforms were originally developed,

research has produced routing protocols that are inherently more scalable and power efficient. Hardware capabilities have similarly advanced, enabling improved signal processing and greater spectrum efficiency. While the commercial sector has widely adopted many of these capabilities, the Army's waveform development and hardware acquisition strategies lack the agility to do so in a timely and efficient manner.

Given these barriers to technology integration, the current acquisition strategy is detrimental to delivering an effective, suitable, or survivable piece of operational equipment to the warfighter. The Army cannot hold the most critical technological element of the radio — the waveform — constant, and at the same time, expect hardware partners to demonstrate sweeping advancements in capabilities. The Army should consider not specifying the waveform in requirements documents but rather allowing industry to compete integrated solutions of the waveform and the radio hardware based on realistic threat and mission command data needs.

PATH FORWARD

Frequent program restructuring and acquisition delays have translated to very few radios fielded to date. To date, the Army has procured less than 10 percent of its full procurement goal. HMS Rifleman Radio has fielded 7 percent of its procurement goal and has re-entered source selection to allow for full and open competition. The remaining tactical radio programs (MNVR and HMS Manpack) are in the early stages of source selection for full and open competition. WIN-T Increment 2 went into full-rate production in 2015, but heavy brigades cannot begin fielding until Armored Multi-purpose Vehicle production in 2021. The notable exception is WIN-T Increment 1, which completed fielding, but is still undergoing product improvements so there is still opportunity for technology injection.

In addition to limited fielding, several aspects of network design are still being deliberated. The Army will conduct an Analysis of Alternatives to the current mid-tier networking solution, MNVR operating WNW. A departure from WNW would represent a major shift in the Army's network plan, affecting not only MNVR, but also SANR, the Army's future aerial networking radio. With network design still being conceptualized and SANR NDI activities yet to start, a clear opportunity exists to influence the direction of the aerial tier.

There is opportunity for the Army to recover performance trade-offs, re-align requirements with operational needs, and pursue technology solutions that could more effectively mitigate these shortfalls. Regardless of the extent to which the Army's networking radios have been fielded or procured, to adapt to the changing threat landscape, a re-direction from the current path is necessary. In order to adapt to these threats the Army will need to adopt new technology (hardware and waveforms) and confront trade-offs in performance.

Network Integration Evaluation (NIE)

The Army conducted one NIE during FY16. NIE 16.2 was conducted in April and May 2016 at Fort Bliss, Texas. In a change from previous years, instead of conducting two NIEs a year to support test and evaluation, the Army conducted a single NIE. Beginning in FY16, the Army is devoting one NIE a year to operational testing and using another annual event, the Army Warfighting Assessment, for experimentation and force development. The first Army Warfighting Assessment was conducted at Fort Bliss in October 2015.

The purpose of the NIEs is to provide a venue for operational testing of Army acquisition programs, with a particular focus on the integrated testing of tactical mission command networks. The Army also intends the NIEs to serve as a venue for evaluating emerging capabilities. These systems, termed by the Army as "systems under evaluation," are not acquisition programs of record, but rather systems that may offer value for future development.

The Army's intended objective of the NIE – to test and evaluate network components in a combined event – is sound. The NIE events allow for a more comprehensive evaluation of an integrated mission command network than is possible through piecemeal evaluations of individual network components.

NIE 16.2

During NIE 16.2, the Army conducted a Limited User Test (LUT) for Warfighter Information Network – Tactical (WIN-T) Increment 3 Network Operations/Net Centric Waveform and an LUT for Spider Increment 1A. In addition, the Brigade Modernization Command conducted an operational assessment of the Mid-Tier Networking Vehicular Radio (MNVR). Individual articles providing assessments of WIN-T, Spider, and MNVR can be found separately in this annual report.

NIE ASSESSMENT

NIE 16.2 was the tenth such event conducted to date. NIEs have been an excellent venue for conducting operational tests of network acquisition programs.

Dedicated Test Unit. Since the first NIE in July 2011, the 2nd Brigade Combat Team, 1st Armored Division has served as the dedicated NIE test unit. Having a dedicated test unit stationed at Fort Bliss, Texas, has been a critical element in successful operational testing conducted during NIEs. It has made the planning and execution of complex brigade-sized operational tests of Army networks much more effective than would be the case if new test units were selected for each event. Past experience demonstrates that having a dedicated test unit enables good operational testing. Due to its experience and the organizational learning that has occurred over time, the dedicated NIE test brigade has shown that it is more attuned to incorporating new systems into its formation for testing than has been the case with one-off test units. As a result, the system under test receives a robust evaluation.

A dedicated test unit is desirable in that it relieves the stress on the Army to designate a test unit of appropriate size each time an operational test is on the schedule for a given program. Some tests require large-scale units up to brigade in size and, when testing command and control systems, sometimes even require a division headquarters element. It is not uncommon to require a brigade combat team-sized or battalion-sized unit. Having a dedicated test unit of a mixed composition enables all of those requirements to be met at one place.

Another aspect of good operational testing is a capable opposing force (OPFOR). The dedicated test brigade has been very proficient in creating this OPFOR. Good operational testing requires an aggressive, adaptive threat unit intent on winning the battle in order to adequately stress the system under test and to fully understand its capabilities. A realistic demanding OPFOR requires capabilities which are not easily assembled and integrated. These capabilities include electronic warfare and cybersecurity threats as well as a mix of heavy and light forces. In particular, the integration of electronic warfare and cyber capabilities into an OPFOR requires practice and is not easily replicated by new units tasked to conduct an OPFOR operational testing mission. The units permanently assigned to conduct the NIEs have, over time, demonstrated the ability to employ an effective OPFOR with a variety of combat multipliers to include

electronic warfare and cyber-attack. This OPFOR capability has grown increasingly sophisticated and can be readily adapted to reflect new real-world threat capabilities. This capability may not easily be replicated by a rotational brigade.

For operational reasons unrelated to test and evaluation, the Army has removed 2nd Brigade Combat Team, 1st Armored Division from its mission as the dedicated NIE test unit and has decided to no longer provide a dedicated test unit. This is unfortunate from an operational test and evaluation perspective and, for reasons noted above, the quality of future NIE execution may suffer.

Threat Operations. One of the most significant benefits of NIEs has been the extensive incorporation of threat information operations, such as electronic warfare and computer network operations. Nowhere else has the Army routinely integrated this level of threat capability in either a testing or a training venue. As a result, NIEs have provided numerous insights with respect to operations in this type of threat environment. This capability should be retained and upgraded, as necessary, in future NIEs.

One challenge associated with providing these threat capabilities is cost. They are expensive to provide. The programs of record – or "systems under test" – have borne the cost despite not being funded for these capabilities in their test and evaluation budgets. This has created a funding mismatch before every NIE. The Army should consider centrally funding NIE threat operations to relieve the cost burden on the programs undergoing formal operational testing. This makes particular sense given that the benefits accrue to many of the other systems undergoing some sort of assessment during NIEs, such as "systems under evaluation" and risk reduction events.

Instrumentation and Data Collection. The Army should continue to improve its instrumentation and data collection procedures to support operational testing. For example, the Army Test and Evaluation Command (ATEC) should devote increased effort towards developing instrumentation to collect network data to support WIN-T operational test and evaluation. WIN-T instrumentation has not been adequate to support a thorough evaluation. Improvements are needed with respect to Simple Network Management Protocol polling and Internet Protocol-packet capture and matching. ATEC should also devote effort towards developing instrumentation to collect network data for dismounted radios, such as the Manpack radio. Additionally, the Army needs to place greater emphasis on the use of Real-Time Casualty Assessment instrumentation – an essential component of good force-on-force operational testing – such as that conducted at NIEs. A Real-Time Casualty Assessment is intended to accurately simulate direct and indirect fire effects for both friendly and threat forces. Finally, the Army should continue to refine its methodology for the conduct of interviews, focus groups, and surveys with the units employing the systems under test.

NETWORK PERFORMANCE OBSERVATIONS

The following are observations of tactical network performance during NIEs. These observations focus on network performance deficiencies that the Army should consider as it moves forward with integrated network development.

Network Implementation Challenges. Significant questions remain as to how the network will be implemented in each of the three types of maneuver brigade combat teams (Armored, Infantry, and Stryker). For example:

- Armored Brigade Combat Team Integration. It is not clear how the desired tactical network will be incorporated into heavy brigades, as the challenge of integrating network components into tracked combat vehicles remains unresolved. Due to vehicle space and power constraints, the Army has yet to integrate desired network capabilities into Abrams tanks and Bradley infantry fighting vehicles. For example, at the company level it will be some years before the Manpack network radio will be installed on Abrams tanks and Bradley infantry fighting vehicles. Additionally, it is not clear how the mid-tier tactical network will be established at company level, given that the MNVR radio will not be integrated on either of these vehicles. Implementation of the WIN-T network into the Armored Brigade Combat Team is also some years away, as it is dependent upon successful development and fielding of the Armored Multipurpose Vehicle Mission Command variant.
- Infantry Brigade Combat Team Integration. Integration of the tactical network into an Infantry Brigade Combat Team has not been adequately evaluated in a light infantry unit assigned to the NIE test unit. Integration of the network into the light forces will be challenging given the limited number of vehicles in the Infantry Brigade Combat Team. Most of the key network components, such as Joint Battle Command – Platform, are hosted on vehicles. The challenge of linking into the tactical network is particularly acute at company level and below, where light infantry units operate dismounted. Without a vehicular network node, dismounted units cannot connect to the network above company level.

Networking Waveforms. The Army is committed to using networking waveforms – such as the Soldier Radio Waveform and Wideband Networking Waveform – to implement a networked tactical communications network. While networked communications at lower tactical levels may create enhanced operational capability, the use of networking waveforms brings negative attributes which need to be fully evaluated and understood. For example, networking waveforms, due to their higher frequencies, have shorter ranges and are more affected

by terrain obstructions compared to the legacy Single Channel Ground and Airborne Radio System waveform. Networking waveforms and the corresponding software-defined radios were conceived to support data intensive capabilities such as real time video. Such capabilities require high bandwidth, and hence high frequencies, at the cost of shorter ranges. The Army should re-examine whether the current radio and waveform programs best meet the operational needs of maneuver commanders. One clear lesson from previous NIEs is that the two most critical network needs for maneuver commanders at battalion and below are reliable voice communications and GPS-supplied position location information. These needs may be met by a network with much lower bandwidth but increased operating ranges.

Complexity of Use. Network components, including mission command systems and elements of the transport layer, remain very complex to use. The current capability of an integrated network to enhance mission command is diminished due to pervasive task complexity. It is challenging to achieve and maintain user proficiency. Units remain dependent upon civilian field service representatives to establish and maintain the integrated network. This dependency corresponds directly to network complexity of use.

Survivability. An integrated tactical network introduces new vulnerabilities to threat countermeasures – such as threat computer network attacks – and the ability of a threat to covertly track friendly operations. Since networked communications are constantly emitting, they are much more vulnerable to threat electronic direction finding.

The Army should continue to improve its capability to secure and defend its tactical network. The Army should ensure that division and brigade-level cybersecurity teams are appropriately manned and trained.

Air-Ground Communications. The Army has yet to equip its rotary-winged aircraft with radios capable of operating in the same network as ground forces at the company level and below. This remains an important operational gap.

Abrams M1A2 System Enhancement Program (SEP) Main Battle Tank (MBT)

Executive Summary

- In December 2015, the Army conducted a live fire user test event with the Common Remotely Operated Weapon System – Low Profile (CROWS-LP). CROWS-LP demonstrated no degradation to performance over the CROWS II in powered mode. Crews were also able to engage targets effectively in manual mode, an improvement to CROWS II where the height of the weapon hindered accuracy.
- In June 2016, the Army conducted a User Beta Test for Version 4.6 of the Abrams software. There were unexplained accuracy problems with the M829A4 service rounds during the test. The Program Office initiated the investigation of vehicle software, ammunition type, and gun tube wear as potential causes.
- DOT&E approved the Operational Test Agency test plan for the LFT&E of the M1A2 System Enhancement Program Version 3 (SEPv3) Engineering Change Proposal (ECP) la Turret Half-Bustle Ammunition Vulnerability Test Phase I in June 2016. The test is scheduled to start January 2017.
- The Army continued developmental and verification testing to characterize the performance of the M1A2 SEPv3 Next Evolutionary Armor (NEA) against multiple, operationally realistic threats. DOT&E is working with the Army to utilize data from ongoing test phases to support its final assessment of M1A2 SEPv3 survivability against existing and emerging threats in FY20.

System

- The M1A2 SEP Version 2 (v2) and M1A2 SEP Version 3 (v3) are tracked, land combat, assault weapon systems designed to possess significant survivability, shoot-on-the-move firepower, joint interoperability (for the exchange of tactical and support information), and a high degree of maneuverability and tactical agility. The Army intends the M1A2 SEPv2 and M1A2 SEPv3 to enable the crew to engage the full spectrum of enemy ground targets with a variety of point- and area-fire weapons in urban and open terrain.
- The M1A2 SEPv2 is currently fielded. It upgrades the M1A2 SEP by providing increased memory and processor speeds, full color tactical display, digital map capability, compatibility with the Army Technical Architecture, improved target detection, recognition, and identification through incorporation of second generation Forward Looking Infrared technology and electronics and crew compartment cooling through the addition of a thermal management system.
- The Abrams M1A2 SEPv3 fielding is planned for FY20. The M1A2 SEPv3 is an upgrade to the M1A2 SEPv2. The upgrades include the following:

Common Remotely Operated Weapon Station-Low Profile (CROWS-LP)

M1A2 SEP

  - Power generation and distribution to support power demands of future technologies.
  - Network compatibility.
  - Survivability against multiple threats by incorporating NEA, a new underbody IED kit, and other vulnerability reduction measures to reduce the tank's vulnerability to IEDs. These measures include redesigned crew seating, additional floor stiffeners, hardware to provide lower limb protection, and changes in the material and dimensions of internal structural supports.
  - Lethality by providing the ability for the fire control system to digitally communicate with the new large caliber ammunition through use of an Ammo Data Link.
  - Energy efficiency (sustainment) due to the incorporation of an auxiliary power unit.
- The M153A1E1 CROWS-LP is an ECP integration onto the M1A2 SEPv2. The system addresses visibility concerns associated with the existing M153 CROWS II by relocating the sights and laser range finder to the side of the weapon and ammunition box rather than under the weapon, reducing the system height by 10 inches. The ECP includes upgraded software.
- The M1A2 SEP MBT utilizes 120 mm main gun rounds to defeat enemy targets.
  - The XM1147 Advanced Multipurpose (AMP) Round, which is currently in development, is a 120 mm

munition fired utilizing an ammunition datalink-equipped Abrams MBT. The round is optimized for use in urban environments in direct support of assaulting infantry. The Army intends the round to have three defeat modes including Point Detonate (PD), Point Detonate Delay (PDD), and airburst. It will be used to defeat a combination of targets including anti-tank guided missile teams, dismounted infantry, double reinforced concrete wall, light armor, bunkers, obstacles, and armor.
- The M829A4, which was fielded in 2014, is an Armor-Piercing, Fin-Stabilized, Discarding Sabot, 120 mm line-of-sight kinetic energy cartridge. It is the materiel solution for the Abrams' lethality capability gap against threat vehicles equipped with third-generation explosive reactive armor.

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

Major Contractor
General Dynamics Land Systems – Sterling Heights, Michigan

Activity
- All testing was conducted in accordance with a DOT&E-approved test plan.
- In December 2015, the Army conducted a live fire user test event with the CROWS-LP. Four tank commanders fired 80 different scenarios and approximately 18,000 rounds during the event at Aberdeen Proving Ground, Maryland.
- In June 2016, the Army conducted a User Beta Test for Version 4.6 of the Abrams software. This software version provides full functionality for the CROWS-LP, the Ammunition Data Link required to support the M829A4 kinetic energy round, and integration for the Joint Chemical Agent Detector.
- In June 2016, DOT&E approved the Operational Test Agency test plan for the LFT&E of the M1A2 SEPv3 ECP la Turret Half-Bustle Ammunition Vulnerability Test Phase I.
- In FY16, the Army continued testing to characterize M1A2 SEPv3 armor performance against multiple threat types under the auspices of NEA, a separate materiel development verification and production effort. DOT&E is following the NEA development and verification program to leverage all relevant data to support the M1A2 SEPv3 survivability assessment. The Army plans to continue testing to characterize NEA and explosive reactive armor performance, vulnerabilities associated with stowed ammunition, and underbody IED protection in FY17.

Assessment
- During the live fire test event, CROWS-LP demonstrated no degradation to performance over the CROWS II in powered mode. Crews were also able to engage targets effectively in manual mode, an improvement to CROWS II where the height of the weapon hindered accuracy.
- There were unexplained accuracy problems with the M829A4 service rounds during the User Beta Test for Version 4.6 of the Abrams software. Crews reported an increase in firing system faults compared to home station vehicles operating on the current software version. The Army is currently conducting a test-based, root cause analysis of the accuracy issue. DOT&E is overseeing these diagnostic tests and analyses and will amend the DOT&E M829A4 report if the test series reveals deviations in originally reported ammunition effectiveness/lethality.
- DOT&E continues to assess data resulting from the Army's ongoing efforts to characterize the protection provided by NEA against expected, operationally-realistic threats. DOT&E will leverage all relevant vulnerability test data from the armor characterization and underbody IED test phases and evaluate all modeling and simulation tools available to support an FY20 final assessment of the tank's survivability to current and expected threats.

Recommendations
- Status of Previous Recommendations. There are no previous recommendations.
- FY16 Recommendations. None.

AH-64E Apache

Executive Summary
- The Army submitted an AH-64E Version 6 Test and Evaluation Master Plan (TEMP) dated October 19, 2016, for OSD approval. The purpose of the TEMP is to support the FOT&E II of the Version 6 AH-64E and a subsequent Post-Full-Rate Production Cut-in Review. The TEMP adequately addresses the operational, cybersecurity, and live fire portions.
- The Director approved the TEMP on November 9, 2016.

System
- The AH-64E is a modernized version of the AH-64D Attack Helicopter. The Army intends to sustain the Apache fleet through the year 2040. The AH-64E is organized in Attack/Reconnaissance Battalions assigned to the Combat Aviation Brigades. Each Battalion has 24 aircraft.
- The Army redesignated the AH-64D Apache Block III as the AH-64E in September 2012.
- The AH-64E's advanced sensors, improved flight performance, and ability to integrate off-board sensor information provide increased standoff and situational awareness in support of the joint force.
- The AH-64E is fielded in two Versions (1 and 4) with a future Version 6 planned in 2017.
- The major Version 1 AH-64E capability improvements included:
  - The ability of the aircrew to control the flight path and the payload of an Unmanned Aircraft System
  - Improved aircraft performance with 701D engines, composite main rotor blades, and an improved rotor drive system
  - Enhanced communication capability, which includes satellite communication and an integrated communication suite to meet global air traffic management requirements
- Version 4 AH-64E retained Version 1 capabilities and added hardware and software for Link 16 network participation.
- The future Version 6 will add multiple enhancements to include:
  - Radar Frequency Interferometer (RFI) passive ranging
  - Fire Control Radar range extension

  - Cognitive Decision Aiding System
  - Maritime Targeting mode
  - Modernized Day Sensor Assembly with color and high definition displays
- The Army acquisition objective is to procure 690 AH 64E aircraft: 634 remanufactured and 56 new build aircraft.

Mission

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

Major Contractors
- Aircraft: The Boeing Company Integrated Defense Systems – Mesa, Arizona
- Sensors and Unmanned Aircraft System datalink: Longbow Limited – Orlando, Florida, and Baltimore, Maryland

Activity
- The Army submitted an AH-64E Version 6 TEMP dated July 29, 2016, for OSD approval in September 2016. The purpose of the TEMP is to support the FOT&E II of the Version 6 AH-64E and a subsequent Post-Full-Rate Production Cut-in Review. The Army submitted this particular TEMP as a draft for ongoing developmental testing.
- The Army resubmitted an updated version of the TEMP, dated October 19, 2016. The TEMP adequately addresses previous shortcomings from the July version of the TEMP to include operational, cyber, and live fire portions.
- The Director approved the TEMP on November 9, 2016. The Apache Program Management Office (PMO) established

a contract with Boeing that began in April 2015 to address cybersecurity deficiencies from FOT&E I. The Cooperative Vulnerability and Penetration Assessment (CVPA) and Adversarial Assessment (AA) are planned for FOT&E II.

Assessment

- Version 4 AH-64E and its interfacing systems have potentially significant cybersecurity deficiencies. Further testing of the AH-64E embedded systems is necessary to determine the significance of the deficiencies.
- Version 4 AH-64E embedded systems are vulnerable to cyber penetration attacks. The AH-64E has been selected by Headquarters, Department of the Army G3/5/7 as one of the five systems to complete an evaluation of cyber vulnerabilities to comply with the National Defense Authorization Act Section 1647 directive. Additionally, the PMO has scheduled a CVPA conducted by the Army Research Laboratory/Survivability Lethality Analysis Directorate for January 2017 and an AA planned for October 2017 as part of FOT&E II.

Recommendations

- Status of Previous Recommendations. The Army has addressed some recommendations from the FY14 annual report. The following recommendations have not been fully implemented:
  1. Improve infrared countermeasures performance, upgrade radar- and laser-warning systems, and improve integration of aircraft survivability equipment on the Version 4 AH-64E.
  2. Address demonstrated cybersecurity vulnerabilities. Plan and conduct unconstrained exploitation of vulnerabilities during adversarial cybersecurity testing.
- FY16 Recommendations. None.

Army Integrated Air & Missile Defense (IAMD)

Executive Summary

- Army Integrated Air and Missile Defense (AIAMD) is a command and control system that will enable an integrated air and missile defense (AMD) system of systems.
- In January 2016, the Army conducted developmental testing of AIAMD that included a Cooperative Vulnerability and Penetration Assessment and missile flight tests. Also, the Army conducted an AIAMD Limited User Test (LUT) in March through May 2016, which included sustained operations to assess system reliability, two missile flight tests, and hardware-in-the-loop (HWIL) events to assess effectiveness and suitability.
- During the HWIL events, operators' assessment was limited to basic air defense missions because of software immaturity and instability, as well as a lack of training for operators on new equipment and new capability operations.
- The IAMD Battle Command System (IBCS) software is neither mature nor stable, as evidenced in numerous software problem reports. This precludes a full assessment of capabilities. Also, software immaturity contributed to the AIAMD Engagement Operations Center's (EOC) reduced reliability; operator workstations often became sluggish or ceased to operate
- AIAMD was unable to effectively operate on the Link 16 network.
- AIAMD system setup, operations, and maintenance technical manuals were incomplete or inadequate.

System

- AIAMD is a command and control system that integrates sensors, weapons, and a common mission command capability across an integrated fire control network (IFCN) to provide a single air picture.
- The IBCS provides the capabilities to control and manage AIAMD-enabled sensors and weapons.
- AIAMD's IBCS will replace and enhance Patriot Data Information Link communication structure, integrate with the currently fielded Sentinel air surveillance sensors, and improve command and control of missile employment.
- The IBCS includes the EOC, hardware interface kits, and IFCN Relays.
  - EOCs provide the operating environment for all levels (battalion and battery) of employment. They will be equipped with IBCS software that enables operators to monitor, interface with, and direct sensor employment and engagement of air threats.
  - Hardware interface kits connect IBCS with the current Patriot and Sentinel missiles, and will incorporate future AMD capabilities to support engagement of air threats. The IFCN is the primary organic communications infrastructure for AIAMD system of systems and provides the capability for fire control connectivity and distributed operations.
  - The IFCN Relay provides a mobile IFCN communications node with an interface kit which extends connectivity to remote launcher and sensor platforms.

Mission

- Army commanders will use AIAMD to provide timely detection, identification, monitoring, and (if required) engagement of air threats (e.g. aircraft, cruise missiles, ballistic missiles, rockets, artillery, and mortars) in an assigned area of responsibility.
- AMD forces deploy to provide active protection for the following:
  - Air defense of the homeland
  - Air defense of priority critical assets and locations
  - Air defense of forces

Major Contractors

- Northrop Grumman – Huntsville, Alabama
- Raytheon – Huntsville, Alabama, and Andover, Massachusetts
- Lockheed Martin – Dallas, Texas

Activity

- In May 2015 (Missile Flight Test 2) and November 2015 (Missile Flight Test 1), the Army conducted two live fire developmental tests in accordance with the DOT&E-approved Test and Evaluation Master Plan (TEMP) during which Northrup Grumman contractors used AIAMD to defeat missile threats. Both tests were conducted at White Sands Missile Range, New Mexico.

- In January 2016, the Army conducted a Cooperative Vulnerability and Penetration Assessment as part of a developmental test effort. The test was not conducted in accordance with a DOT&E-approved test plan. Results from this test will be incorporated in future software builds.
- From March through May 2016, the Army completed a LUT on AIAMD at White Sands Missile Range, New Mexico, and Fort Bliss, Texas. The LUT was conducted in accordance with a DOT&E-approved test plan. The LUT consisted of three phases:
  - Sustained operations phase (three 72-hour mission pulses)
  - Missile Flight Test 3-1 and 3-2
  - HWIL phase
- In July 2016, the Army conducted a developmental test of new IBCS software, version 3.2.1. Numerous system performance deficiencies were identified during Government Software Integration Laboratory assessments and soldier check-out events.

Assessment

- During the LUT, the operators' assessment was limited to basic air defense missions because of software immaturity and instability, as well as a lack of training for operators on new equipment and new capability operations. Due to AIAMD software immaturity and limited capability to effectively operate at a multi-echelon level, soldiers were unable to effectively coordinate with engagement and identification authorities, a key function in air defense.
- As of February 3, 2016, AIAMD's IBCS software had 32 Severity 1 and 2 software problem reports. Also, AIAMD demonstrated poor system reliability, with 6 to 8 hours of Mean Time Between System Abort (MTBSA) compared to the LUT entrance criteria of 31 hours MTBSA.
  - Despite DOT&E's concerns that AIAMD is an immature system and not ready for a Milestone C decision, the Army elected to proceed with the LUT as an operational test.
- During the LUT, AIAMD demonstrated a 6 percent likelihood that it could operate for 72 hours without experiencing a failure that would result in system abort.
  - The warfighter requirement is a 90 percent likelihood that the system will operate for 72 hours without experiencing a failure that results in system abort.
- The EOC, a critical subsystem of AIAMD, demonstrated an average operating time of up to 16 hours without a failure that results in ineffective operations; this is significant when compared to the minimum requirement to operate for up to 446 hours.
- The computer workstations in the EOC were not reliable and a constant source of frustration for operators.
  - Due to IBCS software immaturity, workstations lagged and froze during mission operations, significantly affecting crew operations and mission execution.
  - The median time to repair a workstation was approximately 13 minutes. During air defense operations against aircraft and missile threats, this could result in multiple failed engagements and loss of critical defended assets.
- During the majority of the sustained operations phase, the workstations showed multiple false tracks when only one test target aircraft was flying. The operators often struggled to identify targets of interest in the cluttered air picture.
- AIAMD was unable to effectively operate on the Link 16 network and had significant problems with dual tracks and reporting responsibility with the IBCS network. The LUT was the first time AIAMD attempted interoperability with the Marine Tactical Air Operations Center.
- The IFCN relays were not reliable. Additionally, on multiple occasions the IFCN relay was inoperable thus disconnecting the associated radar or shooter from the AIAMD system. Once the IFCN is disconnected, the operators are unable to employ that associated radar or shooter.
- The AIAMD system setup, operations, and maintenance technical manuals were incomplete or inadequate.
- In surveys, 40 percent of operators identified poor training (includes training time, documentation, and lesson plans) on system employment.
- In August 2016, Milestone C (planned for November 2016), was placed on hold until IBCS software deficiencies are resolved in accordance with contracted requirements. The Program Management Office is working with Northrop Grumman Corporation to resolve IBCS software deficiencies.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The Army should:
  1. Fix all Severity 1 and 2 software problem reports and conduct another operational assessment of AIAMD performance to inform a Milestone C decision.
  2. Develop and publish an AIAMD operational mode summary/mission profile for planned AIAMD employment.
  3. Update the program TEMP in accordance with updated program acquisition way forward.
  4. Determine the required IBCS reliability for initial fielding and outline a reliability growth plan in an updated program TEMP.
  5. Correct and formalize all AIAMD system documentation and training deficiencies.

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

Executive Summary
- Army testing of demilitarization systems in the Chemical Demilitarization Program has been adequate to ensure the safe and secure disposal of chemical warfare material.
- The Army conducted operational testing in accordance with DOT&E-approved test plans.
- The Army began operational testing at the Pueblo Chemical Agent-Destruction Pilot Plant (PCAPP) located in Colorado in FY16.
- Disposal operations of the U.S. chemical stockpile did not meet the original Chemical Weapons Treaty deadline of April 2007. Congress, through Public Law 114-38, has established a new stockpile elimination deadline of December 31, 2023.

System
- The Chemical Demilitarization Program involves the destruction of lethal chemical agents, chemical munitions, and non-stockpile chemical warfare material.
- The PCAPP stockpile disposal facility in Pueblo, Colorado, has started operations while the Blue Grass Chemical Agent-Destruction Pilot Plant (BGCAPP) facility in Richmond, Kentucky, is preparing for operations. These facilities employ chemical neutralization of agents followed by post-treatment of the neutralized products.
  - The PCAPP is a first-of-a-kind facility designed to destroy the chemical blister agent mustard (HD and HT) stored in 155 mm projectiles, 105 mm projectiles, and 4.2-inch mortar rounds through the use of a low-temperature, low-pressure neutralization process. PCAPP will process the neutralized agent (hydrolysate) using biotreatment.
  - The BGCAPP is a first-of-a-kind facility designed to destroy chemical nerve agents Sarin (GB) and VX stored in 155 mm projectiles, 8-inch projectiles, M55 rockets, and M56 rocket warheads through the use of a chemical (caustic) neutralization process. BGCAPP will process hydrolysate using supercritical water oxidation (SCWO) technology.
- Explosive destruction technology is used in the Assembled Chemical Weapons Alternatives (ACWA) program:
  - PCAPP uses the Explosive Destruction System (EDS) for destruction of problematic munitions not easily processed in the main plant. The EDS uses shaped explosive charges to access chemical munitions and destroy the munitions' explosive components. After detonation, EDS chemically treats the munitions' contents within the containment vessel and collects vapor and liquid samples as required. The products of this neutralization process (neutralents) are transferred to drums and will be packaged for shipment to an approved treatment, storage, and disposal facility (TSDF).
  - BGCAPP will use the Static Detonation Chamber (SDC) to destroy mustard munitions. The SDC uses explosive destruction technology designed to destroy conventional munitions, munition components, and chemical-filled munitions by indirect heating in a detonation chamber. The heat produced in the chamber allows for detonation and/or deflagration of the agent-filled munition and its energetic components, and subsequently treats the chemical fill. The air pollution abatement system captures and treats any resulting harmful vapor products.

Mission
The United States is using the Chemical Demilitarization Program to comply with the Chemical Weapons Convention. This is an arms control and nonproliferation treaty that requires the destruction of the U.S. stockpile of lethal chemical agents, chemical munitions, and chemical warfare material.

Major Contractors
- Chemical Materials Activity – Aberdeen, Maryland
- Assembled Chemical Weapons Alternatives (ACWA) sites:
  - Bechtel National, Inc. – San Francisco, California
  - Parsons Infrastructure and Technology Group, Inc. – Pasadena, California

Activity
- The Chemical Demilitarization Program is not a traditional acquisition program. DOT&E oversight began in 1999 when Congress directed that the DOD oversee this program as a major defense acquisition program due to cost and schedule overruns.

- The test and evaluation program for chemical demilitarization consists of two phases:
  - The developmental testing phase consists of system and subsystem component testing without an agent culminating in end-to-end operations of the facility.
  - The operational testing phase consists of pilot testing and campaign changeover testing involving operations with an agent. Operational testing supports a decision to proceed to full operational status for a specific agent/munitions campaign. For example, one campaign would destroy 155 mm projectiles containing mustard blister agent, another would destroy 8-inch projectiles equipped with Sarin nerve agent, and the third would destroy M55 rockets equipped with Sarin. After the completion of each campaign, the facility reverts to operational test status for changeover to the next planned campaign. This process is repeated until the destruction of all agent/munitions configurations in the site's stockpile is complete. DOT&E monitors the test activity and independently analyzes test data at PCAPP and BGCAPP.
- As of August 2016, the Chemical Demilitarization Program has destroyed over 90 percent of the total U.S. chemical weapons stockpile (originally 31,498 agent tons).
- On February 11, 2016, the PCAPP EDS completed the destruction of 560 overpacked munitions and agent containers that could not be processed by the main plant. The PCAPP EDS campaign began in March 2015 after successfully completing multiple pre-operational reviews.
- The systems contractor led by Bechtel successfully conducted an Integrated Operations Demonstration (IOD) in August 2016, demonstrating main plant facility readiness for operations.
- The Army conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) and an Adversarial Assessment (AA) on the industrial control system (ICS) and laboratory information system (LIS) at PCAPP. DOT&E observed all cybersecurity assessment activities. The Program Executive Office and the systems contractor committed to correcting defects prior to the start of operations, and the Army conducted two follow-on events to verify the correction of noted vulnerabilities.

Assessment

- Army testing of demilitarization systems in the Chemical Demilitarization Program has been adequate to ensure the safe and secure disposal of chemical warfare material. The U.S. Army Material Systems Analysis Activity (AMSAA) is providing effective independent oversight of the testing of both stockpile and non-stockpile programs. Fully integrated operational demonstrations that confirm all phases of operations (including preparation, destruction/neutralization, and disposal) remain critical prerequisites for transitioning to operations with live agents.
- Disposal operations of the U.S. chemical stockpile did not meet the original Chemical Weapons Treaty deadline of April 2007. Congress, through Public Law 114-38, has established a new stockpile elimination deadline of December 31, 2023.
- Cybersecurity testing at PCAPP identified technical and physical security vulnerabilities, which were corrected by the systems contractor and verified by both AMSAA and DOT&E.
  - Cybersecurity testing of the PCAPP LIS showed that the risk was low and acceptable based upon the assessment of the protect, detect, respond, and restore capabilities.
  - Cybersecurity testing of the PCAPP ICS resulted in a number of system improvements, including enhanced policies and procedures, installation of a Security Information and Event Management (SIEM) system for threat monitoring, and configuration of the SIEM to alert operators to suspicious activities. DOT&E and AMSAA have verified these improvements. The system contractor also made improvements to physical security following the AA.
  - The PCAPP IOD identified areas for procedural improvement, which were corrected and verified by the test community. The IOD demonstrated that the plant was ready to begin processing agent rounds as part of a controlled ramp-up (pilot testing). Following the correction of deficiencies noted during cybersecurity assessments and the IOD, PCAPP's main plant began processing chemical munitions as part of pilot (operational) testing on September 7, 2016. DOT&E is monitoring the pilot testing and operations.
- The BGCAPP test program started planning for FY17 activities by:
  - Developing IOD and pilot test plans for the SDC, to include a cybersecurity CVPA and AA. The SDC, based on current credible estimates, could begin processing mustard rounds in 4QFY17.
  - Planning cybersecurity test activities for the LIS, BGCAPP Main Plant, and SDC systems.
- AMSAA is monitoring BGCAPP systemization activities to support the readiness assessment to proceed into IOD.

Recommendations

- Status of Previous Recommendations. There are no outstanding previous recommendations.
- FY16 Recommendation.
  1. The Program Executive Officer ACWA should incorporate lessons learned from PCAPP test planning and cybersecurity testing at BGCAPP.

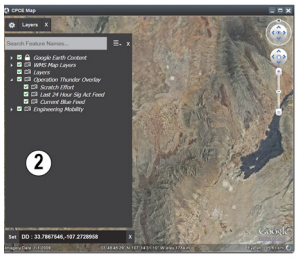
Command Web

Executive Summary

- Command Web is the Army's lead program to field a web-based set of tools designed in accordance with Common Operating Environment (COE) architectures and standards.
- During 2016, the Army conducted a two-phase Command Web Limited User Test (LUT) at Grafenwoehr, Germany, and Fort Bliss, Texas. The test was conducted in accordance with a DOT&E-approved test plan.
- The Army intends to use the results of the Command Web LUT to support a 3QFY17 material release decision.
- DOT&E's preliminary results for the Command Web LUT indicate:
  - Soldiers found Command Web tools easy to use and were successful at creating and posting engineer tasks on the Common Operational Picture (COP).
  - Since Command Web is a client-based application, the unit could install the tools on any computer within the command post. This allowed staff sections (beyond the intended engineer cell) to access the COP without the need of a legacy mission command hardware/software suite.
  - Lack of trained system administrators to manage tactical operations center (TOC) servers hinders Command Web's ability to support soldiers in the accomplishment of their mission. Training afforded soldiers did not allow them to troubleshoot server problems and share the COP between unit echelons and mission command applications.
  - Command Web demonstrated its reliability requirement.
- Command Web experienced cybersecurity vulnerabilities that could affect its ability to support the unit's mission.

System

- Command Web is a collection of web-based applications or "widgets" designed to provide combat engineer staffs and leaders with tools that enhance tactical mission command at brigade and battalion command posts, and support their functional responsibility for the planning and execution of combat engineer tasks.
- The Army designed Command Web to fill an engineer capabilities gap created with the termination of the Maneuver Control System (MCS). Command Web provides web-based engineer tools to enhance the operations of Command Post of the Future (CPOF), which replaced MCS.
- Command Web includes the Obstacles and Hazards Services and Engineering Mobility Services widgets. These tools provide soldiers the ability to create, receive, and analyze obstacle and hazard information; road, route, and bridge information; and engineering project information.
- The Maneuver widget allows soldiers to view relevant COP information (e.g., maneuver graphics, friendly position location information, enemy situation) to provide context for executing combat engineer functions. The Maneuver widget supports collaboration with other engineer staff cells and with the integrated battle staff through the use of mission command applications during planning and execution phases of mission operations. Data and products from Command Web widgets are displayed on the Common Map widget.
- Command Web is the Army's lead program to field a web-based set of tools designed in accordance with COE architectures and standards. The Army intends for the Command Post Computing Environment V3.0 to provide these capabilities as part of a larger set of mission command tools and replace Command Web when fielded in FY19.



1 - Soldier operating Command Web
2 - Command Post Computing Environment Map Widget
3 - Maneuver Widget

Mission

- Army combat engineer leaders and soldiers use Command Web tools to perform technical and operational tasks for mobility, counter-mobility, survivability, and construction to support the synchronization of engineer activities and their integration into maneuver operations.
- Engineer staff use Command Web widgets to synchronize engineer products via the COP, create and disseminate graphics, and publish/subscribe to data feeds from other Warfighter Functional Area mission command applications. Engineer soldiers and other Command Web users within the TOCs share and collaborate using a variety of data sources visualized on a common map. The Army intends Command Web products to inform commanders during the military decision-making process.

Major Contractor

- U.S. Army Communications – Electronics Command, Software Engineering Center, Aberdeen Proving Ground, Maryland

Activity

- During 2016, the Army conducted a two-phase Command Web LUT at Grafenwoehr, Germany, and Fort Bliss, Texas. The test was conducted in accordance with a DOT&E-approved test plan. The purpose of the Command Web LUT was to:
  - Assess Command Web effectiveness, suitability, and survivability, and provide an evaluation in support of the Army's planned 3QFY17 material release decision.
  - Assess Command Web's ability to fill the engineer capability gap created with the termination of MCS, and enhance the mission support provided by CPOF.
  - Assess Command Web's ability to support combat engineer functions at battalion and brigade, and update relevant engineer information to the unit's COP to share information across brigade mission command applications.
  - Provide performance insights and lessons learned for future testing and development of the Army's Command Post Computing Environment.
- The Army conducted the first phase of the Command Web LUT at Grafenwoehr, Germany, as part of a U.S. European Command joint coalition exercise during February 2016. The Germany test consisted of two assessment activities:
  - Soldiers and leaders from the 15th Engineer Battalion manned TOCs representing three battalions, a brigade, a division, and corps. The soldiers responded to operations orders and fragmentary orders to create combat engineer tasks in support of larger mission requirements using Command Web and mission command applications associated with their TOCs. The resulting products were posted to the COP and reviewed by subject matter experts for completeness and accuracy.
  - Soldiers and leaders from the 173rd Airborne Brigade Combat Team employed Command Web within the brigade's TOC in support of the unit's real-time training mission within the U.S. European Command joint coalition exercise. The unit integrated Command Web into their existing TOC servers, and distributed Command Web widgets to the brigade's combat engineer cell and other staff within the TOC. The brigade conducted noncombatant evacuation operations and used Command Web to produce engineer staff products in support of the unit's mission.
- The Army conducted the second phase of the Command Web LUT during the April through May 2016 Network Integration Evaluation (NIE) 16.2. The operational test employed the 2nd Brigade, 1st Armored Division conducting operationally realistic missions at Fort Bliss, Texas, and White Sands Missile Range, New Mexico. This phase of the test focused on unit's use of Command Web at brigade and battalion TOCs while performing operationally realistic missions supported by tactical communications.
- DOT&E approved a Command Web Test and Evaluation Master Plan update on July 21, 2016.

Assessment

- DOT&E and the Army are assessing Command Web LUT data to produce evaluations in support of the Army's 3QFY17 material release decision.
- DOT&E's preliminary results for the Command Web LUT indicate:
  - Soldiers found Command Web tools easy to use and were successful at creating and posting engineer tasks on the COP.
  - The airborne brigade commander was innovative in using Command Web by installing the tools in several staff sections within his TOC. Although Command Web was intended for the combat engineer cell, the unit could install the tools on any TOC computer since Command Web is a client-based application. This allowed staff sections to access the COP without the need of a legacy mission command hardware/software suite (e.g. CPOF).
  - Lack of trained system administrators to manage TOC servers hinders Command Web's ability to support soldiers in the accomplishment of their mission. During the Germany phase, system administrators were not able to troubleshoot server problems that slowed Command Web operations, and had to reboot the servers. During NIE16.2, system administrators were not able to configure TOC servers to share the COP with Command Web products between brigade and battalion, but could share the COP between Command Web and other mission command applications within their TOC.
  - Command Web demonstrated its reliability requirement during the Germany phase of test.
  - During NIE 16.2, Command Web experienced cybersecurity vulnerabilities that could affect its ability to support the unit's mission.

Recommendations

- Status of Previous Recommendations. This is the first annual report for Command Web.
- FY16 Recommendations. The Army should:
  1. Improve Command Web training to include system administrator training to install, operate, and maintain it, and integrate the unit's COP across mission command applications.
  2. Correct cybersecurity vulnerabilities and validate corrections during operational test.

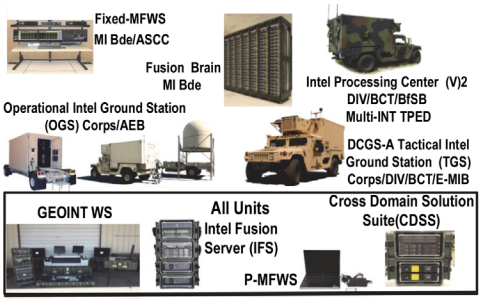
Distributed Common Ground System – Army (DCGS-A)

Executive Summary

- DOT&E reported on January 29, 2016, that the Distributed Common Ground System – Army (DCGS-A) Increment 1, Release 2 is operationally effective and suitable, but not survivable against cyber threats due to the vulnerability of the Army network.
- The Defense Acquisition Executive approved the DCGS-A Increment 2 Material Development Decision on October 9, 2015.
- DCGS-A Increment 2 includes two releases. The Army Test and Evaluation Command (ATEC) will conduct the IOT&E with Release 1 in FY19 to inform the Full Deployment Decision in early FY20. The Army will continue Increment 2 development and testing with Release 2. The increment 2, Release 2 fielding decision is planned for FY22.

System

- DCGS-A is the Army Service component of the DOD DCGS family of systems, providing multi-Service integration of intelligence, surveillance, reconnaissance (ISR), and targeting capabilities. DCGS-A connects with the DCGS family of systems via the DCGS Integration Backbone (DIB). The DIB is a cohesive set of modular, standards-based data services focused on enterprise information sharing. The DCGS Multi-Service Execution Team manages the DIB.
- DCGS-A Increment 1, Release 2 is a command and control system that tasks, processes, exploits, and disseminates ISR information from battalion to Echelons Above Corps (EAC) by combining 16 independent legacy systems of record into one comprehensive network, including the capability to process Top Secret/Sensitive Compartmented Information.
- DCGS-A Increment 1 has a planned modernization strategy until Increment 2 fielding. The modernization efforts focus on end-of-life obsolescence and cyber updates. The system picture above shows the Increment 1, Release 2 configuration.
- DCGS-A Increment 2 will consist of a collection of software packages selected to provide each Army echelon from battalion to EAC the capability to synthesize and exploit intelligence data.
  - The software packages will be commercial off-the-shelf and government off-the-shelf hardware components, configured to meet the Army unit's intelligence mission and mobility requirements.
  - The program intends to deliver these Increment 2 capabilities in two releases. The Army will develop the Increment 2 configuration after the Milestone B decision in FY17.



AEB – Area Exploitation Battalion
ASCC – Army Service Component Command
BCT – Brigade Combat Team
Bde – Brigade
BfSB – Battlefield Surveillance Brigade
DIV – Division
E-MIB – Military Intelligence Battalion, Expeditionary
GEOINT – Geospatial Intelligence
MFWS – Multi-Function Work Station
MI – Military Intelligence
P-MFWS – Portable Multi-Function Work Station
TPED – Task, Process, Exploit and Disseminate
WS – Work Station

Mission

- Army intelligence units use DCGS-A to fuse intelligence information and produce enemy situational awareness products.
- Army intelligence analysts use DCGS-A to perform receipt and processing of select ISR sensor data, intelligence synchronization, ISR planning, reconnaissance and surveillance integration, fusion of sensor information, and direction and distribution of relevant threat, non-aligned, friendly, and environmental (weather and geospatial) information.

Major Contractors

- General Dynamics – Taunton, Massachusetts
- ManTech – Fort Hood, Texas
- Booz Allen Hamilton – Aberdeen Proving Ground, Maryland
- Exelis Incorporation – Mclean, Virginia

Activity

- ATEC conducted the DCGS-A Increment 1, Release 2 FOT&E in May 2015 during the Army's Network Integration Evaluation (NIE) 15.2 at Fort Bliss, Texas, and in a database synchronization test at the Ground Station Integration Facility (GSIF) at Aberdeen Proving Ground, Maryland, in September 2015. Cybersecurity tests were conducted during NIE 15.2 and at the GSIF before and after the NIE 15.2. ATEC conducted the tests in accordance with the DOT&E-approved test plan, but did not conduct the data collection, reduction, and analysis as described in the test plan.

- DOT&E provided a report to Congress on January 29, 2016, evaluating DCGS-A based on data obtained from the test events.
- The Defense Acquisition Executive approved the DCGS-A Increment 2 Material Development Decision on October 9, 2015.
- DCGS-A Increment 2 includes two releases. ATEC will conduct the IOT&E with Release 1 in FY19 to inform the Full Deployment Decision in early FY20. The Army will continue Increment 2 development and testing with Release 2. The Increment 2, Release 2 fielding decision is planned for FY22.

Assessment

- DOT&E evaluated the Increment 1, Release 2 to be operationally effective and suitable, but not survivable against cyber threats due to the vulnerability of the Army network.
- DCGS-A Increment 1 is operationally effective. DCGS-A allows Army intelligence units to rapidly receive and organize intelligence from more than 700 sources, search relevant information, perform analysis, and share the results with the Army command and control network as well as the intelligence community through the DCGS Integration Backbone.
- DCGS-A Increment 1 is operationally suitable, provided the Army intensively trains DCGS-A users and provides continued refresher training to units in garrison. DCGS-A is a complex system, and the skills required to use it are perishable. The operational availability of DCGS-A satisfied the requirements at all echelons, and reliability improved from the IOT&E in 2012. There were no hardware failures during the FOT&E. Software failures were still a challenge for users; the system required reboots about every 20 hours for users who had heavy workloads such as the fire support analysts and data managers in Brigade Combat Team Tactical Operations Centers.
- The survivability results are classified but can be found in classified annex B of the January 2016 DOT&E report on DCGS-A Increment 1, Release 2 FOT&E.

Recommendations

- Status of Previous Recommendations. The Army is implementing the previously recommended actions.
- FY16 Recommendations.
  1. ATEC should continue to develop the Test and Evaluation Strategy for Increment 2.
  2. The Army should continue to provide intensive training to DCGS-A users, including refresher training to units in garrison.

HELLFIRE Romeo and Longbow

Executive Summary
- The HELLFIRE missile (AGM-114) is a family of air-to-surface, guided munitions consisting of a missile body with different warhead types. The Air Force authorized fielding of the latest HELLFIRE Romeo missile variant (with R warhead) in December 2014. Other Services have since pursued different variations of the HELLFIRE missile.
- The Army successfully completed testing of the Romeo missile in 2016 against a new, more representative masonry target at high temperature. The Army plans to implement the R warhead on the Joint Air-to-Ground Missile System, which begins developmental and live fire tests in FY17.
- The Navy plans to employ the HELLFIRE Longbow L8A variant, which utilizes the K2A warhead, on the Littoral Combat Ship (LCS) against threat boat swarms as part of the Surface-to-Surface Mission Module (SSMM). The Navy is in the process of crafting a developmental test program; the operational and live fire test programs were codified in change pages to the LCS Test and Evaluation Master Plan, which DOT&E approved in March 2016.
- The Navy began developmental HELLFIRE Longbow testing in FY15 with the Guided Test Vehicle – 1 (GTV-1) test. In December 2015 and August 2016, the Navy carried out GTV-2 developmental tests from a barge against small boat representative high-speed maneuvering surface targets. These tests could have been leveraged to support the DOT&E effectiveness/lethality evaluation but the Navy has planned and executed all GTV tests to date without DOT&E oversight.

System
- The AGM-114 HELLFIRE is a family of guided missiles for use against fixed and moving targets by both rotary- and fixed-wing aircraft, including unmanned aerial vehicles (UAVs).
- The HELLFIRE Romeo laser-guided missile variant:
  - Is an air-to-surface missile intended to be launched from Army and Air Force UAV platforms, Air Force Special Operations and Marine Corps fixed-wing aircraft (e.g., MC-130 and KC-130 variants), and Army rotary-wing aircraft. It uses a new warhead and a semi-active laser seeker to home in on its target.

  - Has a multi-function warhead that includes variable time delay fuzing options, in order to provide improved lethality against combatants within building structures while maintaining lethality against non-armored targets.
  - Is compatible with other HELLFIRE missiles fired from other Air Force UAVs.
- The HELLFIRE Longbow radar-guided missile variant:
  - Is being redesigned from its prior air-to-surface role as employed on Army Longbow Apache helicopters to a new role as a Navy surface-to-surface missile intended to be launched from LCS against threat boats in swarm attacks
  - Has a single-function K2A warhead with a fragmentation wrap designed to provide lethality against small boat targets

Mission
- Army, Air Force, and Marine Corps commanders will employ HELLFIRE Romeo from a range of UAV, fixed wing, and rotary wing platforms to engage enemy combatants located within complex building and bunker structures, in non-armored vehicles, in small boats, and in the open.
- Navy LCS commanders will employ HELLFIRE Longbow missiles as part of its SSMM against small threat boats involved in swarming attacks against the LCS.

Major Contractor
Lockheed Martin Corporation, Missiles and Fire Control Division – Grand Prairie, Texas
(The missiles are manufactured in Ocala, Florida, and Troy, Alabama.)

Activity
- In FY15, lot acceptance testing of HELLFIRE Romeo R warheads against non-operationally representative (harder than the requirement) masonry targets at elevated temperatures failed in two of the four tests. Subsequently, the Army tested the Romeo missile with the R warhead in June and August 2016 against the operationally representative target at high temperature. The warhead operated successfully in eight of eight tests.
- The Navy carried out GTV-2 HELLFIRE Longbow developmental tests against small boat representative high

speed maneuvering surface targets in December 2015 and August 2016 without DOT&E oversight. The Navy has not yet delivered an LFT&E Lethality Test Plan for the SSMM utilizing the HELLFIRE Longbow missile, which could have leveraged these developmental tests.

Assessment

- As reported in DOT&E reports to Congress in FY14, the HELLFIRE Romeo missile demonstrated adequate lethality across a spectrum of expected targets, including small boats, light armor, technical vehicles (trucks), and personnel both in the open and behind/under a variety of masonry structures.
- Army tests of the HELLFIRE Romeo R warhead, completed to support the testing and procurement of the Joint Air-to-Ground Missile program, verified the assessment of adequate lethality against the operationally representative masonry target but have not addressed the underlying cause of the observed failures against harder targets.
- The Navy conducted the early developmental tests of the HELLFIRE Longbow without DOT&E involvement or oversight, missing an opportunity to leverage these data in operational effectiveness and lethality assessments.

Recommendations

- Status of Previous Recommendations. The Army has begun to address the recommendations in the 2015 DOT&E classified report to further quantify lethality estimates against specific targets in specific conditions and engagement circumstances. However, several target types require additional characterization. The Air Force provided the classified test results to the Joint Technical Coordinating Committee for Munitions Effectiveness (JTCG/ME) for incorporation into JTCG/ME products as indicated in the final classified DOT&E report.
- FY16 Recommendations.
  1. The Army HELLFIRE program should characterize the spectrum of masonry target conditions (hardness, density, etc.) where the Romeo warhead fails to detonate when operating at high temperature.
  2. The Navy should develop a Lethality Test Plan for the SSMM utilizing the HELLFIRE Longbow missile, which must be approved by DOT&E.
  3. The Navy should fully fund and fully execute the operational and live fire test plans articulated in the 2016 update to the LCS Test and Evaluation Master Plan.

Javelin Close Combat Missile System – Medium

Executive Summary

- In FY16, the Army tested the Spiral 2 missile improvements and continued development of Spiral 3 missile improvements and a new Light Weight Command Launch Unit (CLU). The Army intends these efforts to improve lethality against non-armored targets and to reduce unit cost and weight.
- Early arena testing and lethality modeling of the Spiral 2 missile, which includes a new Multi-Purpose Warhead (MPWH), has demonstrated improved warhead fragmentation and similar armor penetration compared to the legacy warhead. This indicates the potential for improved lethality against non-armored targets and personnel in the open while maintaining performance against armored threats.
- The precursor warhead (PCWH) has failed to detonate in two of two flight tests and two of nine static warhead tests, and the MPWH failed to detonate in one of nine static warhead tests. The Army stopped the testing of the Spiral 2 missile and convened a failure review board to investigate the cause of the failures. Testing of the Spiral 2 missile will continue into FY17 following resolution of the warhead detonation problems.
- The Program Office has chosen to delay production of the FGM-148F or Spiral 2 missile until the successful resolution of the warhead failures and completion of the missile test program in FY17.
- DOT&E and the Army are planning testing required for the Spiral 3 missile and Light Weight CLU developments.

System

- The Javelin Close Combat Missile System – Medium is a man-portable, fire-and-forget, anti-tank guided missile employed by dismounted troops to defeat threat armored combat vehicles out to 2,500 meters.
- The Javelin system consists of a missile in a disposable launch tube assembly and a re-usable CLU. The CLU mechanically engages the launch tube assembly for shoulder firing, has day and night sights for surveillance and target acquisition, and electronically interfaces with the missile for target lock-on and missile launch. An operationally-ready Javelin system weighs 49.5 pounds.
- The Javelin missile employs a tandem shaped charged warhead to defeat vehicle armor and can be fired in direct-fire or lofted trajectory top-attack modes.
- The Army has planned four Javelin system improvements to reduce unit cost and weight and improve lethality against non-armored targets. These improvements are referred to as missile Spiral 1, 2, 3, and Light Weight CLU.
  - The Spiral 1 effort will replace electronic components in the control actuator section of the missile for cost and weight savings. Production missiles will be designated FGM-148E.
  - The Spiral 2 effort will develop an MPWH, which uses enhanced fragmentation to improve lethality against non-armored targets and personnel in the open while maintaining lethality against armored threats. Production missiles will be designated FGM-148F.
  - The Spiral 3 effort will develop a new launch tube assembly and battery unit, and will replace the current gas-cooled seeker with an uncooled seeker in the guidance section of the missile. Production missiles will be designated FGM-148G.
  - The Light Weight CLU effort will develop a new CLU that is smaller and lighter while maintaining or improving system performance.

Mission

- Infantry, Engineer, Reconnaissance, and Special Operations Forces within Army and Marine Corps ground maneuver units employ the Javelin to destroy, capture, or repel enemy assault through maneuver and firepower.
- Service members use the Javelin to destroy threat armor targets and light-skinned vehicles, and to incapacitate or kill threat personnel within fortified positions. In recent conflicts, Javelin was used primarily against enemy bunkers, caves, urban structures, mortar positions, snipers, and personnel emplacing IEDs.

Major Contractors

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

Activity

- In 2016, the Army Aviation and Missile Research, Development, and Engineering Center continued testing of the Spiral 2 missile improvements in accordance with the DOT&E-approved live fire strategy. A total of 7 of 21 planned missile flight tests and 9 of 16 planned static warhead tests have been conducted at the Redstone Test Center, Alabama.
  - Of the seven flight test missiles, one was a tactical round including both a PCWH and MPWH, one contained a PCWH and telemetry payload, and five contained a telemetry payload only
  - The nine static tandem warhead tests included both the PCWH and MPWH
- DOT&E and the Army are planning testing required for the Spiral 3 missile and Light Weight CLU.
- The Javelin Program Office completed testing of the Spiral 1 missile improvements and approved the FGM 148E for the FY17 production lot.

Assessment

- Missile Warhead Performance:
  - Preliminary results of static warhead testing of the MPWH indicate improved fragmentation versus the legacy warhead while maintaining effectiveness against armor. The Army intends the improved fragmentation to enhance lethality of the weapon against non-armored targets and personnel in the open.
  - The PCWH failed to detonate in two of nine static tests and in two of two flight tests. The MPWH failed to detonate in one of nine static tests. Prior Government qualification testing at a contractor facility demonstrated no PCWH or MPWH failures in 62 static tandem warhead tests.
  - The Army conducted investigations after the first two PCWH and the one MPWH failures. Potential problems with the static test setup at Redstone Test Center were corrected and testing resumed. The Army stopped testing and initiated a failure review board after two more PCWH failures occurred. Testing of the Spiral 2 missile will continue following identification and resolution of the failures.
- Missile Flight and Tracking Performance:
  - In seven of seven flight tests conducted to date, the Spiral 2 missiles have demonstrated proper target lock on and missile launch resulting in six successful hits and one miss. The six successful hits were against five tank targets and one pickup truck target; the miss was against a three-man IED team in the open. The miss is attributed to a combination of test range conditions that pulled the tracker off of the target during the flight. Personnel in the open are a secondary target for the Javelin.
- The Program Office has chosen to delay production of the FGM-148F, Spiral 2 missile, until the successful resolution of the warhead failures and completion of the missile test program in FY17.

Recommendations

- Status of Previous Recommendations. The Army and DOT&E are planning testing required for the Spiral 3 and Light Weight CLU. The Army agrees that an operational test should be conducted prior to fielding to confirm that effectiveness/lethality and suitability have not been compromised, and to ensure compatibility with applicable fielded variants of the missile.
- FY16 Recommendation.
  1. The Javelin Program Office should update the Javelin Test and Evaluation Master Plan in preparation for Spiral 3 and Light Weight CLU testing.

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

Executive Summary

- The industry protest after the Army awarded the Joint Light Tactical Vehicle (JLTV) initial production contract delayed the program schedule by 6 months. The Multi-Service Operational Test and Evaluation (MOT&E) is planned for February 2018. The Army and Marine Corps Initial Operational Capability dates are scheduled for 1QFY20.
- In May 2016, the Defense Acquisition Executive delegated the Milestone Decision Authority for JLTV to the Army, designating the program Acquisition Category 1C.
- In July 2016, DOT&E approved the JLTV Milestone C Test and Evaluation Master Plan (TEMP). The TEMP approval was delayed by 10 months based on the Army decision to submit the TEMP after the JLTV low-rate initial production contract award and review of the test program budget. The Army's intent was to reduce test costs based on assessing the extent of JLTV production design changes relative to the JLTV prototype vehicles performance during Engineering Manufacture Development (EMD) testing.
- Based on the JLTV Allocation Baseline Review, the program plans to implement several design changes intended to improve JLTV performance:
  - A new piston pump that reduces suspension transition times and increases reliability
  - Larger ammunition storage racks
  - Smaller engine air filter mount to improve driver visibility
  - Replacing several aluminum parts with steel to improve reliability
  - Replacing composite armors with all-metal to eliminate the multi-hit problem with ceramic armors
  - Modified gunner restraint system to improve gunner protection during underbody blast events
- The program plans to replace:
  - The engine used in the prototype JLTVs during EMD, with a newer model. The new engine will require several design modifications to fit in the engine compartment.
  - The roof hatch on the General Purpose and Utility variants with a bolt-on cover plate that eliminates a crew egress point.

System

- The JLTV Family of Vehicles (FoV) is the Marine Corps and Army partial replacement for the High Mobility Multi-purpose Wheeled Vehicle (HMMWV) fleet. The Services intend JLTV to provide increased crew protection against IEDs and underbody attacks, improved mobility, and higher reliability than the HMMWV.

General Purpose

Heavy Guns Carrier

Utility/Shelter Carrier

Close Combat Weapons Carrier

- The JLTV FoV consists of two vehicle categories: the JLTV Combat Tactical Vehicle, designed to seat four passengers, and the JLTV Combat Support Vehicle, designed to seat two passengers.
- The JLTV Combat Tactical Vehicle has a 3,500-pound payload and three mission package configurations:
  - Close Combat Weapons Carrier Vehicle
  - General Purpose Vehicle
  - Heavy Guns Carrier Vehicle
- The JLTV Combat Support Vehicle has a 5,100-pound payload and one mission package configuration:
  - Utility Prime Mover that can accept a shelter
- JLTVs are equipped with two separate armor levels: the A-kit, or base vehicle, which is intended for use in low-threat environments, and the B-kit, an add-on armor kit, for additional force protection to include enhanced small arms, fragmentation, and underbody protection in the intended deployment configuration.

Mission

- Commanders employ military units equipped with JLTV as a light, tactical-wheeled vehicle to support all types of military operations. JLTVs are used by airborne, air assault, amphibious, light, Stryker, and heavy forces as reconnaissance, maneuver, and maneuver sustainment platforms.
- Small ground combat units will employ JLTV in combat patrols, raids, long-range reconnaissance, and convoy escort.

Major Contractor

Oshkosh Corporation – Oshkosh, Wisconsin

Activity

- The industry protest after the Army awarded the contract delayed the program schedule by 6 months. The MOT&E is planned for February 2018. The Army and Marine Corps Initial Operational Capability dates are scheduled for 1QFY20.
- The program conducted a JLTV Allocation Baseline Review in February 2016. The meeting covered details of the JLTV design changes, vendor's organization, and manufacturing processes to improve vehicle performance, simplify production, and reduce cost.
- In May 2016, the Defense Acquisition Executive delegated the Milestone Decision Authority for JLTV to the Army, designating the program Acquisition Category 1C.
- In July 2016, DOT&E approved the JLTV Milestone C TEMP. The Army/Marine Corps TEMP submission to OSD was delayed by 10 months based on the Army/Marine Corps decision to submit the TEMP after the JLTV low-rate initial production contract award. The goal was to reduce the test budget based on assessing the extent of JLTV production design changes relative to JLTV prototype vehicles performance during EMD.
- The program began armor coupon live fire testing in July 2016 and ballistic cab testing in August 2016.
- The Army received the first delivery of production JLTVs in October 2016. The initial order included 657 JLTVs and 25 trailers.
- The Army Test and Evaluation Command (ATEC) began Reliability Qualification Testing (RQT) in January 2017 at Aberdeen Test Center, Maryland, and Yuma Proving Ground, Arizona. The objective of the RQT is to assess whether the JLTV can meet the Mean Miles Between Operational Mission Failure requirement prior to MOT&E. This testing is planned to consist of 96,000 miles on JLTVs.
- Full-Up System-Level live fire testing, intended to evaluate crew survivability and vehicle performance against mine and IED threats, overhead artillery, rocket-propelled grenades, homemade explosives, and the performance of the Automatic Fire Extinguishing System, is scheduled to begin in January 2017 at Aberdeen Test Center.
- The ATEC plans to conduct extreme cold weather testing beginning in February 2017 at Cold Regions Test Center in Fort Greeley, Alaska. The testing will provide information to assess the JLTV performance and reliability in extreme cold weather environments.

Assessment

- In August 2015, DOT&E's JLTV Milestone C Operational Assessment and classified Live Fire Report recommended the program develop a plan to improve the performance of the JLTV:
  - Increase the speed of suspension and tire pressure adjustments to improve vehicle responsiveness and maneuver
  - Strengthen the vehicle hood and add steps and hand-holds on the side of the vehicle to support rigging/de-rigging, ingress/egress, weapon mounting, and loading task
  - Redesign the JLTV to allow access to the cargo compartment from within the cab
  - Relocate mission equipment to improve storage of additional ammunition in the cab, and redesign ammunition platforms and storage straps in the cab to better accommodate ammunition cans
  - Reduce the Essential Function Failure rate, focusing on the sub-systems with high-failure rate
  - Fix command and control failures
  - Mitigate effect of placing items under energy absorbing seats to improve occupant protection
  - Improve gunner protection during underbody blast events
  - Modify frame clip systems to improve recoverability
  - Modify cooling lines to prevent coolant intrusion into crew cab
- Based on the JLTV Allocation Baseline Review, the program intends to implement several design changes to improve JLTV performance:
  - A new piston pump that reduces suspension transition times and increases reliability
  - Larger ammunition storage racks
  - Smaller engine air filter mount that improves driver visibility
  - Replacing several aluminum parts with steel to improve reliability
  - Replacing composite armors with all-metal to eliminate multi-hit problem with ceramic armors
  - Modified gunner restraint system to improve gunner protection during underbody events
- The program is developing and prioritizing the following Engineering Change Proposals:
  - Integration of a weight-bearing hood
  - Investigate modifying the Utility variant to support carrying troops in the rear cargo bed
  - Redesign the JLTV to fit a litter in the JLTVs
- Replacing aluminum parts with cast iron parts and ceramic armor with metal is intended to improve the multi-hit protection capability but will increase the JLTV weight by approximately 250 pounds.
- The engine used in the prototype JLTVs during EMD is being replaced by a newer model. The new engine will require several design modifications to fit within the JLTV engine compartment.

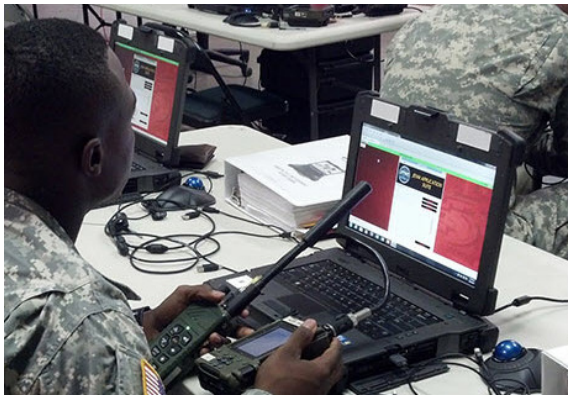
Recommendations

- Status of Previous Recommendations. The Army has made progress addressing the previous FY15 recommendations.
- FY16 Recommendations. None.

Joint Tactical Networks (JTN)
Joint Enterprise Network Manager (JENM)

Executive Summary
- DOT&E assessed the Joint Enterprise Network Manager (JENM) during the Mid-tier Networking Vehicular Radio (MNVR) Limited User Test (LUT) during the Network Integration Evaluation (NIE) 15.2.
  - Contractors using JENM were able to plan, configure, and load MNVRs prior to the LUT. Soldiers did not demonstrate these tasks during the operational test.
  - Soldiers were trained on JENM, but they could not effectively monitor or manage MNVR networks, or characterize the health of individual MNVR nodes and Wideband Networking Waveform (WNW) links.
- The Army's development, test, and fielding strategy since moving into sustainment has been to conduct government testing of JENM with waveforms, perform operational assessments based on surveys, and field new software increments. Project Manager (PM) Warfighter Information Network – Tactical (WIN-T) is developing a Test and Evaluation Master Plan (TEMP) that describes the test and evaluation strategy of the JENM and waveforms in coordination with the host radio programs. The target timeframe for completion is 1QFY17.
- The Army collected data from the Mobile User Objective System (MUOS) Multi-Service Operational Test and Evaluation 2 (MOT&E 2), NIE 16.2, Army Warfighting Assessment 17.1, and WNW simulation testing at the program manager's San Diego, California, facility to support a fielding of JENM 3.3. Data to support the fielding consisted of developmental testing and operator interviews and surveys.

System
- JENM is the Army enterprise solution for network operations to the Joint Tactical Network (JTN). JENM is designed to support planning, loading, monitoring, and managing current and future waveforms and software-defined radios.
- Software-defined waveforms are loaded into and considered a part of a radio set. JENM is capable of supporting radios integrated with the following software-defined waveforms: Soldier Radio Waveform (SRW), WNW, Single Channel Ground and Airborne Radio System (SINCGARS), ultra-high frequency satellite communications (SATCOM), and MUOS.



- The Army intends JENM to:
  - Provide network operations to current and future waveforms and software-defined radios. Current software-defined radios include Rifleman Radio, Manpack Radio, and MNVR. JENM will support the future Airborne Maritime Fixed Station Small Airborne Networking Radio.
  - Enable configuration, loading, monitoring, and management of the tactical radio network.
  - Provide an enterprise over-the-air management (eOTAM) capability. eOTAM is a real time command/response protocol between JENM and radios, enabling over-the-air radio and network management with JENM as the controller.

Mission
- Military forces use the software-defined radios to communicate and create networks to exchange voice, video, and data during all aspects of tactical military operations.
- Signal staffs use JENM to:
  - Plan, load, monitor, configure, troubleshoot, and prioritize network operations involving software-defined radio sets running SRW, WNW, SINCGARS, and tactical SATCOM
  - Provision a MUOS terminal to connect to a MUOS satellite network

Major Contractor
Government-developed by Network Management Reference Implementation Laboratory – San Diego, California

Activity
- As previously reported in the FY15 Annual Report (MNVR article), DOT&E assessed JENM 3.1 as a part of the MNVR LUT during NIE 15.2. The Army conducted the test according to a DOT&E-approved test plan. Prior to the LUT, contractors planned and configured the WNW and SRW networks. Contractors loaded the network plan and communications

security (COMSEC) into the MNVR radios. During the exercise, soldiers attempted to monitor and manage the network.
- Although still funded as one program, the JTN program split responsibilities for JENM and Waveforms between two PMs. Responsibility for JENM transferred from PM JTN to PM WIN-T. PM Tactical Radios assumed responsibility for the waveforms.
- JENM had a draft TEMP prior to the transition from PM JTN to PM WIN-T. PM WIN-T is developing a TEMP that describes the test and evaluation strategy of the JENM and waveforms in coordination with the host radio programs. The target timeframe for completion is 1QFY17.
- Consistent with the previous test and evaluation strategy, the Army collected data to support the fielding of JENM 3.3 consisting of developmental testing and operator interviews and surveys. The Army collected data during MUOS MOT&E 2, NIE 16.2, Army Warfighting Assessment 17.1, and government-conducted WNW simulation testing.
  - In October 2015, during MUOS MOT&E 2, soldiers equipped with JENM 3.2 provisioned Manpack radios using the Simple Key Loader to load COMSEC keys and MUOS terminal profile information.
  - Prior to NIE 16.2, the Army conducted new equipment training for soldiers on how to configure a network with JENM 3.3. During the validation exercise, soldiers loaded network plans and COMSEC keys on Manpack radios running SRW, SATCOM, and SINCGARS waveforms. The Army assessed the ability of the unit equipped with JENM to execute network management and monitoring tasks.
  - During NIE 16.2, contractors demonstrated some eOTAM functionality with Manpack and MNVR over the SRW and WNW networks as a proof of concept.
  - During Army Warfighting Assessment 17.1, the Army conducted an over-the-shoulder assessment of soldiers configuring, loading, monitoring, and managing a WNW network on the MNVR with JENM 3.3.

Assessment
- During the MNVR LUT at NIE 15.2, soldiers could not effectively monitor or manage MNVR networks with JENM 3.1, and were not able to characterize the health of individual MNVR nodes or individual WNW links. Contractors using the JENM were able to plan, configure, and load MNVRs prior to the LUT.
- In October 2015 during MUOS MOT&E 2, soldiers took several days to provision the Manpacks and they relied on contractors to complete the loading and provisioning of the radios.
- During the NIE 16.2 validation exercise, soldiers loaded network plans and COMSEC on Manpack radios running SRW, SATCOM, and SINCGARS waveforms. Soldiers were comfortable with the loading process. It took between 1.5 to 2.0 hours to load all of the radios in a company. The Army observed the ability of the unit equipped with JENM to execute network management and monitoring tasks. At the company level, communications soldiers are too busy to monitor the SRW network. JENM network monitoring of SRW lacks a map display showing the location of the radios.
- During Army Warfighting Assessment 17.1, the loading of the radio-configuration files and COMSEC keys was complicated and lengthy. Soldiers used JENM to configure the WNW network over-the-air by conducting over-the-air zeroization with the support of contractors.
- The PM demonstrated JENM's capability to monitor the WNW network and conduct eOTAM at a laboratory event using WNW simulation.
- The Army's development, test, and fielding strategy since moving into sustainment has been to conduct government testing of JENM with waveform versions, perform operational assessments based on surveys, and field new software increments.
  - The JENM program in the past 18 months has coordinated its schedule with Waveforms and not Tactical Radio programs. This process has precluded the ability to discover radio-unique integration problems. The implementation of waveform protocols is unique to each vendor. In addition, waveforms are frequently updated, so the version on the tactical radio available at operational testing may not be the version the JENM product office has built to. Changing focus of coordination to the Tactical Radio programs would synchronize JENM with both the radios and the waveform resident on the radio for both testing and fielding.
  - The operational evaluation strategy, based on surveys and observations, lacks an objective assessment of the effectiveness of the system. Future evaluations require instrumented data to verify JENM capabilities.
  - To remedy this, PM WIN-T is developing a TEMP that describes an adequate test and evaluation strategy of the JENM and waveforms in coordination with the host radio programs. The target timeframe for completion is 1QFY17.
- The Army tactical network is complex for soldiers to design and plan. Network planning consists of developing the signal support architecture and radio platform preset architecture (Internet Protocol addressing and router programming). In all cases this is done by government engineers and contractors. Soldiers have executed network configuration (i.e., establishing call groups) with significant training, retraining, and contractor assistance.
- JENM has improved in usability and functionality with each software version as indicated by the ability of the soldiers to successfully perform network loading tasks without contractor assistance with JENM 3.3. Future capabilities and upgrades should be undertaken against prioritized and validated requirements.

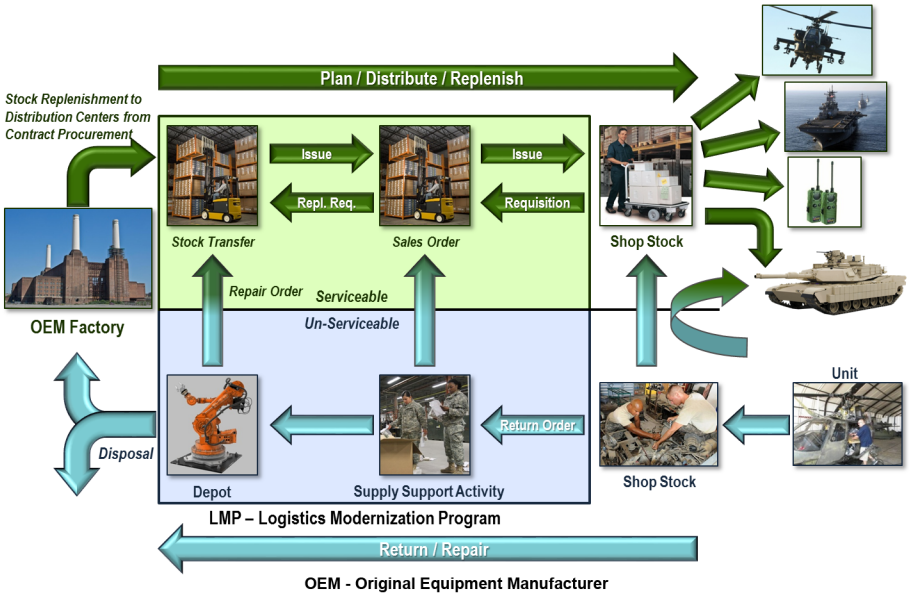
Recommendations

- Status of Previous Recommendations. The Army still needs to evaluate the force structure requirements of adding software-defined, networking radios and network management responsibilities into company-level organizations.
- FY16 Recommendations. The Army should:
  1. Complete a JENM TEMP that describes robust testing and objective evaluations of the JENM in conjunction with the Army's software-defined radio operational tests.
  2. Prioritize and validate the requirements for JENM.
  3. Reduce the need for contractors and reduce the complexity of soldier tasks for network configuration.

Logistics Modernization Program (LMP)

Executive Summary

- From September 8 through November 20, 2015, the Army Test and Evaluation Command (ATEC) conducted the IOT&E of the Logistics Modernization Program (LMP) Increment 2 Wave 3 Release 7 at three Army Materiel Command (AMC) depots. The test and evaluation of LMP was adequate to support a DOT&E assessment of operational effectiveness, suitability, and survivability.
- LMP is operationally effective. The system successfully completed 98 percent of the observed tasks and successfully processed more than 99 percent of the more than 1.3 million Intermediate Documents to and from interfacing systems in 2015. Since LMP Increment 2 Wave 3 Release 7 went live in June 2015, users reported zero critical or major problems.
- LMP is operationally suitable; however, usability and user workload need improvement. LMP performance exceeded the requirements for system reliability and availability.
- LMP is survivable against an unaided outsider cyber threat having nascent- to limited-level capabilities, but demonstrated it is vulnerable to both nascent- to limited-level insider threats and to an outside threat aided by insiders.
- During the August 1 – 4 , 2016, cybersecurity Verification of Fixes (VoF), LMP demonstrated it had corrected all high- and medium-risk cybersecurity vulnerabilities; however, detect, react, and restore cybersecurity capabilities were not in scope for that event and will be assessed in future cybersecurity testing.
- In support of its 2015 Cyber Economic Vulnerability Assessment (CEVA), the LMP Program Management Office (PMO) chose a commercial vendor that had provided cybersecurity economic subject matter expertise on another Enterprise Resource Planning (ERP) program; however, the vendor's lack of experience regarding LMP and AMC's business processes yielded only high-level findings and recommendations.
- On September 2, 2016, AMC made a full deployment declaration for LMP Increment 2, which will allow the increment to transition to the operation and sustainment phase of the acquisition lifecycle.



System

- LMP is the Army's core logistics Information Technology initiative and is one of the world's largest, fully integrated supply chain, maintenance, repair and overhaul, planning, execution, and financial management systems.
- LMP is an SAP-based commercial off-the-shelf ERP solution that manages and tracks orders and delivery of materiel from the AMC to soldiers where and when they need it.
- LMP transforms Army logistics operations in eight core business areas: acquisition, distribution, finance, product lifecycle management, supply chain planning, depots/arsenals (formerly manufacturing/remanufacturing), maintenance, and warehouse inventory management.
- LMP replaced the two largest national-level logistics systems: the inventory management Commodity Command Standard System, and the depot and arsenal operations Standard Depot System. LMP Increment 2 expands on the already deployed/operational production baseline to specifically address shop floor automation, automatic identification technology, and expanded ammunition requirements. Increment 2 improves outdated or manual processes, updates the other Army ERP systems with relevant information about the Army's military equipment, and provides the tools to support total asset visibility.
- LMP is currently deployed to approximately 30,000 users in more than 50 Army and DOD locations around the world, and interfaces with more than 80 DOD systems.

Mission

The AMC uses LMP to sustain, monitor, measure, and improve the Army's modernized national-level logistics support in order to save Army manpower and money through streamlined activities and greater visibility of logistics operations.

Major Contractors
- CSRA – Fairfax, Virginia
- INSAP Services Inc. – Marlton, New Jersey
- Attain, LLC – McLean, Virginia

Activity
- From September 8 through November 20, 2015, ATEC conducted an adequate IOT&E of the LMP Increment 2 Wave 3 Release 7 at three AMC depots (Corpus Christi Army Depot, Texas; McAlester Army Ammunition Plant, Oklahoma; and Rock Island Arsenal, Illinois). The Army conducted all testing in accordance with a DOT&E-approved test plan.
- Army Research Laboratory's Survivability/Lethality Analysis Directorate conducted a cybersecurity VoF January 19 – 22, 2016, and a follow-up cybersecurity VoF August 1 – 4, 2016.
- On September 2, 2016, the AMC signed a full deployment declaration memorandum for LMP Increment 2, which ends the technical and testing requirements allowing the increment to transition to the operation and sustainment phase of the acquisition lifecycle. DOT&E will continue oversight of LMP's improvements to cybersecurity.
- In FY17, LMP is scheduled to transition its program and data to Defense Information Systems Agency (DISA) Defense Enterprise Computing Centers (DECCs).

Assessment
- LMP is operationally effective.
  - During the IOT&E, users successfully completed 98 percent of the observed Mission Critical Function (MCF)-associated tasks and the Business Operations Test (BOT) confirmed that all but one of the remaining tasks functioned correctly.
  - LMP had no Severity 1 "critical" or Severity 2 "major" problems since the system went live in June 2015. LMP successfully processed more than 99 percent of the more than 1.3 million Intermediate Documents to and from interfacing systems during 2015.
  - Data collectors did not observe some tasks during the IOT&E because the test took place at live, operational locations and users did not perform the tasks over the course of the IOT&E. Data associated with Item Unique Identification (IUID) were not collected because IUID tags have not been placed on all Army logistics items.
  - ATEC assessed LMP Increment 2 as not effective because testers observed only 67 percent of the MCFs during the IOT&E. DOT&E disagrees with the ATEC assessment because testers observed all the missing MCF tasks during the BOT. The BOT involved actual LMP operators using realistic LMP data on a production-representative system.
- LMP is operationally suitable. Users surveyed during the IOT&E rated LMP a mean System Usability Scale score that is representative of "ok" usability and noted their workload remains high because they are using legacy systems concurrently with LMP. This will be the case until LMP completely replaces legacy systems in FY18. LMP demonstrated a Mean Time Between System Failure (MTBSF) of 1,026 hours, which exceeded the requirement of 110 hours MTBSF. LMP had an availability of 96 percent meeting the 95 percent requirement.
- LMP is survivable to an unaided outsider cybersecurity threat having nascent- to limited-level capabilities, but is not survivable to both nascent- to limited-level insider threats and to an outside threat aided by insiders.
- During the August 1 – 4 , 2016, cybersecurity VoF, LMP demonstrated it had corrected all high- and medium-risk cybersecurity vulnerabilities; however, detect, react, and restore cybersecurity capabilities were not in scope for that event and will be assessed in future cybersecurity testing. The remaining low-risk vulnerabilities are either mitigated or will be corrected after LMP migrates to DISA DECCs.
- The 2015 CEVA portion of the LMP cybersecurity testing was inadequate because the LMP PMO chose a commercial vendor that lacked experience with LMP and AMC's business processes and because the vendor failed to conduct a significant portion of the CEVA. Although the vendor had provided cybersecurity economic subject matter expertise on another ERP program, its work during the LMP CEVA yielded only high-level findings and recommendations.
- Although the CEVA was inadequate, the overall test and evaluation of LMP was adequate to support a DOT&E assessment of operational effectiveness, suitability, and survivability.
- During its annual continuity of operations (COOP) test in December 2015, LMP demonstrated the feasibility of, but did not conduct, a transfer of operations to and from the COOP location.
- The 2010 National Defense Authorization Act requires financial audibility by 2017. The Program Office continues to work to achieve certification in accordance with the Federal Financial Management Improvement Act through various audits.

Recommendations
- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The LMP Program Office should:
  1. Conduct an FOT&E of LMP, focused on IUID and the tasks that were not observed during the IOT&E, when the IUID capability is fully available to LMP users.

2. Continue to survey LMP users to determine if the problem of increased user workload relative to legacy systems is improving.
3. After LMP data and program services transition to DISA DECCs, conduct another cybersecurity test from both the insider and outsider posture to verify the correction of known vulnerabilities and to possibly identify new vulnerabilities.
4. Ensure the cybersecurity economic subject matter experts chosen for the next CEVA understand the operational capabilities and key business processes used within the system to include roles and responsibilities.
5. Use the transition to the DISA DECCs to simulate a full transfer of operations to and from the COOP location.

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

Executive Summary

- The Army continued multiple phases of the M109 Family of Vehicles (FoV) Paladin Integrated Management (PIM) developmental testing at Yuma Proving Ground, Arizona, that included live firing performance, automotive performance, and reliability.
- The Army continued with live fire testing of the underbody IED protection kit, validation live fire testing of modified armored areas, and simulated damage testing of the electrical system at Aberdeen Proving Ground, Maryland.
- The Army began the M109 FoV PIM IOT&E in October 2016 at Fort Hood, Texas, but suspended it due to safety concerns. DOT&E will submit an IOT&E report in 2QFY17. A second IOT&E will be rescheduled for FY18 once corrective actions are complete.

System

- The M109 FoV PIM consists of two vehicles: the Self-Propelled Howitzer (SPH) and Carrier Ammunition Tracked (CAT) resupply vehicle.
  - The M109A7 SPH is a tracked, self-propelled 155 mm howitzer designed to improve sustainability over the legacy M109A6 howitzer fleet. The production howitzers have a modified M109A6 turret with a high-voltage electrical system and a modified Bradley Fighting Vehicle chassis, power train, and suspension. The M109A7 does not include upgrades to the cannon. A crew of four soldiers operates the SPH and can use it to engage targets at ranges of 22 km using standard projectiles and 30 km using rocket-assisted projectiles.
  - The M992A3 CAT supplies the SPH with ammunition. The full-rate production ammunition carriers have a chassis similar to the SPH. The ammunition carriers are designed to carry 12,000 pounds or 98 rounds of ammunition in various configurations. A crew of four soldiers operates the CAT.
- The Army will equip the SPH and CAT with two armor configurations to meet two threshold requirements for force protection and survivability – Threshold 1 (T1) and Threshold 2 (T2).
  - The base T1 armor configuration is integral to the SPH and CAT. The Army intends the T2 configuration to meet protection requirements beyond the T1 threshold with add-on armor kits.
  - The Army plans to employ PIM vehicles in the T1 configuration during normal operations and will equip the SPH and CAT with T2 add-on armor kits during combat operations.
- The Army designed an underbody kit to determine the potential protection an SPH and CAT could provide against IEDs similar to those encountered in Iraq and Afghanistan. The Army purchased five underbelly kits for test purposes. At this time, the Army does not intend to equip the SPH or CAT with the underbody kit.
- The Army intends to employ the M109 FoV as part of a Fires Battalion in the Armored Brigade Combat Team and Artillery Fires Brigades to support any Brigade Combat Team.
- The Army plans to field up to 557 sets of the M109 FoV with full-rate production planned for FY17.

Mission

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

Major Contractor

BAE Systems – York, Pennsylvania

Activity

- In FY16, the Army received 16 low-rate initial production (LRIP) SPH and CAT vehicles and conducted Production Qualification Testing (PQT) on the CAT and SPH at Yuma Proving Ground, Arizona:
  - PQT of LRIP vehicles included Cold Regions testing, performance live firing and automotive testing, characterization testing with T2 armor and underbelly kit, testing with the Crew Remote Operated Weapon System, and the Logistics Demonstration to validate operator and maintainer technical manuals and work packages.
  - The program began replacement of the steel cannon tubes with chrome-lined tubes to address tube wear and corrosion issues caused by use of the Modular Artillery Charge System (MACS).
  - In concert with the Program Executive Office Ammunition, the PIM program will use a redesigned M82 primer in IOT&E to better withstand pressures introduced by the higher zones (4&5) of the MACS propellant charges.
- The Army continued the execution of the LFT&E program at Aberdeen Proving Ground, Maryland, in accordance with DOT&E-approved test plans:
  - Exploitation testing on the CAT to validate armor modifications. Additional exploitation testing will be conducted on the SPH to complete validation of modifications to the T1 and T2 armor systems, made to address vulnerable areas identified in early testing.
  - Controlled damage experimentation on the high voltage electrical system to determine the consequences of ballistic damage.
  - The Army conducted all LFT&E in accordance with DOT&E-approved test plans.
  - The Army began full-up system-level testing of the M109 SPH and CAT resupply vehicle in 1QFY16.
- The Army began the M109 FoV PIM IOT&E in October 2016 at Fort Hood, Texas, but suspended testing after one of three test vignettes to determine the root cause of the toxic fumes coming into the cab of the howitzer. That effort continues. DOT&E will submit an IOT&E report in 2QFY17. A second IOT&E will be rescheduled for FY18 once corrective actions are complete.

Assessment

- Over the course of the Developmental Performance, Automotive, and LFT&E program, the Program Office has taken considerable action to correct deficiencies identified in early testing and to validate associated fixes.
  - During armor exploitation testing, most of the modified armored areas demonstrated that they provide protection against Key Performance Parameter threats.
  - Changes to the crew compartment Automatic Fire Extinguisher System (AFES) in the CAT mitigate the deficiency identified in early testing and reduce the CAT's vulnerability to fires.
- The crew compartment AFES in the SPH was designed to protect a small, localized area in the crew compartment. Live fire testing demonstrated that the system is deficient in providing adequate fire survivability. The Program Office is developing courses of action to redesign this system and improve SPH survivability to fires. While not yet optimized, the M109A7 provides improved crew fire safety compared to the currently fielded M109A6 because:
  - The M109A7 has crew compartment AFES capability while the M109A6 has none.
  - The M109A7 has reduced fire hazards compared to the M109A6 because of the replacement of hydraulic systems, found on the M109A6, with electric drives.
- The Army verified that the base SPH has the potential to provide underbody IED protection against the requirement blast threat and the objective level threat when equipped with the underbody blast kit.
- Reliability issues found on both the CAT and the SPH have been addressed in a comprehensive test-fix-test cycle throughout the PQT phase.
- Legacy system (parts common to the current M109A6) failures involving breech componentry and primer failures continue to arise in live fire testing and will not be addressed until follow-on developmental work is completed. Engine component failures in both the CAT and the SPH have been initially traced to transmission oil cooler design discrepancies. An interim design change has mitigated further failures and additional testing is ongoing. A final design change will occur during full-rate production.

Recommendations

- Status of Previous Recommendations. In FY15, the Army made design changes to mitigate the deficiencies in the CAT's crew compartment AFES and validated those changes in test. The Army has not yet incorporated changes to address the deficiencies in the SPH's crew compartment AFES but has developed and is reviewing several courses of action to address this issue.
- FY16 Recommendations. The Army should:
  1. Continue development of breech component upgrades and verify corrections for both the breech and engine deficiencies in testing.
  2. Correct the deficiencies in the SPH's crew compartment AFES and validate those fixes in test.

Mid-Tier Networking Vehicular Radio (MNVR)

Executive Summary

- In April through May 2016, the Army's Brigade Modernization Command (BMC) conducted a Mid-Tier Network and Mid-Tier Networking Vehicular Radio (MNVR) Operational Assessment (OA) as part of the Network Integration Evaluation (NIE) 16.2. The BMC assessed the concept of operations and basis of issue of a brigade's MNVR network operating in and out of a satellite-denied environment. The Army's assessment was not conducted according to a DOT&E-approved test plan, but DOT&E did observe the entire assessment and wrote an independent MNVR evaluation.
- The Army's BMC assessment of the NIE 16.2 MNVR OA is the following:
  - Recommend continued development of the mid-tier network solution to bridge the upper and lower tactical internets. Commanders validated the Army requirement for a mid-tier network solution.
  - Recommend the Army not field the MNVR as the mid-tier network solution. The limitations of the MNVR did not meet commanders' requirements to include the ability to provide consistent and reliable mission command services, maintain an effective operational range, and integrate into appropriate combat platforms.
- DOT&E's evaluation of the NIE 16.2 MNVR OA is the following:
  - MNVR did not meet commanders' requirements for a mid-tier network solution. Statistical analysis of NIE 16.2 results demonstrated there was no significant difference in the ability of commanders to accomplish their missions having the MNVR and not having the radio in a satellite-denied environment.
  - Commanders desired a 16-kilometer range for the mid-tier network, which is substantially further than the 6 – 10 kilometer requirement in the MNVR Capabilities Production Document. During NIE 16.2, infantry companies and cavalry troops operated in excess of 10 kilometers forward of their battalions for over 60 percent of the exercise.
  - The Army needs to conduct a complete IOT&E to test all features of MNVR and Joint Enterprise Network Manager (JENM) within an operationally representative unit.
- In July 2016, DOT&E approved the MNVR Test and Evaluation Master Plan (TEMP) in support of a September 2016 Milestone C decision to describe post-Milestone C developmental testing and an MNVR IOT&E.
- In September 2016, the Defense Acquisition Executive approved a low-rate initial production (LRIP) of 478 MNVRs. The Army intends to field the LRIP MNVRs to five Infantry Brigade Combat Teams (IBCTs), which far exceeds the one-brigade set needed to support the MNVR IOT&E.

- In September 2016, the Army published a new MNVR competitive acquisition that shifts the MNVR IOT&E to FY20. The new MNVR competitive acquisition is scheduled for a source selection against revised MNVR requirements and contract award in FY18-19. The results of this acquisition effort will likely result in a different radio and waveform to meet the Army's modified requirements and therefore, be of significantly different design than the LRIP MNVRs fielded to the five IBCTs.
- The Army needs to revise the approved MNVR TEMP to reflect the Army's new competitive strategy and testing that leads to an FY20 MNVR IOT&E.

System

- The Army's AN/VRC-118 MNVR program evolved from the terminated Joint Tactical Radio System, Ground Mobile Radio to provide software-programmable digital radios to support Army tactical communications requirements from company through brigade.
- The Army intends the MNVR to:
  - Operate at various transmission frequencies using the Soldier Radio Waveform (SRW) and the Wideband Networking Waveform (WNW).
  - Bridge the upper tactical communications networks at brigade and battalion with the lower tactical networks at company employing a terrestrial radio network.
  - Provide an alternative terrestrial transmission path in the absence or limited availability of satellite communications.
- The MNVR operates up to 75 watts maximum power output for WNW and up to 50 watts maximum power output for SRW.
- The JENM provides the means to plan, load, configure, and monitor MNVR networks.
- The MNVR includes both vehicle-mounted and Tactical Operations Center kit versions.

- The MNVR is a non-developmental item selected through multi-vendor competition.

Mission
- Army commanders intend to use the MNVR to:
  - Provide networked communications for host vehicles and Tactical Operations Centers during all aspects of military operations
  - Communicate and create terrestrial radio networks to exchange voice, video, and data using the SRW and the WNW.
  - Share data between different tactical communication networks and mission command systems
- Signal staffs employ the JENM to plan, load, monitor, control, and report on network operations of MNVR networks running SRW and WNW.

Major Contractor
Harris Corporation, Tactical Communications – Rochester, New York

---

Activity
- In November 2015, the Army conducted the MNVR Government Regression Test (GRT) at the Electronic Proving Ground in Fort Huachuca, Arizona. The GRT tested fixes to deficiencies discovered during the April to May 2015 NIE 15.2 MNVR Limited User Test and previous developmental testing, and assessed new MNVR capabilities. During the GRT, MNVR:
  - Demonstrated WNW and SRW data requirements
  - Demonstrated JENM configuration and over-the-air management of the MNVR
  - Was interoperable with Advanced Field Artillery Tactical Data System, Nett Warrior, and Joint Battle Command – Platform (JBC-P)
  - Met reliability requirements for all waveforms except the WNW anti-jam waveform
  - Did not demonstrate significant improvement in cybersecurity
- In April through May 2016, the Army BMC conducted a Mid-Tier Network and MNVR OA during NIE 16.2. During the MNVR OA, the Army equipped the 2nd Brigade, 1st Armored Division with MNVRs. The brigade headquarters and six battalions conducted missions under operationally realistic conditions. The BMC assessed the concept of operations and basis of issue of the MNVR network operating in and out of a satellite-denied environment. The mid-tier network and MNVR operated as part of the larger NIE 16.2 network during the OA, which included Warfighter Information Network – Tactical (WIN-T) Net Centric Waveform (NCW) satellite and JBC-P Blue Force Tracker (BFT) satellite. The Army's BMC assessment was not conducted according to a DOT&E-approved test plan, but DOT&E did observe the entire assessment and wrote an independent MNVR evaluation.
- In July 2016, DOT&E approved the MNVR TEMP in support of a September 2016 Milestone C decision to describe post-Milestone C developmental testing and an MNVR IOT&E.
- On July 5, 2016, DOT&E published a report on the results of BMC's NIE 16.2 Mid-Tier Network and MNVR OA.
- In September 2016, the Defense Acquisition Executive approved an LRIP of 478 MNVRs. The Army intends to field the LRIP MNVRs to five IBCTs, which far exceeds the one-brigade set needed to support the MNVR IOT&E.
- In September 2016, the Army published a new MNVR competitive acquisition that shifts the MNVR IOT&E to FY20. The new MNVR competitive acquisition is scheduled for a source selection against revised MNVR requirements and contract award in FY18-19.

Assessment
- The Army's BMC assessment of the NIE 16.2 MNVR OA is the following:
  - Recommend continued development of the mid-tier network solution to bridge the upper and lower tactical internets. Commanders validated the Army requirement for a mid-tier network solution.
  - Recommend the Army not field the MNVR as the mid-tier network solution. The limitations of the MNVR did not meet commanders' requirements to include the ability to provide consistent and reliable mission command services, maintain an effective operational range, and integrate into appropriate combat platforms.
- DOT&E's evaluation of the NIE 16.2 MNVR OA is the following:
  - MNVR did not meet commander's requirements for a mid-tier network solution.
  - Statistical analysis of NIE 16.2 results demonstrated there was no significant difference in the ability of commanders to accomplish their missions having the MNVR and not having the radio in a satellite-denied environment.
  - Commanders did not detect a difference between having the MNVR and not having the MNVR when the BFT and NCW satellite were off.
  - Having the brigades full authorization of MNVRs (85 nodes) did not improve mid-tier communications.
  - Commanders desired a 16-kilometer range for the mid-tier network.
  - The MNVR Capabilities Production Document requirement is 6 – 10 kilometers.
  - During NIE 16.2, infantry companies and cavalry troops operated in excess of 10 kilometers forward of their battalions for over 60 percent of the exercise.

  - Commanders identified a need for a mid-tier network, but not the one provided by the MNVR WNW network.
  - Soldiers identified position location information and text messaging as the most important messages. These messages do not require the bandwidth provided by WNW.
  - MNVR requires more power to operate than legacy radio equipment. This requires vehicles to maintain continuous idle during MNVR operations.
  - MNVR is too large and draws too much power to be integrated into the leader vehicles (Abrams and Bradley).
- The results of the new MNVR competitive acquisition effort will likely result in a different radio and waveform to meet the Army's modified requirements and therefore, be of significantly different design than the LRIP MNVRs fielded to the five IBCTs.
- Due to the program changes resulting from the MNVR competitive acquisition, the Army needs to revise the approved MNVR TEMP to reflect the Army's MNVR competitive source selection and testing leading to a FY20 MNVR IOT&E.

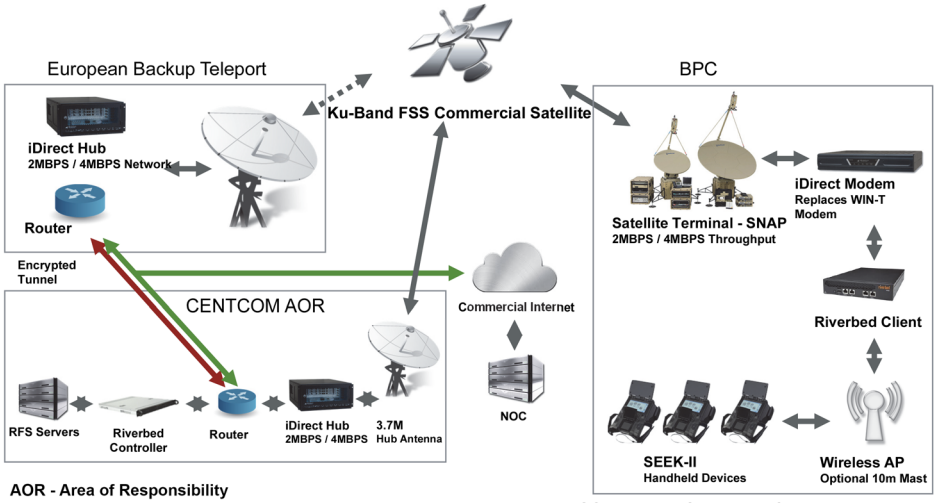
Recommendations

- Status of Previous Recommendations. The MNVR Program Office has addressed the previous recommendations to continue development and develop a Milestone C TEMP. Planning of the IOT&E has continued.
- FY16 Recommendations. The Army should:
  1. Reevaluate MNVR transmission range and throughput requirements to reflect operational mission needs of the unit.
  2. Revise its post-Milestone C MNVR TEMP to reflect the developmental test and activities leading to the planned FY20 MNVR IOT&E.
  3. Plan and conduct an MNVR IOT&E using an IBCT equipped with WIN-T, JBC-P, and MNVR in accordance with an Army-approved MNVR basis of issue plan.

Near Real Time Identity Operations (NRTIO)

Executive Summary

- Near Real Time Identity Operations (NRTIO) is a Joint Emerging Operational Need (JEON) intended to provide the following capabilities to U.S. Central Command (USCENTCOM) in support of Operation Inherent Resolve:
  - Near real-time identity information to U.S. conventional forces to enhance force protection, stem the flow of foreign fighters, and counter the threat from IEDs
  - Increased partnership capacity by sharing collected biometric data with partner nations and other coalition forces to establish the identity of adversaries transiting the USCENTCOM Area of Responsibility (AOR)
- NRTIO achieved Initial Operating Capability (IOC) in February 2016, and the Army Test and Evaluation Command (ATEC) conducted an IOC operational assessment (OA) from March through July 2016 using data from the USCENTCOM AOR.
- Test limitations precluded the assessment of operational effectiveness, operational suitability, and cybersecurity during the IOC OA, including:
  - Due to the IOC state of NRTIO, soldiers could not use its full capability. The biometric dataset on the Remote Forward Server (RFS) was incomplete, which reduced the rate of biometric submission matches against the biometrically enabled watchlist (BEWL). The IOC OA demonstrated that biometric submissions to the RFS had a lower than acceptable match accuracy.
  - To avoid disruption to real-world missions, USCENTCOM did not permit testers in theater but ATEC received 25 survey responses from NRTIO users. It is not known if these responses represent a statistically significant sample size.
  - USCENTCOM did not permit cybersecurity testing on the production hardware and software due to mission constraints.
- During the IOC OA, soldiers successfully completed enrollments and matches with their local collection device against watchlists on the NRTIO RFS and the DOD authoritative database (Automated Biometric Identification System (ABIS)). Due to IOC OA constraints, RFS response timeliness could not be adequately assessed. During the OA, most biometric submissions consisted of batch submissions of biometric enrollment records, which are not near real-time submissions. As part of the OA, the capability to make biometric submissions and receive near real-time responses was demonstrated but the sample size is not statistically significant.



- Prior to reaching Full Operating Capability (FOC), NRTIO requires a technical modernization to improve the accuracy and completeness of the RFS biometric dataset. An accurate and complete biometric dataset in the RFS that contains all of the watchlisted identities relevant to the USCENTCOM AOR is necessary to demonstrate near real-time identity operations.

System

The NRTIO JEON intends to provide the forward-deployed Service member the capability to receive an identity response in near real-time of submission of biometric information. The IOC OA configuration includes:

- Handheld Biometric Collection devices. The Secure Electronic Enrollment Kit (SEEK) II performs fingerprint capture, dual iris scan, and facial capture. The devices are compliant with Electronic Biometric Transmission Specification (EBTS) and Electronic Fingerprint Transmission Specification (EFTS), which are requirements for interface with ABIS.
- Dedicated communications capacity including tactical satellite (TACSAT), satellite communications (SATCOM), and WiFi connectivity.
- RFS. The RFS includes the USCENTCOM AOR-specific biometric records that allow for rapid, non-authoritative match results to be provided to the forward deployed warfighter. ABIS verifies the biometric matches using the authoritative database, which possesses a larger dataset.
- Web-based Exploitation and Analysis Portal. An identity operations portal that provides web-based real-time collaboration, automated report generation, materiel management, data search and correlation, alerting, and a database for exploitation and collaboration. The portal used

during the IOC OA was the Identity Resolution Exploitation and Management Services Collaborative Workstation (ICW).

Mission
- USCENTCOM forces use the NRTIO IOC capability for identity operations to provide timely, accurate, and complete responses indicating whether persons of interest encountered in the field have a prior history of derogatory (e.g. criminal) activity, to assist in identifying potential threats to U.S. forces and facilities throughout the USCENTCOM AOR.
- Upon achieving FOC, forward-deployed Service members will use NRTIO to provide biometric responses including tailored biometric matching and watchlisting within the USCENTCOM AOR.

Major Contractors
- Booz Allen Hamilton – Belcamp, Maryland
- Envistacomm LLC – Atlanta, Georgia

Activity

ATEC conducted the following testing in FY16:
- The IOC OA of the NRTIO system from March to July 2016
- A cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA) during developmental testing of a clone of the IOC portal, one component of the NRTIO, in July 2016

Assessment
- The IOC OA leveraged the operational assessment process of the JEON and focused on whether the technology is viable to meet the warfighter requirements and will be used to inform the tailored Test and Evaluation Master Plan (TEMP) and operational test plan to support FOC. At the FOC OA, the operational assessment will focus on the operational effectiveness, suitability, and survivability of the NRTIO system under test. Accordingly, the test needs to have a DOT&E-approved test plan and tailored TEMP.
- During the IOC OA, the biometric dataset on the RFS was incomplete, which reduced the rate of biometric submission matches against the BEWL. To meet mission timelines, ATEC started operations on the RFS without the complete biometric and latent dataset relevant to the USCENTCOM AOR. Match consistency between the RFS and ABIS is a key criterion for establishing operator confidence in the RFS. If biometric matches are missed by the RFS, a potential person of interest may not be identified. The RFS technology limitation of having not fully ingested the entire biometric database precluded assessment of the dynamic synchronization of the DOD BEWL with the RFS.
- Due to IOC OA constraints, DOT&E could not adequately assess RFS response timeliness. During the OA, most biometric submissions consisted of batch submissions of biometric enrollment records, which are not near real-time submissions. As part of the OA, the capability to make biometric submissions and receive near real-time responses was demonstrated. However, the majority of the IOC OA biometric enrollments were submitted using a bulk file upload to the portal, which forwarded the data on to both ABIS and the RFS. Bulk uploading of biometric submissions is adequate for many operational needs.
- To avoid disruption to real-world missions, USCENTCOM did not permit testers in theater but ATEC received 25 survey responses from NRTIO users. It is not known if these responses represent a statistically significant sample size. Survey responses noted suitability problems that included high workloads including periods of enrollment surges, long upload times, and communications outages. There were many non-materiel shortcomings. Areas to address to improve suitability include lack of leadership awareness of the importance of biometrics, the need for intensive training of soldiers with no prior biometrics experience, and transportability hardships because of the hostile terrain in parts of the USCENTCOM AOR.
- ABIS operators at the Biometrics Identity Management Agency reviewed over 800 NRTIO biometric enrollments to assess whether soldiers were able to collect biometric data of match quality. For the NRTIO biometric enrollments, fingerprint quality was generally acceptable for obtaining accurate matches, whereas iris and facial images showed greater variability. Since most matches primarily rely on fingerprint data, the data quality of NRTIO biometric enrollments was adequate to support identity operations.
- Mission constraints prevented an adequate assessment of the cybersecurity posture during the ATEC-conducted CVPA on a clone of the ICW.

Recommendations
- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The Army should:
  1. Mature tactics, techniques, and procedures and address manpower requirements to improve suitability prior to FOC.
  2. Prior to FOC operational testing, load the current USCENTCOM subset of the BEWL on their SEEK IIs, so watchlisted individuals can be identified in near real-time.
  3. For FOC, streamline or automate training to improve the suitability of NRTIO.
  4. Conduct an operational CVPA and Adversarial Assessment on the NRTIO system including the RFS prior to FOC.
  5. Complete a technical modernization of the NRTIO system that has an accurate and complete biometric dataset in the RFS that contains all of the watchlisted identities relevant to the USCENTCOM AOR prior to FOC.
  6. Provide an operational test plan and tailored TEMP 30 days prior to the start of the FOC OA to DOT&E for approval.

Patriot Advanced Capability-3 (PAC-3)

Executive Summary
- The Army completed the Patriot Post-Deployment Build-8 (PDB-8) Developmental Test and Evaluation (DT&E) from July 2015 to July 2016.
- The Army conducted four Patriot flight tests and two Army Integrated Air and Missile Defense (AIAMD) flight tests using Patriot interceptors in FY16, achieving successful intercepts of all targets: five short-range ballistic missile (SRBM) targets, three cruise missile targets, and one fixed-wing aircraft target.
- The Army commenced the Patriot PDB-8 IOT&E in September 2016. This testing will continue through August 2017.

System
- Patriot is a mobile air and missile defense system that counters missile and aircraft threats. The newest version of Patriot hardware and software under development is PDB-8, which consists of improvements required to counter the evolving threat, to improve combat identification and the Air Defense Interrogator Mode 5 Identification, Friend or Foe (IFF) capability, to mitigate false tracks, to improve electronic protection, and to further integrate Missile Segment Enhancement (MSE) interceptor/ground system capabilities.
- The system includes the following:
  - C-band multi-function phased-array radars for detecting, tracking, classifying, identifying, and discriminating targets and supporting the guidance functions
  - Battalion and battery battle management elements
  - Communications Relay Groups and Antenna Mast Groups for communicating between battery and battalion assets
  - A mix of Patriot Advanced Capability-3 (PAC-3) hit-to-kill interceptors and PAC-2 blast fragmentation warhead interceptors for negating missile and aircraft threats
- The newest version of the PAC-3 interceptor under development is the PAC-3 MSE. The MSE provides increased battlespace defense capabilities and improved lethality over prior configuration Patriot interceptors.
- Earlier versions of Patriot interceptors include the Patriot Standard interceptor, the PAC-2 Anti-Tactical Missile, the Guidance Enhanced Missile (GEM) family (includes the GEM-T and GEM-C interceptor variants intended to counter tactical ballistic missiles and cruise missiles), the PAC-3 (baseline), and the PAC-3 Cost Reduction Initiative (CRI) variant.

Mission

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

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

Activity
- The Army conducted the Patriot PDB-8 DT&E from July 2015 to July 2016 at White Sands Missile Range (WSMR), New Mexico. The ground portion of this testing concluded in October 2015, with developmental flight tests occurring later:
  - In Flight Test P8-2 in November 2015, Patriot conducted a mixed ripple engagement of an SRBM target with PAC-3 CRI and PAC-2 GEM-T interceptors and then engaged a second SRBM target with two PAC-2 GEM-T interceptors.
  - In Flight Test P8-4 in December 2015, Patriot engaged an SRBM target with two PAC-3 MSE interceptors.
  - In Flight Test P8-3 in March 2016, Patriot conducted a mixed ripple engagement of an SRBM target with PAC-3 MSE and PAC-2 interceptors.
  - In Flight Test P8-1 in July 2016, Patriot engaged a cruise missile target with a PAC-2 GEM-T interceptor and then

engaged a maneuvering, full-scale, fixed-wing, air-breathing target with a PAC-3 MSE interceptor. The Army did not conduct this test in accordance with the DOT&E-approved Test and Evaluation Master Plan (TEMP), which stated that the fixed-wing aircraft would be employing electronic countermeasures while maneuvering. The Army has deferred testing of this capability to a Patriot PDB-8.1 flight test in 2020.

- The Army conducted two AIAMD flight tests at WSMR during FY16 using Patriot interceptors:
  - In AIAMD Flight Test-1 (FT-1) in November 2015, Patriot engaged a cruise missile target with a PAC-3 interceptor.
  - In AIAMD FT-3 in April 2016, Patriot engaged an SRBM target with one PAC-3 interceptor and conducted two separate PAC-2 GEM-T engagements against a cruise missile target, with the first engagement resulting in a missed intercept and the second engagement resulting in a successful intercept.
- The Army conducted lethality testing of the PAC-3 MSE lethality enhancer titanium fragments against Composition B explosive from July 2015 through June 2016 at Aberdeen Proving Ground, Maryland, to update the lethality model that predicts when a high-explosive initiation occurs within a warhead impacted by fragments.
- The Army conducted all testing in accordance with the DOT&E-approved TEMP and/or test plans, with the exception of the previously discussed P8-1 flight test and the PDB-8 flight test against an anti-radiation missile, which the Army deferred to a Patriot PDB-8.1 flight test in 2021 due to the lack of an available target.
- The Army commenced the Patriot PDB-8 IOT&E in September 2016 at Yuma Proving Ground, Arizona. The IOT&E, which will include flight tests conducted at WSMR and the Reagan Test Site at the Kwajalein Atoll in the Marshall Islands, will continue through August 2017. The IOT&E will provide information to support the PAC-3 MSE Full-Rate Production decision and the Army's deployment of Patriot PDB-8.
- The 2016 National Defense Authorization Act directs that the Missile Defense Agency and the Army conduct at least one intercept flight test each year that demonstrates interoperability and integration among the covered air and missile defense capabilities of the United States. In response to this act, Aegis Ballistic Missile Defense (BMD) will participate in Patriot's final operational flight test in FY17 as a forward-based sensor.

Assessment

- Problems previously discovered during the PDB-7 Limited User Test (LUT), if not corrected by the Army, could adversely affect Patriot PDB-8 effectiveness, suitability, or survivability. These problems, the details of which can be found in DOT&E's classified April 2013 Patriot PDB-7 LUT report, include:
  - Patriot PDB-7 performance against some threats improved compared to PDB-6.5, but there were degradations in performance against other threats. Patriot had some effectiveness shortfalls.
  - Patriot ground system reliability did not meet the threshold requirement, but would have met it had the Patriot radar achieved its allocated reliability goal.
  - Patriot ground system maintainability did not meet the threshold requirement.
  - Patriot training remained inadequate to prepare operators for complex Patriot engagements. This was also true during the PDB 6.5 and PDB-6 LUTs.
  - Patriot had some survivability and cybersecurity shortfalls.
- The Patriot system met most of its test objectives during the Patriot PDB-8 DT&E, but not all. During the ground test portion using simulated interceptors and mostly simulated targets, Patriot did not always properly transmit messages; detect, classify, and discriminate targets; or select the preferred interceptors against targets (e.g., Patriot would sometimes incorrectly select a PAC-2 GEM against a fast tactical ballistic missile or a PAC-3 interceptor against a threat aircraft).
  - There were anomalies in the Patriot PDB-8 implementation of IFF, which led to over-interrogations and indicated degradation from the previously demonstrated PDB-7 IFF capability. The Army updated the PDB-8 software to correct these problems and the fixes will be verified during IOT&E.
  - Patriot PDB-8 Training Software sometimes generated spurious alerts and improperly displayed some scripted targets.
  - The Patriot system did not meet its reliability requirements during this test.
- During Flight Test P8-2, Patriot demonstrated the capability to detect, track, engage, intercept, and kill an SRBM target with a mixed ripple method of fire using PAC-3 CRI and PAC-2 GEM-T interceptors and a second SRBM target with two PAC-2 GEM-T interceptors. In both instances, the first interceptor in the ripple intercepted and killed the target at the planned altitude, and performance of the ground system and interceptor was nominal.
- During Flight Test P8-4, Patriot demonstrated the capability to detect, track, engage, intercept, and kill an SRBM target with two PAC-3 MSE interceptors. The first PAC-3 MSE intercepted and killed the target at the planned altitude, and performance of the ground system and interceptor was nominal, although some post-intercept ground system anomalies occurred that did not affect the mission objectives.
- During Flight Test P8-3, Patriot demonstrated the capability to detect, track, engage, intercept, and kill an SRBM target with a mixed ripple method of fire using a PAC-3 MSE and a PAC-2 GEM-T interceptor. The PAC-3 MSE (the first interceptor) intercepted and killed the target at the planned altitude and both ground system and interceptor performance was generally nominal, although a Link-16 network initialization problem prevented the demonstration of Patriot PDB-8 interoperability on Link-16 during this flight test. Other parts of the Patriot PDB-8 DT&E demonstrated Link-16 interoperability.

- During Flight Test P8-1, Patriot demonstrated the capability to detect, track, engage, intercept, and kill a low-radar cross section cruise missile target at low altitude and in a clutter environment with a PAC-2 GEM-T interceptor and, following this, a maneuvering full-scale aircraft target with a PAC-3 MSE interceptor. The interceptors killed both targets at the planned ranges and altitudes, and performance of the ground system and interceptors were nominal for both engagements. Patriot demonstrated PDB-8 interoperability on Link-16 during this flight test.
- During AIAMD FT-1, Patriot demonstrated the capability to engage, intercept, and kill a low-altitude cruise missile target with a PAC-3 interceptor based on remote Sentinel radar data sent through an AIAMD Battle Command System Engagement Operations Center.
- During AIAMD FT-3, Patriot demonstrated the capability to detect, track, engage, intercept, and kill an SRBM target using a PAC-3 interceptor and a cruise missile target with the second of two PAC-2 GEM-T interceptors after the first GEM-T missed.
- The PAC-3 MSE lethality enhancer testing showed that the existing lethality model for titanium did not predict, within 10 percent of the observed critical velocities, when a high-explosive initiation of a warhead would occur. The Army used these results to develop new coefficients for their lethality model that more accurately represent the PAC-3 MSE titanium fragments.

Recommendations

- Status of Previous Recommendations. The Army satisfactorily addressed 15 of the previous 23 recommendations. The Army should continue to address the following recommendations:
  1. Conduct Patriot air and missile defense testing during joint and coalition exercises that include large numbers of different aircraft types, sensors, battle management elements, and weapons systems. Additionally, the Army should conduct Red Team Adversarial Assessments during joint exercises to test Patriot cybersecurity.
  2. Conduct a Patriot flight test against an anti-radiation missile target to validate models and simulations.
  3. Improve Patriot training to ensure that Patriot operators are prepared to use the system in combat.
  4. Have Patriot participate with live interceptors in Terminal High Altitude Area Defense (THAAD) flight testing to determine Patriot-to-THAAD interoperability and the capability for Patriot to intercept tactical ballistic missile targets that THAAD does not intercept.
  5. Collect operational reliability data on Patriot systems in the field so that the Mean Time Between Critical Mission Failure can be calculated.
  6. Use test units for future Patriot operational tests that have operationally representative distributions in soldier proficiency.
  7. Conduct future operational flight tests with unannounced target launches within extended launch windows.
  8. Improve Patriot radar reliability.
- FY16 Recommendations. The Army should:
  1. Conduct a simultaneous engagement of a cruise missile target with a PAC-2 GEM-T interceptor and a maneuvering full-scale fixed-wing aircraft target employing electronic countermeasures with a PAC-3 MSE interceptor.
  2. Have Patriot participate with live interceptors in Aegis BMD flight testing to determine Patriot-to-Aegis BMD interoperability and the capability for Patriot to intercept ballistic missile targets that Aegis BMD does not intercept.

Soldier Protection System (SPS)

Executive Summary

- The Soldier Protection System (SPS) is a suite of personal protection subsystems intended to provide equal or increased levels of protection against small-arms and fragmenting threats compared to existing personal protection equipment and at reduced weights.
- The SPS consists of four subsystems: soft armor Torso and Extremity Protection (TEP); hard armor Vital Torso Protection (VTP); the Integrated Head Protection System (IHPS); and Transition Combat Eye Protection (TCEP). Each SPS subsystem is compatible with existing personal protective equipment. The Army plans to add SPS to Deployer Equipment Bundles for issue to deploying units rather than issue SPS to individual soldiers at an Army installation.
- The Army made a Full-Rate Production decision for the TEP and a Milestone C decision for IHPS and TCEP in September 2016. The Army plans to make separate Full-Rate Production decisions for the VTP in July 2017 and IHPS in April 2018. The Army plans to make the TCEP available for unit purchase rather than to field it across the Army.
- The Army completed testing the TEP and began testing the VTP subsystem in 2016. The Army completed developmental testing of the IHPS in 2016, and awarded a low-rate initial production contract for IHPS in 2016. The Army will continue testing both the VTP and IHPS in FY17.
- Compared to the current Improved Outer Tactical Vest, the SPS TEP provides similar protection at a reduced weight against the threats tested.

System

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

- The Army initially plans to add SPS to Deployer Equipment Bundles for issue to deploying units rather than issue SPS to individual soldiers at each Army installation.

Mission

Units with soldiers wearing the SPS will accomplish assigned missions while concurrently protecting themselves against injury from a variety of ballistic (small-arms and fragmenting) threats.

Major Contractors

- TEP LRIP Vendors/Designs (Multiple vendors to stimulate competition and achieve best price through Fair Opportunity awards):
  - KDH Defense Systems INC – Eden, North Carolina (MSV, BPP)
  - Bethel Industries Inc. – Jersey City, New Jersey (MSV, BPP)
  - Hawk Protection – Pembroke Pines, Florida (MSV, BPP)
  - Short Bark Industries – Venor, Tennessee (BCS)
  - Carter Enterprises Industries Inc. –Brooklyn, New York (LDS, BCS)
  - Eagle Industries Unlimited – Virginia Beach, Virginia (BCS)
- IHPS Vendors (developmental testing awardees):
  - 3M/Ceradyne – Costa Mesa, California
  - Gentex – Simpson, Pennsylvania
  - Revision Military –Essex Junction, Vermont
- VTP LRIP Vendors:
  - BAE Systems – Chandler, Arizona (XSAPI, ESBI, XSBI)
  - 3M/Ceradyne – Costa Mesa, California (ESAPI)

Activity

- While the SPS consists of four subsystems (TEP, VTP, IHPS, and TCEP), the development, testing, and production/fielding of the four subsystems are on different timelines. The Army made a Full-Rate Production decision for TEP and a Milestone C decision for IHPS and TCEP in September 2016, and plans to make separate Full-Rate Production decisions for the VTP in July 2017 and IHPS in April 2018. The Army plans to make TCEP available for unit purchase rather than to field it across the Army. Each SPS subsystem is compatible with existing (legacy) personal protective equipment (for example, soldiers can use existing hard armor plates in the new MSV). The Army is testing SPS ballistic performance in accordance with DOT&E-approved LFT&E test plans.
- The Army completed TEP testing in July 2016, to support the TEP Full-Rate Production decision. TEP testing included:
  - IOT&E of the TEP in March 2016, at Fort Hood, Texas, to assess the impact of the TEP on soldier mobility and subsequent mission effectiveness.
  - A series of first article and sub-system level live fire testing of the TEP from January through July 2016. Sub-system level testing included testing of the MSV with currently fielded hard armor plates, and testing of the MSV/hard armor subsystem against foreign threats. Testing also included a series of blast testing events to characterize the performance of the TEP and current hard armor plates when subjected to blast events. The Army also conducted flash heat and fire threat testing to evaluate the TEP's ability to protect an individual from burns resulting from a flash fire.
  - The Army used data from first article testing to model the ability of the TEP to protect the wearer from serious injury from fragments perforating the TEP.
- The Army began VTP testing in December 2015, with first article testing of the ESAPI hard armor plates. Shortly thereafter, the Army halted further ESAPI testing because test personnel found deficiencies in the plates while conducting physical characterization of the plates prior to starting ballistic testing. Following a period of corrective action, the vendor resubmitted the ESAPI plates for first article testing, which occurred from July through August 2016. The Army conducted first article testing of the ESBI, XSBI, and XSAPI hard armor plates in May 2016. The XSAPI plate did not meet the ballistic requirements. The Army is waiting for the vendor to complete corrective actions and resubmit the XSAPI for another first article test. XSAPI resubmission is unknown at this time. The Army will continue VTP testing in FY17.
- The Army completed a third round of IHPS developmental testing in April 2016. The Army awarded a low-rate initial production contract for IHPS in September 2016. The Army will continue IHPS testing in FY17.
- The Army conducted technical and user testing of TCEP in FY16. The Army will continue TCEP testing in FY17.

Assessment

- IOT&E results indicate that some soldiers had trouble aiming their weapons when wearing the BCS and LDS with the MSV while in a prone firing position. Additionally, some female soldiers experienced restricted upper-body movement due to ill-fitting and uncomfortable BCS.
- The SPS TEP met its ballistic requirements against the threats tested.
- Compared to the currently fielded Improved Outer Tactical Vest, the SPS TEP provides similar protection at a reduced weight against the threats tested.
- Wearing body armor reduced the peak overpressure behind the armor during blast testing, but additional investigation is needed to understand how the pressure data can be analyzed and correlated to injury.
- TEP modeling required extrapolation of test data to estimate performance, which added uncertainty in evaluation of TEP performance for those conditions. The use of a broader range of fragment masses to more fully represent a threat would: provide additional test data to support future modeling efforts; make such extrapolation unnecessary; and improve confidence

in the modeling results and subsequent conclusions made about TEP performance.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The Army should:
  1. Improve the design of the LDS so it does not interfere with the wearer's ability to properly aim a weapon. The Army should also provide BCS sizes and designs that correctly fit all female soldiers and are comfortable to wear.
  2. Continue to improve its body armor blast testing and analysis procedure. Improvements should include determining whether results can be correlated to injury.
  3. Use a broader range of fragment simulators to more fully represent the expected threat environment and to then more fully characterize TEP performance.
  4. Quantify the uncertainty associated with its modeling estimates and assess the impact of that uncertainty on the evaluation of TEP performance. This should include additional end-to-end testing of an actual threat (not just representative fragments) against the actual TEP as represented in the model.

Spider Increment 1A M7E1 Network Command Munition

Executive Summary

- The Army uses Spider as a landmine alternative to satisfy the requirements outlined in the 2004 National Landmine Policy.
- Spider Increment 1A is an upgrade to the fielded Increment 1 system. The Increment 1A system has the requirement to fire anti-vehicular, obstacle-producing munitions and to operate seamlessly with mission command systems. The upgrade is backwards compatible with the Spider Increment 1 system and includes:
  - A new Remote Control Unit (RCU) with an enhanced colored map background
  - Updated software to promote ease of user operability
  - A Secure Mission Data Loader (SMDL)
  - An Interactive Electronic Training Manual (IETM)
- The Army conducted a Limited User Test (LUT) in 3QFY16. During the LUT, Spider Increment 1A demonstrated no new capability over the fielded system. Units accomplished their missions using Spider Increment 1A, but Increment 1A did not meet its reliability requirement and had cybersecurity vulnerabilities during the test.
  - Increment 1A demonstrated significant reliability problems during the LUT. The reliability threshold is 0.96 probability of having no failures during a 72-hour mission. During the LUT, the system computer achieved a 0.65 probability of completing a mission without a failure.
  - Increment 1A did produce anti-vehicular obstacles during the LUT. This capability existed with the fielded Increment 1 system, but was not previously demonstrated.
  - Increment 1A could not properly demonstrate the requirement to operate seamlessly with the classified mission command system. While it is technically possible for Increment 1A to exchange information in an unclassified environment using a surrogate mission command system, this is not operationally relevant since mission command systems must operate on a classified network. The Army is in the process of changing the seamless interoperability requirement from a threshold to an objective requirement. The Army has not yet approved the change.

System

- The Army uses Spider as a landmine alternative to satisfy the requirements outlined in the 2004 National Landmine Policy that directs the DOD to:
  - End use of persistent landmines after 2010
  - Incorporate self-destructing and self-deactivating technologies in alternatives to current persistent landmines
- The Army fielded Spider Increment 1 systems in FY09 under an Urgent Materiel Release. The system reached Initial Operational Capability in FY11 and obtained its Full Materiel Release in FY13.
- A Spider munition field includes:
  - Up to 63 Munition Control Units (MCUs), each housing up to 6 miniature grenade launchers or munition adapter modules (the modules provide remote electrical firing capabilities)
  - A remote control station, used by the operator to maintain "man-in-the-loop" control of all munitions in a field (this is the component upgraded in Increment 1A)
  - A communications relay device known as a Repeater for use in difficult terrain or at extended ranges
- Spider incorporates self-destructing and self-deactivating technologies to reduce residual risks to non combatants and has the capability to use non-lethal munitions such as the Modular Crowd Control Munition that fires rubber sting balls.

Mission

Brigade Combat Team commanders employ engineer units equipped with Spider to provide force protection and counter-mobility obstacles using lethal and non-lethal munitions. Spider functions as a stand-alone system or when combined with other obstacles to accomplish the following:

- Provide early warning
- Protect the force
- Delay and attrit enemy forces
- Shape the battlefield

Major Contractor

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

Activity

- In January 2016, the Army conducted a Cooperative Vulnerability and Penetration Assessment. This assessment identified four cybersecurity vulnerabilities.
- In March 2016, the Army conducted a System Verification Test at Fort Leonard Wood, Missouri. Multiple Software Change Requests were submitted to the contractor based on this test.
- During May 2016, the Army conducted the Spider Increment 1A LUT at the Network Integration Evaluation 16.2 at Fort Bliss, Texas, in accordance with a DOT&E-approved Test and Evaluation Master Plan (TEMP) and test plan.
- During FY16, the Army continued its contract with Northrop Grumman to refine Spider Increment 1A software.
- At the end of FY16, the Army was updating the Spider Increment 1A TEMP to support a Milestone C decision and a projected IOT&E for FY18.

Assessment

- During the LUT, Spider Increment 1A demonstrated suitability and survivability deficiencies.
  - Operational effectiveness – A trained unit can employ Spider Increment 1A as a component of a protective obstacle and provide obstacle effects as intended by the commander.
  - Suitability – The system's computer did not demonstrate its reliability requirement during the LUT. The system is required to have a 0.96 probability of completing a 72-hour mission without failures. During the LUT, 13 of 20 missions had no essential function failures, resulting in the computer demonstrating a mission success rate of 0.65.
  - Survivability – Due to cybersecurity deficiencies, Spider Increment 1A components are not survivable in an operational environment.
- Based on the Capability Development Document, Spider Increment 1A demonstrated no new capability during the FY16 LUT.
  - Spider Increment 1A could not properly demonstrate the requirement to operate seamlessly with the classified mission command system. While it is technically possible for Increment 1A to exchange information in an unclassified environment using a surrogate mission command system, this is not operationally relevant since mission command systems must operate on a classified network.
  - A cross-domain solution that could enable two-way communication between unclassified and classified systems does not currently exist. The Army was aware of this cross-domain problem prior to the LUT and did not attempt to include this functionality during the test.
  - The Army is in the process of changing the Spider Increment 1A seamless interoperability requirement. The Program Office and user representatives propose downgrading the requirement from a threshold to an objective requirement. The Army has not yet approved the change.
- Increment 1A did produce anti-vehicular obstacles during the LUT. This capability existed with the fielded Increment 1 system, but was not previously demonstrated.
- The Army did not correct all identified cybersecurity vulnerabilities prior to the LUT. The Army plans on addressing and testing all cybersecurity deficiencies prior to the IOT&E.

Recommendations

- Status of Previous Recommendations. The Army corrected Spider Increment 1 deficiencies addressed in previous recommendations.
- FY16 Recommendations. The Army should:
  1. Design the Spider Increment 1A IOT&E to enable the characterization of the system's end-to-end mission effectiveness, over the maximum operational distance, to inform the system operators of its capabilities and limitations in the various conditions that will be encountered during combat operations. These conditions should include cyber and electronic warfare.
  2. Include doctrine, tactics, and techniques on engagement area development in unit pre-IOT&E training. The maneuver unit commander should assume the responsibility to ensure leaders, soldiers, and the Spider equipped engineer unit are trained properly. Training should include a situational training exercise on collective tasks related to engagement area development augmented by an engineer unit resourced with Spider Increment 1A systems.
  3. Resolve the problem between Spider Increment 1A and the mission command system preventing Spider Increment 1A from sending digital obstacle reports to the classified mission command systems. This will allow units to know in real time where Spider fields are located on the battlefield.
  4. Prior to IOT&E:
     - Develop, fund, and implement a comprehensive reliability growth plan to correct system reliability deficiencies.
     - Demonstrate fixes to the RCU, RCU Transceiver, MCU, and Repeater reliability and communication issues through testing.
     - Develop fixes for the known cybersecurity vulnerabilities.

Warfighter Information Network – Tactical (WIN-T)

Executive Summary

- The Army Acquisition Executive (AAE) conducted a Warfighter Information Network – Tactical (WIN-T) Increment 3 decision review based upon the Network Integration Evaluation (NIE) 16.2 WIN-T Increment 3 Operational Assessment in September 2016. The DOT&E evaluation was:
  - Net Centric Waveform (NCW) satellite enhancements are operationally effective and provide improved support of mission command applications, increased bandwidth, and a stable network.
  - Network Operations (NetOps) enhancements were not operationally effective and, due to database failures, did not provide timely and accurate information to NetOps soldiers to conduct their WIN-T network mission. Some NetOps features – such as the NCW and Highband Networking Waveform (HNW) planning tools – enhanced the soldiers' ability to perform NetOps.
  - Due to complexity, the WIN-T Increment 3 tunnel-less architecture is not effective and adversely affected NetOps soldiers' planning, controlling, monitoring, and visualization functions.
  - The execution of NIE 16.2 WIN-T Increment 3 Operational Assessment was not adequate to assess operational suitability.
  - Although survivability has improved, WIN-T Increment 3 still has significant cybersecurity vulnerabilities.
- The WIN-T program took prompt action to resolve NetOps problems identified during operational test and demonstrated these fixes during a July 2016 contractor development test (CDT) conducted under benign conditions.
- In September 2016, the AAE approved the deployment of WIN-T Increment 3 NetOps and NCW enhancements.
- The Army is updating the WIN-T Increment 2 post-full-rate production Test and Evaluation Master Plan (TEMP) to include an FY17 FOT&E to test WIN-T Increment 2 configuration items designed to support light brigades with downsized, air-transportable WIN-T assemblages.

System

- The Army designed WIN-T as a three-tiered communications architecture (space, terrestrial, and airborne) to serve as the Army's high-speed and high-capacity tactical communications network.
- The Army intends WIN-T to provide reliable, secure, and seamless communications for units operating at theater level and below.
- The WIN-T program consists of three funded increments. In May 2014, the Defense Acquisition Executive approved the Army's request to stop development of the Increment 3 aerial tier of networked, airborne, communications relays and limit

M-ATV Point of Presence

M-ATV Soldier Network Extension

Stryker Point of Presence

1 - Net-Centric Waveform Antenna
2 - High-Band Networking Waveform Antenna

M-ATV - Mine Resistant Ambush Protected (MRAP) All-Terrain Vehicle (M-ATV)

Tactical Comms Node

Increment 3 to network management and satellite waveform improvements. The Army intends to increase procurement of WIN-T Increment 2 configuration items to satisfy the number of capability sets previously planned for Increment 3.

- Increment 1: "Networking At-the-Halt" enables the exchange of voice, video, data, and imagery throughout the tactical battlefield using a Ku- and Ka-satellite-based network. The Army has fielded WIN-T Increment 1 to its operational forces.
- Increment 2: "Initial Networking On-the-Move" provides command and control on-the-move down to the company level for maneuver brigades and implements an improved network security architecture.
- WIN-T Increment 2 supports on-the-move communications for commanders with the addition of the Point of Presence and the Soldier Network Extension, and provides a mobile network infrastructure with the Tactical Communications Node.
- WIN-T Increment 2 provides a downsized, air transportable variant of High Mobility Multi-purpose Wheeled Vehicle (HMMWV) mounted configuration items to support the Army's Global Response Force and other light brigades.
- Increment 3: "Full Networking On-the-Move" was to provide full mobility mission command for all Army field commanders, from theater to company level using networked airborne communication relays. With program reductions, WIN-T Increment 3 now provides enhanced NetOps and an improved satellite waveform to WIN-T Increments 1 and 2.

Mission

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

- Integrate satellite-based communications capabilities into an everything-over-Internet Protocol network to provide connectivity, while stationary, across an extended, non-linear battlefield, and at remote locations (Increment 1)
- Provide division and below maneuver commanders with mobile communications capabilities to support initial command and control on-the-move (Increment 2)

Major Contractor

General Dynamics, C4 Systems – Taunton, Massachusetts

Activity

- In October 2015, the Army conducted a WIN-T Increment 3 Government Developmental Test (GDT) of the enhanced Net-Centric Waveform 10.1.2b (NCW 10.x) at Aberdeen Proving Ground, Maryland. The GDT demonstrated that NCW 10.x could support 12 megabits per second (Mbps) throughput at the larger-dish Satellite Transportable Terminals, which support the WIN-T Increment 2 Tactical Communications Node.
- The Army conducted the final of three WIN-T Increment 3 functional qualification tests at the contractor's facility in December 2015. In the January 2016 report, the Army did not report any significant problems.
- In January and February 2016, the Army Test and Evaluation Center (ATEC) conducted an instrumentation accreditation event on the proposed instrumented data collection, reduction, and assessment (DCRA) process intended for use during the WIN-T Increment 3 Operational Assessment. The instrumentation accreditation event did not accredit the DCRA process, and ATEC continued efforts to fix DCRA problems into the NIE 16.2 WIN-T Increment 3 Operational Assessment.
- The Army conducted a WIN-T Increment 3 Operational Assessment during the May 2016 NIE16.2. The operational test employed the 2nd Brigade, 1st Armored Division conducting operationally realistic missions at Fort Bliss, Texas, and White Sands Missile Range, New Mexico. The operational assessment focused on WIN-T Increment 3 enhancements, including NetOps software tools and an enhanced NCW 10.x. Prior to the operational assessment, the Army withdrew 7 of the planned 17 NetOps features because they were not ready for test. The test was conducted in accordance with a DOT&E-approved test plan with the exception of executing adequate manual and instrumented data collection.
- In July 2016, the Army conducted a WIN-T Increment 3 CDT at the contractor's facility. The CDT was designed to demonstrate fixes for NetOps problems discovered during the WIN-T Increment 3 Operational Assessment.
- In September 2016, DOT&E published a WIN-T Increment 3 Operational Assessment report to support a WIN-T Increment 3 AAE decision review.
- In September 2016, the AAE approved the deployment of WIN-T Increment 3 NetOps and NCW enhancements.
- The Army is updating the WIN-T Increment 2 post-full-rate production TEMP to include an FY17 FOT&E to test WIN-T Increment 2 configuration items designed to support light brigades with downsized, air-transportable WIN-T assemblages.

Assessment

- The overall execution of the NIE 16.2 WIN-T Increment 3 Operational Assessment was adequate to support the assessment of operational effectiveness and survivability. It was not adequate to support the assessment of operational suitability due to problems with reliability, availability, and maintainability data collection, documentation of field service representative maintenance activities, and data instrumentation. These problems must be resolved before the next WIN-T operational test event.
- DOT&E assessed the following in the September 2016 WIN-T Increment 3 Operational Assessment report:
  - NCW 10.x enhancements are operationally effective and provide improved support of mission command applications, increased bandwidth and a stable network.
  - Overall, NetOps enhancements were not operationally effective and, due to NetOps and Security Center (NOSC) database failures, did not provide timely and accurate information to NetOps soldiers to conduct their WIN-T network mission. Some NetOps software features – such as the NCW and HNW planning tools – enhanced the soldiers' ability to perform NetOps.
  - Due to complexity, the WIN-T Increment 3 tunnel-less architecture is not effective and adversely affected planning, controlling, monitoring, and visualization at the NOSC.
  - The execution of the NIE 16.2 WIN-T Increment 3 Operational Assessment was not adequate to assess operational suitability.
  - Although survivability has improved, WIN-T Increment 3 still has significant cybersecurity vulnerabilities.
- Following the NIE16.2 WIN-T Increment 3 Operational Assessment, the program took prompt action to resolve NetOps problems identified during operational test. While the July 2016 WIN-T Increment 3 CDT is a good start, none of the tests were of sufficient length and rigor to provide validation of corrective actions.

Recommendations

- Status of Previous Recommendations. The program addressed four of six previous recommendations. They still need to conduct an operational test on WIN-T configuration items designed to support light forces, and improve the integration of WIN-T onto Stryker vehicles.
- FY16 Recommendations. The Army should:
  1. Correct problems with data instrumentation and manual data collection prior to the next WIN-T operational test.
  2. Improve WIN-T cybersecurity and assess its survivability in a future operational test.
  3. Conduct further testing on WIN-T Increment 3 NetOps fixes and validate corrections in a future operational test.
  4. Conduct an operational test to assess WIN-T Increment 2 configuration items designed to support light forces.
  5. Improve Stryker WIN-T integration and demonstrate these improvements in a future operational test.