Information Assurance (IA) and Interoperability (IOP) Evaluations

SUMMARY

Assessments in FY09 were performed during 25 Combatant Command and Service exercises, with the following observations:

- Approximately 75 percent of the fielded systems observed do not have current interoperability certifications. Additionally, interoperability among mission-critical systems is less than expected for certified and previously tested systems. Manual means and overrides are used to ensure the timely and accurate exchange of critical operational information. Data incompatibility among fielded systems continues to inhibit efficient exchange of intelligence as well as command and control information.
- DoD has improved awareness and preparations to meet the growing threats to military information systems and networks. Nonetheless, the ability of DoD to protect critical information, detect intrusions and exploitations, and rapidly react and restore capabilities continues to be challenged by the capabilities of potential adversaries.
- Several major Combatant Commander exercises incorporated more realistic depictions of network adversary tactics and activities; however, many of the effects are simulated or examined in pre/post-exercise table top events. While this approach can support exercise-training objectives, it does not provide the data collection opportunity to support system assessment. A majority of the exercises conducted do not realistically portray the array of cyber threats facing DoD networks. As a result, exercise assessment results may provide a more optimistic portrait of DoD network readiness than may actually exist. The Secretary of Defense (SECDEF) guidance to plan for, implement, and regularly exercise the capability to fight through cyber/kinetic attacks that degrade the Global Information Grid has not yet been fully implemented.
- The majority of vulnerabilities and network security shortfalls observed in both exercise and acquisition system assessments continue to be basic in nature and easily remedied by qualified local personnel. Across assessed organizations, network-defender manning and training has improved slightly, but manning remains well below the level of comparable industry networks.
- Commercially available anti-virus and security-management tools have improved the security of military operations where fielded, but implementation of these tools remains incomplete, and a number of systems/networks remain at risk. Effectively restricting use of network resources to authenticated users, and detecting unauthorized and unauthenticated use of information systems remain challenges.
- Process improvements for FY09 included the following:
  - DOT&E developed updated standards and guidance for exercise assessments to enhance the analytical rigor, consistency, and focus on interoperability of those assessments.
  - DOT&E and Joint Forces Command (JFCOM) have formed a partnership for enhanced interoperability assessments that focus on specific systems identified by Service representatives that are critical for mission accomplishment.
  - DOT&E issued revised procedures for Information Assurance (IA) evaluations during Operational Test and Evaluation (OT&E) events, with added emphasis on attack detection, reaction, and system restoration capabilities.
  - DOT&E and the Under Secretary of Defense (AT&L) have undertaken a combined effort to better integrate IA testing and evaluation across the developmental and operational testing continuum.

PROCESS

DOT&E oversees the execution of the IA and Interoperability (IOP) assessment program. Participating Service and Agency teams perform the assessments and assist the Combatant Commands (COCOMs) and Services in designing the exercise scenario in which the assessments take place. DOT&E aggregates and analyzes assessment data to provide feedback to the Military Services and DoD agencies.

Interoperability assessments include the following phases:

- Review and Coordination – Identify known or suspected interoperability problems, key systems that support the Commanders Critical Information Requirements (CCIRs), or systems and mission threads that support the Joint Forces Command Optimum Capability Mix goals.
- Research and Planning – Research identified systems and mission threads; identify best assessment venue to acquire needed interoperability data; and develop a detailed assessment plan that details how the required data will be captured, analyzed, and reported.
- Execution and Analysis – Collect exercise assessment data and analyze (including post-exercise reconstruction, where available) to document interoperability successes and shortfalls.

The IA assessment process includes the following:

- Review and Coordination – Identify known and suspected IA problems or key systems and mission threads that support the CCIRs. Review appropriate threat assessments and identify

the appropriate level of threat portrayal and Blue and Red Team support requirements.
- Research and Planning – Research identified systems and mission threads and develop a detailed assessment plan that details how the required data will be captured, analyzed, and reported.
- Blue Team Vulnerability Assessment – Perform technical and non-technical assessments, including scans and surveys of networks, network personnel, and network policies and practices.
- Green Team Remediation and Mitigation Support – Assist the Exercise Authority in interpreting the results of an assessment, addressing shortfalls, and coordinating remediation and training, as required.
- Red Team Penetration and Exploitation Assessment – Perform live network assessments via penetration testing and other activities as part of the exercise scenario, and in support of the exercise opposition force.
- Analysis – Collect all data and analyze (aggregating Blue, Green, and Red Team results) to document IA successes and shortfalls.

FY09 ACTIVITY

DOT&E remains partnered with the Joint Staff and the Assistant Secretary of Defense for Networks, Information, and Integration (ASD(NII)) in the oversight and coordination of the IA/IOP assessment program. DOT&E has expanded the reporting process to ensure significant findings are reported to Service acquisition authorities, Service Chief Information Officers, and specific program offices, where appropriate, for investigation and resolution.

To improve assessment rigor, this year the IA and IOP assessment program performed the following activities:

General

- Continued the development, validation, and implementation of a standardized set of IA and IOP metrics and analytical methods that quantify operational performance attributes and outcomes. These metrics are closely linked with other efforts within DoD to quantify and evaluate IA and IOP effectiveness, determine return on investment, and identify areas for improvement. New measurement areas include adversary level-of-effort metrics, direct outcome metrics, and personnel training demographics. DOT&E issued guidance in FY09 to increase the emphasis on threat realism, more rigorous data collection, and analytical requirements.
- Developed an IA & IOP Assessment Database that will provide program analysts with a secure, automated, and standardized source of exercise results. The database will support queries and analyses, and produce automated displays and reports.
- Examined a number of "prototype" IA and IOP metrics and methods of measurement during assessment events. These efforts allowed the experimental use of new measures and techniques in order to evaluate not only the networks and systems in question, but evaluate the assessment process for improvements and enhanced practices.
- The JFCOM led development of a net-enabled Universal Joint Task List (UJTL) will provide a mission context for the interoperability and information assurance findings. DOT&E is incorporating the net-enabled UJTL construct in both OT&E and fielded system assessments.

Interoperability

- Partnered with U.S. Joint Forces Command (JFCOM) for enhanced interoperability assessments that focus on Optimum Capability Mix systems identified by Service leadership that are critical for mission accomplishment. This partnership will be leveraged to enhance assessments during FY10 and beyond, by ensuring realistic C4ISR functionality and appropriate levels of threat portrayal are included for these assessments. By working collaboratively with the JFCOM Joint Systems Interoperability Integration Laboratory, there is an opportunity to provide additional technical rigor to understand problems seen in the field exercises.

Information Assurance

- Expanded the set of core IA compliance measures from 32 to 46 to more fully represent requirements for detection and restoration, in addition to protection and reaction activities. These core measures were also supplemented by a set of specific interoperability measurements, both technical and operational, to permit more accurate measurement of system performance and interoperation in mission contexts.
- Sponsored Defense Intelligence Agency development of cyber threat support documents to guide the realistic portrayal of network threats during COCOM and Service exercises, and worked with the National Security Agency (NSA) and other DoD Red Teams to enhance their tools and techniques to more realistically portray nation-state level threats during exercise assessments.

FY09 ASSESSMENT ACTIVITIES

In FY09, the assessing organizations performed 25 assessments. These included 17 COCOM and eight Service exercise assessments (Table 1). Five of these assessments involved units preparing to deploy (or already deployed) to Iraq and Afghanistan.

DOT&E revised the IA policy for acquisition programs. The policy was updated through a "Lean Six Sigma" process with an emphasis on assessment procedures of attack detection, reaction, and restoration in addition to the long-standing protection focus. A number of programs, including T-AKE, LPD-17, Ship Self-Defense System, Global Hawk, Palladin PIM, F-15E, Integrated Air and Missile Defense, Patriot PAC-3, Mobile User Objective System, Distributed Common Ground Station-Army, Net-Enabled Command Capability, CVN-78, C-5 Reliability Enhancement and Re-engining Program, MQ-9, and SM-6 have begun to implement these new procedures in their OT&E planning.

Interoperability assessments are becoming more effective at identifying problems. Two interoperability assessments

conducted during the latter part of FY09 had a greater operational context and interoperability focus than most of the others, signaling progress toward achieving more realistic and robust interoperability assessments as we move into FY10. One of these assessments focused on achieving real-time sharing of track data among a large number of Command, Control, and Communication systems that support Carrier Strike Group operations. Another focused on achieving information sharing among multiple information systems for intelligence support within a Joint Task Force Service Headquarters.

DOT&E continued the practice of providing classified Finding Memoranda to cognizant Service and Agency senior leadership in FY09. Finding Memoranda detail specific problems identified during one or more assessment exercises that have the potential to negatively impact warfighter operations. In three identified systems, assessors identified a total of six specific issues. To date, two of these issues have been fully resolved and four are partially resolved or mitigated until complete resolution can be accomplished.

ASSESSMENT

Interoperability

In focused assessments of 10 systems, six demonstrated less than full compatibility with other key systems, resulting in data loss, required manual intervention, false alerts and presentations, and reduced speed of information exchange. Often these interoperability problems are remediated with local workarounds; however, the latter are generally not well documented or consistent across DoD networks, and may further exacerbate interoperability problems. Issues caused by the implementation of local solutions generally go unrecorded, including the level of effort required to accomplish the workarounds. Interoperability certification rates continue to be low for assessed systems. Approximately 75 percent of the fielded systems encountered during assessments do not have current interoperability certifications.

Information Assurance

Following several network security incidents in early FY09, DoD undertook aggressive actions that have significantly improved the awareness of – and defenses against – threats to U.S. military information systems and networks. The new policies, procedures, and systems that were rapidly introduced have reduced, in part, the gap between potential adversary actions and demonstrated defensive capabilities. In spite of these improvements, most DoD networks remain insufficiently manned, trained, or equipped to consistently preclude or detect network intrusions during assessed Red Team events. This shortfall increases risk to mission accomplishment.

Assessments of IA in fielded exercises are limited by security considerations and competing objectives that must be met by exercise planners. These constraints can lead participants to a false sense of security. Some exercise authorities adopted exercise structures in FY09 that synchronize the network Red Teams more closely with the exercise opposition force, allowing for more realistic adversary portrayals. Others are seeking new approaches to ensure that warfighters are prepared to successfully operate in realistic threat environments with degraded systems. However, SECDEF guidance to plan for, implement, and regularly exercise the capability to fight through cyber/kinetic attacks that degrade the Global Information Grid still needs to be fully implemented. In FY10, DOT&E, in concert with the Defense Intelligence Agency, will include an evaluation of the level of threat actually portrayed during assessment events, relative to the anticipated threat.

While some improvement in both protection and detection has been seen where new systems and processes have been fully implemented, none of these have been tested to the full level of the anticipated adversary capabilities. Also, Red Teams have reported some improvement in the ability of networks and network personnel to resist short-duration intrusion threats; but long-duration intrusion efforts continue to succeed. Therefore, any noted improvement must be tempered with the fact that the threats presented during these exercises generally fall well below what might be expected from a top-tier nation-state in both capability and duration.

The three most prevalent weaknesses exploited during assessments continue to be: (a) basic compliance with configuration standards, (b) inadequate response to abnormal network activity, and (c) physical security of critical network infrastructure. Assessors continue to find most vulnerabilities are basic in nature, and easily remedied by local personnel, given adequate skills and training, but many organizations lack a full complement of trained personnel, and this remains one root cause in all three issues. In the majority of assessments, penetration testing does not examine the full range of compliance-related vulnerabilities, does not test the full skill range of network operators, and does not aggressively assess physical security.

Collaboration suites, and particularly commercial products designed for other (e.g. conferencing and tele-education) purposes have appeared to improve warfighter interoperability and operational interaction, but often at the expense of introducing network vulnerabilities that are either inherent to the commercial product design or unexpected consequences of user utilizations. Additionally, the life cycle of some commercial products upon which DoD-developed tools depend, has presented challenges where those products have expired or are no longer actively maintained commercially. During FY09 exercise assessments, critical command and control systems were identified as dependent on expiring software operating systems, and one commercial collaboration tool was identified to have a number of inherent vulnerabilities easily induced by inadvertent user actions. In each case, DOT&E identified these issues to the cognizant Service/Agency, resulting in the following rapid resolutions and / or mitigations:

- Stronger network protocols for authentication of system users
- Revised system requirements and procurement/fielding plans
- Upgraded system architectures and components

- Accelerated migration to updated and fully supported software baselines

General exercise assessment trends and findings include the following:

General

- Configuration. Software inventories are assessed as having improved in control and documentation, but hardware configuration controls have not significantly improved. Use of configuration specifications and compliance with configuration standards is assessed as "improved overall." Compliance with port and protocol policies has improved, but is still assessed as satisfactory in only four out of every five assessments.
- Personnel and Training. Manpower requirements for new systems and applications generally do not address additional network support personnel requirements. Some improvement has been seen in the overall expertise levels of network personnel managing COCOM networks during exercises, and user/manager training has increased in frequency overall. The frequency of drills and security exercises remains low, and few commands have viable disaster recovery plans or continuity plans for network operations.

Interoperability

- Techniques and Processes. Operator actions required to manage the exchange of situational awareness information are labor-intensive (e.g., the multi-step manual process necessary to reduce redundant track reporting), and can result in a less than complete or common tactical/operational picture.

Information Assurance

- Intrusions Rates. Red Teams report that penetration of warfighter networks has become more challenging at some sites, but intrusion success rates overall remain high. Long-duration, stealthy intrusion efforts succeed more often than the short-duration attempts most often permitted during exercise scenarios. Few long-duration intrusions are detected. Some improvement has been seen in the detection of short-duration intrusion attempts. In some short-duration scenarios, the Red Teams have been unable to establish an intrusion on the target network, but over time have been able to develop and exploit network weaknesses and successfully intrude. Incident response plans are assessed as improved overall, but effective incident management (response implementation) remains only modestly improved.
- Boundary Defenses. Significant improvement has been seen in reducing vulnerabilities of enclave protection, including control and authentication of users, and configuration/control of network devices. Virus protection was found to be satisfactory at all sites assessed in FY09. Control and compliance of wireless devices is also improved. Correct use and review of audit logs improved substantially in FY09, but still remains low.
- Credentials and Authentication. Common Access Card (CAC)-enabled applications are less vulnerable to compromise and intrusion. Combined use of CAC and upgraded passwords significantly reduce intrusion opportunities. Lack of token-based authentication on classified networks has been seen to permit hard-to-detect exploitation of otherwise protected systems.
- Automated Management Tools. The majority of military information networks and systems are regularly scanned for vulnerabilities. Automated tools for identification and analysis of abnormal activities through audit and correlation are not generally available but are under development by DoD. The recent introduction of an enterprise host-based security suite for DoD has been observed to improve network defenses and detection capabilities, but only after extensive "tuning" of the system and training of the operators.

Exercise assessments and OT&E continue to identify shortcomings in both the information assurance and interoperability of fielded systems. System limitations may compel users to choose between interoperability and network security. Local solutions to IA and IOP shortfalls that are inconsistent with other enterprise efforts often exacerbate the problem. The full implications of a system's use need to be clearly understood before a decision is made to employ it in an operational network. The risk to operational success increases when network administrators and defenders lack the tools and training to rapidly detect, assess, and respond to network exploitations or attacks.

FY10 GOALS AND PLANNED ASSESSMENT ACTIVITIES

DOT&E has identified 23 COCOM and Service exercises for assessment in FY10, with the goal of performing at least one IOP and one IA assessment at each COCOM and Service during the fiscal year. Table 2 lists the planned assessments. Three of the exercises will be for units preparing for deployment to Iraq and Afghanistan. The FY10 assessments will focus on the following:

- Increasing the rigor of IOP and IA assessments to be more operationally realistic and threat representative, and examining mission assurance under degraded network conditions.
- Identifying and tracking IA and IOP problems found in OT&E; preparing and executing exercise assessments that examine current status of problems and/or solutions.
- Executing assessments in accordance with priorities identified by the DOT&E and JFCOM partnership for the Optimum Capability Mix.
- Transmitting critical findings to Service and DoD leadership for their awareness and remediation, as appropriate.

TABLE 1. INFORMATION ASSURANCE AND INTEROPERABILITY EXERCISE EVENTS IN FY09

Exercise Authority	Exercise	Lead OTA	Support OTA
AFRICOM	Judicious Response 09	ATEC	
CENTCOM	Internal Look 09	ATEC	
	CJTF-101	ATEC	
	NAVCENT	ATEC	
EUCOM	Austere Challenge 09	ATEC	JITC, AFIOC
	Jackal Stone 09	ATEC	
JFCOM	Empire Challenge 09	JITC	
NORAD/NORTHCOM	Ardent Sentry 09	AFIOC	JITC, MCOTEA
	Vigilant Shield 09	AFIOC	MCOTEA, JITC
PACOM	Talisman Saver 09	ATEC	MCOTEA
	Terminal Fury 09	ATEC	MCOTEA
SOUTHCOM	HQ Assessment	ATEC	
STRATCOM	Global Lightning/Bulwark Defender 09	JITC	COTF, MCOTEA, AFIOC
	Global Thunder 09	JITC	
TRANSCOM	Turbo Challenge 09	JITC	
USFK	Key Resolve 09	ATEC	
USA	UE-09-1-III (25 ID)	ATEC	
	UE-09-1-V (I Corps & 1st Cav.)	ATEC	JITC
	UE-09-3-IV	ATEC	
	UE-09-3-V	ATEC	
USN	JTFEX-09-4	COTF	
	JTFEX-09-5	COTF	JITC
USAF	Black Demon 09	AFIOC	
USMC	UE-09-1-IV (II MEF)	USMC	JITC
Other	CWID	JITC	COTF, MCOTEA

AFIOC – Air Force Information Operations Center
AFRICOM – African Command
ATEC – Army Test and Evaluation Command
CENTCOM – Central Command
CJTF – Combined Joint Task Force
COTF – Commander, Operational Test and Evaluation Task Force
CWID – Coalition Warrior Interoperability Demonstration
EUCOM – European Command
HQ – Headquarters
JFCOM – Joint Forces Command
JITC – Joint Interoperability Test Command
JTFEX – Joint Task Force Exercise
MCOTEA – Marine Corps Operational Test and Evaluation Activity
MEF – Marine Expeditionary Force
NAVCENT – Navy, CENTCOM
NORAD – North American Defense Command
NORTHCOM – Northern Command
PACOM – Pacific Command
SOUTHCOM – Southern Command
STRATCOM – Strategic Command
TRANSCOM – Transportation Command
UE – Unified Endeavor
USFK – U.S. Forces, Korea
USA – U.S. Army
USN – U.S. Navy
USAF – U.S. Air Force
USMC – U.S. Marine Corps

TABLE 2. PLANNED IA AND INTEROPERABILITY EXERCISE EVENTS FOR FY10

Exercise Authority	Exercise	Lead OTA	Support OTA
AFRICOM	Judicious Response 10	ATEC	
	JTF Horn of Africa 10	ATEC	
CENTCOM	Internal Look 10	ATEC	
	AOR Site Assessment #1	ATEC	
EUCOM	Austere Challenge 10	ATEC	
JFCOM	Unified Endeavor 10-1	JITC	
	Angel Thunder	JITC	24th Air Force
NORTHCOM	Ardent Sentry 10	24th Air Force	JITC, MCOTEA
PACOM	Terminal Fury 10	COTF	ATEC, JITC, MCOTEA
SOCOM	Able Warrior 10	ATEC	
SOUTHCOM	Direct Report Unit Assessment #1	ATEC	
	Direct Report Unit Assessment #2	ATEC	
STRATCOM	Global Lightning/Bulwark Defender 10	JITC	24th Air Force
	Global Thunder 10	JITC	24th Air Force, COTF
TRANSCOM	Turbo Distribution 10	JITC	
USFK	Key Resolve 10	ATEC	
USA	Unified Endeavor 10-1 MRX	ATEC	
	Unified Endeavor 11-1 MRX	ATEC	
USN	Joint Task Force Exercise 10 (LANT)	COTF	
	Joint Task Force Exercise 10 (PAC)	COTF	MCOTEA
USAF	Black Demon/Blue Flag 10	24th Air Force	JITC
USMC	I MEF MRX	MCOTEA	JITC
Other	CWID		24th Air Force,

AFRICOM – African Command
ATEC – Army Test and Evaluation Command
CENTCOM – Central Command
COTF – Commander, Operational Test and Evaluation Task Force
CWID – Coalition Warrior Interoperability Demonstration
EUCOM – European Command
JFCOM – Joint Forces Command
JITC – Joint Interoperability Test Command
MCOTEA – Marine Corps Operational Test and Evaluation Activity
MEF – Marine Expeditionary Force
MRX – Mission Rehearsal Exercise
NORTHCOM – Northern Command
PACOM – Pacific Command
SOUTHCOM – Southern Command
STRATCOM – Strategic Command
TRANSCOM – Transportation Command
UE – Unified Endeavor
USFK – U.S. Forces, Korea
USA – U.S. Army
USN – U.S. Navy
USAF – U.S. Air Force
USMC – U.S. Marine Corps