Information Assurance (IA) and Interoperability (IOP) Evaluations

Summary

- DoD continues to improve the Information Assurance (IA) and Interoperability (IOP) postures of warfighter networks, but the threat to these networks continues to grow significantly.
- Operational assessments of IA/IOP during Combatant Command (COCOM) and Service exercises promote identification and resolution of problems that could impact warfighter mission accomplishment. These assessments have also contributed to improved methods and metrics for assessing IA/IOP during both exercises and acquisition OT&E.
- A full assessment cycle of Blue, Green, and Red teaming provides the most comprehensive assessments and the greatest opportunity to improve IA/IOP postures for assessed units.
- Many of the vulnerabilities and network weaknesses identified in these assessments are fundamental problems for which solutions are readily available. Some problems require more extensive enterprise solutions.
- Exercise authorities appreciate and desire more OT&E expertise during their exercise planning, execution, and assessment phases. There has been more senior-leadership emphasis on IA during most exercises this fiscal year resulting in improved IA performance, but more acceptance of aggressive Red Teaming is needed.
- Assessments and remediation efforts in support of units deploying to Iraq and Afghanistan were tailored by the Operational Test Agencies (OTAs) and conducted during three exercises this fiscal year. Four assessments with deploying units are planned for FY07.
- Coordination across DoD organizations that assess IA and IOP is leading to improved metrics and common standards for the assessment of IA and IOP readiness and investments.
- The IOP assessment methods, which have lagged the IA methods, are maturing. The remediation process for identified IOP problems remains less effective than the Enterprise Solutions Steering Group effort for IA.

Background

The FY03 Appropriations bill directed that the COCOMs and Services conduct operationally realistic IA and IOP evaluations during major exercises. The bill directed the Service OTAs, the Service Information Warfare Centers, and the National Security Agency (NSA) to assist in the planning, conduct, and evaluation of these exercises. DOT&E oversees these efforts and provides annual updates on DoD's progress based on results of the exercise evaluations and acquisition OT&E.

The bulk of the FY06 IA/IOP funds were distributed to the OTAs, who in turn assembled teams with the proper expertise to perform IA and IOP assessments before and during exercises. These teams plan, execute, collect data, analyze, and report the results of all activities associated with IA and IOP assessments. Primary execution elements include:

- Blue Teams -- Perform network scans and surveys of network personnel and policy.
- Green Teams -- Assist the exercise authority in understanding the nature, priority, and remedial activities needed for identified vulnerabilities. They also provide remediation support and training.
- Red Teams -- Design and execute a comprehensive Red Team scenario overlaid on an exercise scenario to examine the performance of blue networks and operators when subjected to information operations attacks.

FY06 Assessment Activities

The OTA teams that lead the IA/IOP assessments continued to build relationships with the COCOMs and other critical partner organizations, such as the Services' Information Warfare Centers (IWCs), the NSA, the Defense Intelligence Agency (DIA), the Defense Information Systems Agency (DISA), and the Joint Task Force – Global Network Operations (JTF-GNO). The OTA teams and their support elements were included in the Information Operations (IO) Cells that the COCOMs used to plan and conduct each exercise.

In order to expedite enterprise-wide solutions to enterprise-wide issues, the results of IA assessments are analyzed and identified trends are documented and briefed to the cognizant agencies, including the Joint Staff (JCSJ6X), the DoD Chief Information Officer (CIO)-Defense Information Assurance Program (DIAP), the National Security Agency Global Information Grid IA Portfolio Office, and specific Service CIOs and program offices, as required. Principal amongst the groups taking action on these issues is the DISA/DIAP/U.S. Strategic Command-sponsored Enterprise Solutions Steering Group (ESSG). This group is directly responsible for the rapid fielding of DoD Enterprise scanning and remediation tools, host-based security tools, network sensors, and other tools within the last year. Trends, as well as specific program issues, are briefed to the ESSG who then procures solutions. The IA/IOP assessment teams assess those solutions after fielding. In addition, under the leadership of the ESSG and the Joint Staff, a DoD-wide effort to standardize IA metrics and establish a common framework for network performance evaluation is underway with full participation from the IA assessment teams. Similar lines of feedback and communication are in development to address interoperability issues, although no central action group similar to the ESSG currently exists for IOP shortfalls.

Although a variety of methods for managing vulnerabilities and shortfalls exists within DoD, DOT&E has instituted the use of a Vulnerability and Shortfall Matrix (VSM). This matrix identifies the vulnerability or interoperability shortfall, proposes a remedy, and includes a statement of the operational impact if remedies are not applied. The matrix is updated following every Blue, Green, or Red Team assessment to reflect the current state of observed vulnerabilities and shortfalls. This tool is used to monitor correction of vulnerabilities and shortfalls, support trend analyses across theaters, and assist in the identification of issues to be reviewed or validated in subsequent events. Several COCOMs have chosen to employ this matrix as their own tracking tool.

During selected exercises, the Red Teams deployed special units to test the physical security of protected facilities, in addition to the network attacks that are routinely performed. These combined attacks along multiple axes provide a more realistic threat portrayal in which to assess the IA posture of the exercise unit. The following summarizes accomplishments by the assessment teams during FY06:

- Performed IA assessments during 11 COCOM, 1 Joint Staff, and 3 Service exercises (see Table 1)
- Performed full Blue, Green, and Red Team assessments for 11 exercises
- Performed three assessments for units preparing to deploy to Iraq and Afghanistan
- Developed a VSM for all IA assessments to consolidate vulnerabilities, identify remedies, and track resolution for the COCOMs; the OTAs disseminated the VSMs to COCOM and Service commanders and network personnel after completion of the IA assessments, providing a ready guide for establishing priorities and performing remediation
- Coordinated with U.S. Special Operations Command (SOCOM) and Central Command (CENTCOM) for IA assessment support during future SOCOM and CENTCOM exercises; with the addition of these exercise events, all COCOMs will be involved in the IA and IOP assessment program

The IA and IOP assessment effort made the following improvements to the planning, assessment, and reporting method during this fiscal year:

- Identified a master list of core IA preparedness metrics that are observable in the exercise environment and suitable for performing baseline assessments and trend analyses
- Identified operational metrics for exploration by assessment teams to enhance the characterization of IA posture with metrics more meaningful to warfighters
- Improved common methods and reduced differences among OTAs in terminology, processes, and depiction of assessment results

Table 1 - Information Assurance and Interoperability Exercise Events in FY06

Exercise Authority	Exercise	Lead OTA	Support OTA
Joint Staff	Bulwark Defender 06	JITC	ATEC, AFOTEC, MCOTEA, COTF
CENTCOM	*No exercises this FY*		
EUCOM	Flexible Response 06	ATEC	AFOTEC, MCOTEA
	Coalition Warrior Interoperability Demo	JITC	MCOTEA, COTF
JFCOM	Unified Endeavor 06-1*	JITC	ATEC, MCOTEA
	Unified Endeavor 06-2*	JITC	MCOTEA
PACOM	Terminal Fury 06	COTF	JITC, ATEC, AFOTEC, MCOTEA
	Reception, Staging, Onward-movement, and Integration 06	COTF	ATEC
SOUTHCOM	Blue Advance 06	ATEC	None
	Fuertas Defensas 06 Joint Task Force Guantanamo 06	ATEC	None
SOCOM	*No exercises this FY*		
TRANSCOM	Turbo Distribution 06	JITC	AFOTEC, MCOTEA
STRATCOM	Global Lightning/Global Shield 06	JITC	AFOTEC, MCOTEA, COTF
NORTHCOM	Ardent Sentry 06	AFOTEC	None
Services	I Marine Expeditionary Force Exercise 06*	MCOTEA	None
	Joint Task Force Exercise 06-2	COTF	None
	Cobra Gold 06	ATEC	None

*Pre-deployment assessment events in FY06.

CENTCOM – Central Command
EUCOM – European Command
JFCOM – Joint Forces Command
NORTHCOM – Northern Command
PACOM – Pacific Command
SOUTHCOM – Southern Command
SOCOM – Special Operations Command
STRATCOM – Strategic Command
TRANSCOM – Transportation Command
ATEC – Army Test and Evaluation Command
AFOTEC – Air Force Operational Test and Evaluation Center
COTF – Commander, Operational Test and Evaluation Force
JITC – Joint Interoperability Test Command
MCOTEA – Marine Corps Operational Test and Evaluation Activity

DOT&E increased the focus on IA as an evaluation issue for systems on the OT&E oversight list. DOT&E identified a dozen acquisition programs in FY06 that required an expanded review of the adequacy of IA evaluation planning to confirm appropriate IA OT&E metrics were in use. This effort included review of Test and Evaluation Master Plans, test plans, and Defense Information Technology Security Certification and Accreditation Process documentation. The OTAs are performing similar efforts on selected acquisition programs. Efforts to heighten IA awareness in acquisition program planning will continue in FY07.

The DOT&E policy for IA evaluations implemented in 1999 remains in effect. An update is in final coordination. The update incorporates new metrics and lessons learned from this initiative that are appropriate for acquisition OT&E, while maintaining compatibility with DoD policies for IA and IOP.

Assessment

Although DoD has made progress in improving IA/IOP for warfighter networks, assessment teams continue to find shortfalls relating to personnel and training, configuration management, network Continuity of Operation (COOP) and recovery, firewalls and intrusion detection systems, and physical security. Trends across FY06 events include the following:

- Vulnerabilities have been found by every Blue and Red Team
- Most problems found are basic (e.g., unprotected servers and open ports, Intrusion Detection Systems not installed or improperly configured, etc.) and easily remedied by trained system administrators
- Improved emphasis on IA existed within all commands; some local practices and innovations have taken place which have resulted, through the process of assessment feedback, in overall improvements to policies and configurations within the entire DoD community
- Network COOP plans need to be improved; network COOP plans should be stressed to exercise "react" and "restore" processes and provide insights into the potential operational impacts of cyber attacks on mission accomplishment
- Additional effort and resources are needed to remedy COCOM IA/IOP deficiencies and to establish an enterprise interoperability solutions program

Specific trends in more detailed assessment areas include the following:

- **Personnel and Training.** No standard manning policies exist that account for network complexity, operational requirements, and joint integrated operations, often resulting in reliance upon un-trained or un-designated personnel. DoD IA training standards have been revised to improve the quality of training available and take advantage of commercial certification standards known to be effective. Joint and organizational training has improved through the introduction of more in-depth joint training events.
- **Configuration Management and Interoperability.** Most networks are equipped with basic security controls, but standards remain complex and difficult to implement, resulting in inconsistent execution. New technologies continue to complicate enforcement of configuration standards. Wide use of collaborative tools, as well as rapid integration of applications, frequently leads to new operational capabilities that have not been tested or certified. DoD has invested in improved network sensors, scanning and remediation tools, and configuration management tools.
- **Physical Security.** Exercise opposition forces continue to penetrate existing physical perimeter safeguards, either due to inadequacy or lack of compliance with procedures. Valuable information remains vulnerable to exploitation of security practices, printed material handling, and general physical protection of network components, often leading to network compromise. Incorporation of assessment findings into Operational Security (OPSEC) planning is being addressed by DoD.
- **Policy Compliance.** Most commands do not possess complete documentation and policies for installed networks. Few commands have COOP and Recovery Plans or have not exercised them. Many classified networks, already protected by cryptographic barriers, lack basic network security tools. Continued challenges with Information Assurance Vulnerability Advisory compliance and expanded use of internal trusted networking increase the risk of compromise, while reducing the likelihood of intruder detection. Improved configuration management tools within DoD will partially address this issue, as will the ongoing development of Network COOP and recovery standards.

FY07 Goals and Planned Assessment Activities

The response from COCOM and Service exercise authorities continues to be very positive. Assessment plans for FY07 include 15 exercises with active Blue, Green, and Red Teams (full assessment support) and 6 additional exercises with lesser efforts (see Table 2). Fourteen of these exercises will include an interoperability assessment. Assessment and remediation support to units preparing to deploy to Iraq and Afghanistan will continue as a priority effort, and four of these assessment events are planned for FY07 (these events are designated with an asterisk in Table 2). Assessment resources will be stretched to the limit in FY07 and mission growth has been curtailed in order to execute the above assessments to an appropriate standard.

The following are specific areas of emphasis for FY07:

- Inclusion of IA as a training objective with the full range of threat-representative Red Team actions during COCOM and Service exercises
- Additional training on mission-oriented operational concepts of operations, processes, and information flows for IA and IOP assessment planners; data collectors and observers; and analysts
- Systematic and mission-oriented IOP assessments during at least one exercise in each COCOM
- Evaluation of network COOP preparation, testing, and effectiveness to determine the capability to recover mission critical network systems, data, and support services

Acquisition program support will continue to expand during FY07 and DOT&E plans to begin integrating IA and IOP problems identified during acquisition OT&E into the IA/IOP VSM. This information will assist in preparing for and executing assessments by knowing where problems may be expected and where new software or procedures may be introduced to remedy those problems. In coordination with the Joint Staff, DOT&E intends to track the delivery and adequacy of solutions promised by program managers at milestone decisions when capabilities are fielded with known deficiencies. Although this mission is traditionally performed via dedicated follow-on operational test and evaluation for major programs, many software upgrades are introduced into the operational forces without an operational test to confirm desired capabilities have indeed been delivered. DOT&E believes that COCOM and Service exercises can provide a venue where training and follow-on test objectives can be simultaneously satisfied, with ensuing cost savings to the DoD.

Table 2 – Planned Information Assurance and Interoperability Exercise Events for FY07

Exercise Authority	Exercise	Lead OTA	Support OTA
Joint Staff	Bulwark Defender 07	JITC	ATEC, AFOTEC, MCOTEA
CENTCOM	Bright Star 08 Planning	ATEC	None
JFCOM	Unified Endeavor 07-1*	JITC	ATEC, MCOTEA
	Unified Endeavor 07-2*	JITC	ATEC, MCOTEA
	Unified Endeavor 07-3*	JITC	ATEC
EUCOM	Sharp Focus 07	ATEC	None
	Flexible Leader 07	ATEC	None
	Coalition Warrior Interoperability Demo 07	JITC	MCOTEA, COTF
Service	Joint Task Force Exercise 07	COTF	None
	II Marine Expeditionary Force Exercise*	MCOTEA	None
	Federation of Systems 07	MCOTEA	None
NORTHCOM	Vigilant Shield 07	AFOTEC	JITC, MCOTEA
	Ardent Sentry/Northern Edge 07	AFOTEC	JITC, MCOTEA
PACOM	Terminal Fury 07	COTF	JITC, ATEC, AFOTEC, MCOTEA
	Reception, Staging, Onward-movement, and Integration 07	COTF	ATEC, MCOTEA, JITC
	Talisman Saber 07	COTF	MCOTEA
SOUTHCOM	Blue Advance 07	ATEC	None
	Fuertas Defensas 07	ATEC	None
SOCOM	Able Warrior 07-1	MCOTEA	None
STRATCOM	Global Lightning 07	JITC	MCOTEA
TRANSCOM	Turbo Challenge 07	JITC	MCOTEA

*Pre-deployment assessment events planned for FY07

Recommendations

- Status of Previous Recommendations. The DoD has taken action on DOT&E's FY05 recommendations. However, more action is needed to create representative threat environments in which full operational assessments of IA can be performed. Although IA was included in the scenarios and storylines of every COCOM exercise assessed under the IA/IOP initiative this year, ground rules governing Red Teams actions usually confine the teams to actions that would not "harm" the network or disrupt the training exercise. Consequently, the training audiences lack exposure to a fuller range of threat-representative Red Team actions and they are not presented with situations to compel them to detect intrusions and restore disrupted networks, services, or corrupted files.
- FY06 Recommendations.
  1. The Joint Staff request that COCOM and Service exercise authorities:
     - Permit more aggressive Red Team attacks representative of projected information-operations activities from adversaries
     - Permit Red Teams to conduct threat representative activities in close coordination with the exercise opposition force
     - Have mature network COOP plans and be prepared to execute them

2. The importance of live-system functionality and corresponding staff activity at selected exercise events should be emphasized by the COCOM leadership and/or the exercise authority. IA and IOP training and assessments require a realistic environment.

3. The Joint Staff should institutionalize a process so that IOP assessment findings are addressed by the appropriate system/process owners and valid workarounds for known IOP problems are promulgated to effect enterprise solutions.