

# Information Assurance (IA) and Interoperability (IOP) Evaluations

## Summary

- The threats to military information networks continue to grow. DoD awareness and activities in response to these threats have grown dramatically this fiscal year, but a significant gap between the threat and our defensive capabilities remains. Failure to close this gap, or inadequate preparation to detect and respond to attacks, may result in degraded mission effectiveness and/or loss of confidence in critical command and control capabilities at inopportune times.
- Most vulnerabilities found during assessment events are basic in nature, and can be remedied by local personnel who possess adequate skills. The fact that many organizations lack a full complement of trained personnel is a root cause of most problems that are exploited by exercise Red Teams.
- The full assessment cycle employed by the Operational Test Agencies (OTAs) continues to contribute to improved warfighter skills and awareness of best practices, identification and resolution of problems, and methods and metrics for measuring operational IA/IOP performance.
- Assessments were performed for 23 Combatant Command (COCOM) and Service exercises this fiscal year.
- Assessment and remediation efforts in support of units deploying to Iraq and Afghanistan were conducted during six exercises; three such assessments are planned for FY08.
- IOP assessment methods and metrics were enhanced and applied to all appropriate exercises this fiscal year.
- More realistic portrayal of threats, and stressing of network Continuity of Operations Plans (COOP) have been emphasized in assessment planning this fiscal year. Several FY08 COCOM exercises are expected to have opposition forces controlling multiple Red Teams that portray nation-state threat capabilities.
- DOT&E issued a new IA Policy for OT&E of acquisition programs in November of 2006. This policy is being implemented by Service OTAs for all programs on the DOT&E oversight list, as well as for many non-oversight programs.

## Background

The FY03 Appropriations bill directed that:

- Operational evaluations of interoperability and information assurance be conducted during COCOM and Service exercises
- The OTAs, the Service Information Warfare Centers (IWCs), and the National Security Agency (NSA) 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 OT&E of acquisition programs

Fiscal year 2007 assessment funds were principally distributed to the OTAs to support the assembly and maintenance of expert teams which perform the IA and IOP assessments, and assist the COCOMs and Services in designing the exercises in which the assessments take place. These teams plan and execute events, assemble and analyze the resulting data, and report the results to the Exercise Authority and DOT&E. This information is collated and analyzed by DOT&E to provide feedback to DoD agencies engaged in IA and IOP solutions, developments, and policies.

The primary elements of the IA/IOP assessment process include:

- Blue Teams – Perform technical network scans and non-technical assessments of networks, network personnel, and network policies and practices.
- Green Teams – Provide assistance to the Exercise Authority in interpreting the results of an assessment, and directly addressing any shortfalls that arise. They coordinate remediation and training, as required.
- Red Teams – Perform live network assessments via penetration testing and other activities based on a comprehensive scenario as part of the exercise scenario and in support of the exercise opposition force. During some assessments, the Red Teams also deploy units to test the physical security of protected facilities. These combined events are seen to provide a more realistic depiction of a multiple-vector threat environment in which the IA posture of a unit may be measured.
- IOP Teams – Perform live network assessments via mission-thread evaluation as part of the exercise scenario to examine information flow in support of stated missions.

OTAs develop assessment plans, quick-look reports, and final reports for each assessment performed. In conjunction with each assessment report, OTAs develop a Vulnerability and Shortfall Matrix (VSM) that consolidates all identified IA vulnerabilities and IOP shortfalls, with proposed priorities and remedies, and a section to track their resolution.

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 execution of the IA/IOP assessment program. The OTA teams that lead the IA/IOP assessments have developed strong relationships with their assigned COCOMs and Services as well as other partner organizations, including the Service IWCs, NSA, the Defense Intelligence Agency (DIA), the Defense Information Systems Agency (DISA), the Joint Task Force – Global Network Operations (JTF-GNO), U. S. Strategic Command, and other elements within DoD.

# INFORMATION ASSURANCE

As many issues identified during the IA/IOP assessment process are not merely local, but represent enterprise-wide issues across multiple theaters, DOT&E provides trend information to a number of cognizant agencies, including the Joint Staff (JCSJ6), the DoD Chief Information Officer (CIO) – Defense Information Assurance Program (DIAP), the NSA Global Information Grid IA Portfolio Manager (GIAP), the Service CIOs, and specific program offices where appropriate. Most of these agencies are additionally addressed via standing bodies, including the IA Senior Leadership group (IASL) and the Enterprise Solutions Steering Group (ESSG) for IA, and the Military Communications & Electronics Board MCEB, which includes both the IA and IOP

panels. These groups address policy issues as well as the rapid fielding of DoD Enterprise tools.

## FY07 Assessment Activities

In FY07, the OTAs performed: (23 events total)

- IA/IOP assessments in conjunction with 14 COCOM and seven Service exercises (Table 1)
- Full Blue, Green, and Red Team events for 15 exercises
- Six exercise assessments for units preparing to deploy to Iraq and Afghanistan

**Table 1 – Information Assurance and Interoperability Exercise Events in FY07**

Exercise Authority	Exercise / Event	Lead OTA	Support OTA
Joint Staff	Bulwark Defender 07	JITC	AFOTEC, ATEC
CENTCOM	Lucky Warrior 07	ATEC	
EUCOM	Coalition Warrior Interoperability Demonstration 07	JITC	MCOTEA
	Sharp Focus 07	ATEC	
	Able Warrior 07-2	ATEC	JITC
JFCOM	Unified Endeavor 07-1*	JITC	ATEC
	1 <sup>st</sup> Armored Division Mission Rehearsal Exercise 07 (Unified Endeavor 07-2)*	ATEC	JITC
NORTHCOM	Vigilant Shield 07	AFOTEC	
	Northern Edge 07	AFOTEC	JITC
PACOM	Terminal Fury 07	ATEC	COTF, AFOTEC
	Talisman Sabre 07	COTF	
	Valiant Shield 07	COTF	
SOUTHCOM	Blue Advance 07	ATEC	
	Panamax 07	ATEC	COTF
	Peace Keeping Operations 07	ATEC	
STRATCOM	Global Lightning 07	JITC	
USFK	Reception, Staging, Onward-movement, and Integration 07	ATEC	
Army	3 <sup>rd</sup> Infantry Division Mission Rehearsal Exercise 07 (Unified Endeavor 07-2)*	ATEC	
	4 <sup>th</sup> Infantry Division Mission Rehearsal Exercise 07 (Unified Endeavor 07-2)*	ATEC	JITC
	101 <sup>st</sup> Airborne Division Mission Rehearsal Exercise 07 (Unified Endeavor 08-1)*	ATEC	JITC
	Combined Arms Center (Fort Leavenworth)	ATEC	
Marine Corps	Federation of Systems 07	MCOTEA	
	1 <sup>st</sup> Marine Expeditionary Force Exercise*	MCOTEA	

\*Pre-deployment assessment events in FY07

AFOTEC – Air Force Operational Test and Evaluation Center  
 ATEC – Army Test and Evaluation Command  
 CENTCOM – Central Command  
 COTF – Commander Operational Test and Evaluation Force  
 EUCOM – European Command  
 JFCOM – Joint Forces Command  
 JITC – Joint Interoperability Test Command

MCOTEA – Marine Corps Operational Test and Evaluation Activity  
 NORTHCOM – Northern Command  
 PACOM – Pacific Command  
 SOUTHCOM – Southern Command  
 STRATCOM – Strategic Command  
 TRANSCOM – Transportation Command  
 USFK – U.S. Forces, Korea

The IA/IOP Assessment Program made improvements to the planning, assessment, and reporting methods employed during this fiscal year:

- Established a common methodology for technical and non-technical Blue Team assessments
- Initiated development of a Green Team Guidebook and linkage of Green Team assistance efforts to formal program support via ASD(NII) and DISA
- Formally adopted a common set of Core Control Measures derived from the Department of Defense Instruction (DoDI) 8500.2 IA Requirements
- Participated in ongoing efforts with NSA, the DIAP, the GIAP, and DISA to establish a common set of IA metrics for DoD assessments
- Established an Interoperability Working Group to develop common metrics for IOP
- Established an online capability for storing, updating, and analyzing assessment data
- Developed a prototype online collaboration and reporting tool for data collection and analysis, to improve timeliness, consistency, and accuracy of data collection
- Conducted a three-year trend analysis of IA/IOP assessments to identify positive and negative performance trends

The Vulnerability and Shortfall Matrix (VSM), used by OTAs to document assessment results, is the subject of significant multi-agency collaborations in IA and IOP. DOT&E is participating with NSA, the Service IWCs, DISA, and JTF-GNO to create standardized sharing protocols that will allow each agency to make full use of the data collected by another agency, potentially improving the depth and validity of analyses across multiple organizations.

DOT&E issued an updated IA policy for OT&E of acquisition programs, and conducted training for DOT&E Action Officers to ensure uniform implementation of the new six-step policy. DOT&E also identified a number of acquisition programs for in-depth IA evaluation. Red Team assessments, using the methodologies and collection techniques developed in the IA/IOP assessment process, were conducted under DOT&E oversight for the:

- Global Broadcasting Service (GBS)
- Patriot (PAC-3) Build 6
- Business Systems Modernization (BSM)
- Global Positioning System (GPS)
- Combat Information Transport System (CITS)

Additional programs such as the Joint Strike Fighter (JSF/F-35) and Ship Self-Defense System (SSDS) are proceeding towards similar IA assessments in the future. In the case of the Net-Enabled Command Capability (NECC) program, DOT&E is actively involved with the Program Office to develop IA test concepts to ensure adequate IA assessments through the Integrated Test Team.

## Assessment

Although emphasis on IA continues to improve at all assessed commands, the threats to military information networks continue to grow. DoD awareness and activities in response to these threats have grown dramatically this fiscal year, but a significant gap between the threat and our defensive capabilities remains. Failure to close this gap, or inadequate preparation to detect and respond to attacks, may result in degraded mission effectiveness and/or loss of confidence in critical command and control capabilities at inopportune times.

Boundary defenses for most DoD networks are improving, making network penetration more difficult for Red Teams than in FY06, but generally not difficult enough. More realistic portrayal of real-world threats and stressing of network COOP are needed to prepare network defenders and warfighters to effectively perform protect, detect, react, and restore missions in the face of network intrusions.

Many of the vulnerabilities found during assessments are basic, with known solutions, and can be remedied by local personnel. In most cases, the lack of adherence to best practices and known solutions is directly traced to the lack of manpower (or sufficiently trained manpower) to carry out the many manpower-intensive tasks necessary to protect information networks. Resource support for conducting these basic tasks is needed. Working with DISA, the DIAP, and the ESSG, DOT&E has been active in identifying areas in which improved automated tools can make more efficient use of the limited manpower available.

General assessments trends include the following:

- Personnel and Training
  - Standard manning templates for IA personnel that account for network complexity and mission do not exist; this forces a reliance on inadequately trained or undesignated personnel for network management.
  - Training and exercise of defensive tactics, techniques, and procedures (TTP) remains low across all assessed commands, giving a distinct advantage to network attackers.
  - Network COOPs are generally in need of improvement and not routinely exercised.
  - Many intrusions could be detected by forensic analysis of logs and audit records. As these activities are manpower intensive, automated log analysis and correlation tools are needed.
- Configuration management and Interoperability
  - Positive configuration control is increasing, but new technologies continue to complicate enforcement of standards. Users implement untested or “work-around” interoperability solutions that can result in vulnerabilities.

# INFORMATION ASSURANCE

- System version information collected during IOP assessments indicate that roughly one-quarter of all assessed systems have an interoperability certification as required by DoD regulation.
- Policy Compliance
  - Most commands do not possess complete network documentation and policies for existing networks.
  - Classified networks frequently do not employ intrusion detection software.
  - Standard tools for internal traffic monitoring and anomaly detection are not available.
- Physical security
  - Opposition forces frequently acquire sensitive information that assists in both physical and network penetration.
  - Use of basic precautions, such as screen-locks and time-outs, is inconsistent, allowing intruders unblocked access to systems.
  - Positive physical control over critical network components is improving, but many network devices such as switches and routers are not secured.

**Table 2 – Planned IA & Interoperability Exercise Events for FY08**

Exercise Authority	Exercise / Event	Lead OTA	Support OTA
Joint Staff	Coalition Warrior Interoperability Demonstration-08	JITC	MCOTEA
CENTCOM	Bright Star 08	ATEC	MCOTEA
EUCOM	Austere Challenge 08	ATEC	AFOTEC, JITC
JFCOM	Combined Joint Task Force/Horn of Africa 08	JITC	
	United Endeavor 08-1*	ATEC	JITC
NORTHCOM	Ardent Sentry 08	AFOTEC	MCOTEA, JITC
	Vigilant Shield 08	AFOTEC	JITC
PACOM	Terminal Fury 08	COTF	ATEC, AFOTEC
	Key Resolve 08	COTF	AFOTEC
SOUTHCOM	Blue Advance 08	ATEC	COTF, MCOTEA
STRATCOM	Global Lightning 08	JITC	MCOTEA
	Bulwark Defender 08	JITC	ATEC, AFOTEC
	Global Storm 08	JITC	MCOTEA
	Global Thunder 08	JITC	
TRANSCOM	Turbo Distribution 08	JITC	MCOTEA
Army	3 <sup>rd</sup> Army	ATEC	
Navy	Joint Task Force Exercise 08-4	COTF	
Marine Corps	1 <sup>st</sup> Marine Expeditionary Force Exercise*	MCOTEA	
	2 <sup>nd</sup> Marine Expeditionary Force Exercise*	MCOTEA	

\*Pre-deployment assessment events in FY08

AFOTEC – Air Force Operational Test and Evaluation Center  
 ATEC – Army Test and Evaluation Command  
 CENTCOM – Central Command  
 COTF – Commander Operational Test and Evaluation Force  
 EUCOM – European Command  
 JFCOM – Joint Forces Command  
 JITC – Joint Interoperability Test Command  
 MCOTEA – Marine Corps Operational Test and Evaluation Activity

NORTHCOM – Northern Command  
 PACOM – Pacific Command  
 SOUTHCOM – Southern Command  
 STRATCOM – Strategic Command  
 TRANSCOM – Transportation Command  
 USFK – U.S. Forces, Korea

## FY08 Goals and Planned Assessment Activities

The Combatant Commands and Services continue to respond positively to the exercise assessment process, and to support deeper and more comprehensive evaluations of readiness.

Assessment plans for FY08 include approximately 20 exercises (See Table 2). The FY08 goals for the IA/IOP Assessment Program include improved:

- Consistency in the collection, analyses, and reporting of performance data to assess network readiness and operational IA and IOP postures
- Portrayal of Red Team and Opposition Force operations to more realistically depict real-world threats
- Emphasis on the exercise and assessment of intrusion detection COOPs, data/system recovery, and restoration
- Operational metrics to better quantify the effectiveness of network defenses under attack
- IOP standards through the use of a mission-thread based approach using COCOM-defined mission processes, tasks, and linkages
- Collaboration, reporting, and analysis tools

Acquisition program IA assessment support will continue to expand in FY08, and DOT&E will continue integrating IA and IOP issues identified during OT&E of acquisition programs into the IA/IOP Assessment Program planning process. COCOM and Service exercises provide an excellent opportunity to track issues identified during OT&E of acquisition programs to ensure they are resolved, and that solutions and upgrades provided after system fielding do not introduce further IOP problems or IA vulnerabilities. In coordination with the Joint Staff and ASD(NII), DOT&E will continue data-sharing and integration efforts with DISA and NSA to create a common foundation for analysis and deficiency tracking.

## Recommendations

- Status of Previous Recommendations. Action has been taken on the DOT&E FY06 recommendations, but more action is needed.
- Limitations continue to be imposed by exercise authorities that prevent more realistic Red Team emulation of adversary capabilities. Some commands permit long-term, sustained Red Teaming, a much more threat-representative approach to IA assessments that should be implemented in all theaters.
- On May 29, 2007, the Joint Staff J6 transmitted a message to COCOM counterparts urging more accurate portrayal of real-world threats during exercises, sufficient command priority to embed rigorous IA scenarios into the exercises, closer ties between the Red Team and the Opposition Force, and greater emphasis on operational impacts.
- COCOMs remain reliant on simulation in many aspects of exercise play, but are increasing the amount of live-system functionality and staff activity.
- Interoperability remediation and assessment findings have been incorporated into the Military Communications and Electronics Board Interoperability Panel.
- FY07 Recommendations.
  - Exercise authorities should permit more realistic network attacks to exercise detection capabilities, and network COOPs and recovery plans; a Joint Staff recommendation to high-level COCOM and Service authorities would be helpful.
  - The Joint Staff and/or USSTRATCOM should undertake the development of standard network manning and training templates based on network function, complexity, and required maintenance.

