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


**Summary**

- DoD awareness and preparation to meet the growing threats to military information systems and networks continued to improve in FY08, but significant gaps still exist between potential adversary actions and demonstrated defensive capabilities.
- Collaboration suites designed to improve warfighter situational awareness may achieve interoperability goals, but in some cases have introduced network vulnerabilities. The Joint Staff has communicated this concern to operational commanders as a near-term response; for the longer term, opportunities to accelerate implementation of the classified Public Key Infrastructure program should be considered.
- Exercise constraints that preclude the realistic employment of sophisticated attack mechanisms can lead exercise participants to a false sense of security. SECDEF guidance to plan for, implement, and regularly exercise the capability to fight through cyber/kinetic attacks that degrade the Global Information Grid needs to be fully implemented.
- Most vulnerabilities found during FY08 assessments are basic in nature and can be remedied by qualified local personnel. However, many organizations lack a full complement of trained personnel. This finding is serious given the fact that the threats presented during these exercises were below what might be expected from a top-tier nation-state.
- Approximately 75 percent of the fielded systems observed do not have current interoperability certifications.


**Process**

DOT&E oversees the execution of the Information Assurance (IA) and Interoperability (IOP) assessment program. Participating Service and Agency teams perform the assessments and assist the Combatant Commanders (COCOMs) and Services in designing the exercises in which the assessments take place. DOT&E aggregates and analyzes assessment data to provide feedback to the Military Services and DoD agencies. The IA/IOP assessment process includes the following:

- Blue Teams – Perform technical and non-technical assessments, including scans and surveys of networks, network personnel, and network policies and practices.
- Green Teams – Assist the Exercise Authority in interpreting the results of an assessment, addressing shortfalls, and coordinating remediation and training, as required.
- Red Teams – Perform live network assessments via penetration testing and other activities as part of the exercise scenario and in support of the exercise opposition force.
- IOP Teams – Conduct assessments focused on specific mission threads or events as part of the exercise scenario to examine information flow in support of stated missions, tasks, or objectives.

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

- Developed, validated, and implemented a standardized set of IA metrics and analytical methods that quantify operational performance attributes and outcomes
- Initiated development of operational performance metrics for IOP assessments, and mission accomplishment/impact metrics for IA assessments
- Instituted a process to formally provide exercise findings regarding specific system issues to the cognizant Services' acquisition leadership
- Created a dedicated IOP team to plan and execute focused IOP assessments
- Funded Defense Intelligence Agency development of cyber threat support documents to guide the realistic portrayal of network threats during COCOM and Service exercises
- Supported ongoing efforts at the Defense IA Program Office to establish standard enterprise metrics and efforts by the Enterprise Solutions Steering Group to assess the return on investment for selected IA products purchased and licensed by DoD

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 that assessing organizations report significant findings to Service acquisition authorities, Service Chief Information Officers, and specific program offices, where appropriate, for investigation and resolution.

**FY08 Assessment Activities**

In FY08, the OTAs performed 19 of 20 planned assessments. These included 12 COCOM and seven Service exercise assessments (Table 1). Five of these assessments involved units preparing to deploy to Iraq and Afghanistan.

The OTAs employed the DOT&E six-step IA Assessment Process for 10 major acquisition systems under DOT&E oversight in FY08. Since the IA certification process tends to focus on design and preparations for operations ("Protect"), OT&E events have been reviewed to ensure additional focus on the operational aspects ("Detect," "React," and "Restore").

The OTAs assessed the following acquisition systems with enhanced IA and IOP focus as indicated:
- Dry Cargo/Ammunition Ship, T-AKE (IA and IOP)
- Amphibious Assault Ship, LPD-17 (IA and IOP)
- Teleport Generation 2 (IA and IOP)
- Global Broadcast Service, GBS (IA and IOP)
- Global Positioning System, GPS (IA and IOP)
- Wideband Global Satellites, WGS (IA)
- Communications Processing System Release 3, CPS-3 (IA)
- Business Systems Modernization, BSM, BSM-E (IA)
- Combat Information Transport System, CITS (IA)
- Public Key Infrastructure, PKI (IA and IOP)

**Assessment**

DoD awareness and preparation to meet the growing threats to military information systems and networks continued to improve in FY08, but significant gaps still exist between potential adversary actions and demonstrated defense capabilities. The inability to detect penetrations or presence of an advanced adversary was a frequently noted shortfall. This gap may place mission accomplishment at risk.

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. COCOM staffs are seeking new approaches to ensure that warfighters are prepared to successfully operate in realistic threat environments with degraded systems. SECDEF guidance to plan for, implement, and regularly exercise the capability to fight through cyber/kinetic attacks that degrade the Global Information Grid needs to be fully implemented. Given their interdependency, assessors need to examine IA and IOP simultaneously during exercises.

Assessors continue to find most vulnerabilities are basic in nature, and easily remedied by local personnel with adequate skills. Many organizations lack a full complement of trained personnel. This remains a root cause of most problems that exercise Red Teams exploit. This finding must be tempered with the fact that the threats presented during these exercises fall substantially below what might be expected from a top-tier nation-state.

Collaboration suites improve warfighter interoperability often at the expense of introducing network vulnerabilities. FY08 exercise assessments identified two fielded collaboration suites that Red Teams have repeatedly exploited. While the technical solutions to closing these gaps are straightforward, the difficulty with simply closing the vulnerabilities highlights the challenge in balancing IOP and IA. These systems enhance information exchange for the warfighter, but for certain configurations, they also introduce serious vulnerabilities. DOT&E shared these findings with the Services, who have initiated several actions in response to these findings, including:
- Guidance to motivate implementation of stronger passwords
- Revision of system software documentation to improve security settings
- Other measures to provide an additional layer of security for collaboration suites

Additionally, the Joint Staff has communicated the specific vulnerabilities to operational commanders so they can reassess their local policies and the associated operational risks imposed across the DoD enterprise. For the longer term, opportunities to accelerate implementation of the Public Key Infrastructure program should be considered.

Interoperability assessments have revealed that:
- Approximately 75 percent of the fielded systems observed do not have current interoperability certifications.
- Many interoperability problems are remediated with local workarounds; however, the latter are often not well documented or consistent across DoD networks.
- Some major C2 systems, such as Command Post of the Future, Fusion Net, and Combined Information Dissemination Network Environment, are not fully interoperable with other C2 systems with which they are expected to operate.
- Network authentication and trust methods (such as Public Key Infrastructure) are not consistent among federal agencies. Each entity identifies, reports, and addresses network events (both IA and IOP) via differing processes.
- There are differing priorities for information sharing in classified networks across federal agencies. Some reduce access in the interests of security, while others broaden access among U. S. agencies and even coalition partners in the interest of information sharing.
- Introduction of enterprise solutions has generally helped standardize procedures and provided efficiencies, but it has also contributed to interoperability challenges. New tools are sometimes not compatible with existing tools (such as network scanners and discovery tools). Technology upgrades often impact training and support. Where network services are outsourced (e.g., Navy Marine Corps Intranet), or in cases where Services have committed to long-term licensing agreements, the hosting of new C2 applications may require significant contractual adjustments in order to achieve desired levels of interoperability.

General exercise assessment trends and findings include the following:
- *Intrusions Rates*. Red Teams report that penetration of warfighter networks has become more challenging over the last three years, although intrusion success rates remain high. Long-duration, stealthy intrusion efforts are more often successful and less frequently detected than short-duration exercise scenarios permit.
- *Maintenance.* Assessments generally found overall support, budgets, and spares to be adequate. Software configuration was the only maintenance factor that routinely adversely impacted network performance.
- *Boundary Defenses.* While boundaries for unclassified networks generally meet required standards, boundary protections for most classified networks assessed do not

meet specified requirements, and appear to rely on presumed network isolation and encryption for protection.
- *Configuration.* Network boundary defenses are seriously undermined by low compliance with port and protocol configuration requirements. Users do not fully comply with System Technical Implementation Guides in many fielded systems. Red Teams report that known, but un-patched, vulnerabilities commonly enable network intrusion and exploitation.
- *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 intrusions. Public Key Infrastructure credentials are not standard across U.S. Federal agencies and departments, inhibiting interoperability, information sharing, and system-to-system trust between DoD and other agencies.
- *Network/System backup.* Few assessed networks have effective back-up practices for individual systems and critical applications.
- *Automated Management Tools*. The majority of military information networks and systems are regularly scanned for vulnerabilities. Use of anti-virus and anti-spyware software is nearly 100 percent for all networks assessed. However, network audit logs, while usually properly configured, are infrequently reviewed, and automated tools for identification and analysis of abnormal activities have not been generally available. The recent introduction of an enterprise host-based security suite for DoD should increase the use of these tools. FY09 assessments will examine the benefits realized from implementing the host-based security suite.
- *Manning*. Manpower requirements for new systems and applications generally do not address additional network support personnel requirements.

Review of assessments of acquisition programs and systems under DOT&E oversight has shown:
- Compliance with DoD IA controls remains incomplete for many systems. The lack of timely patches, use of weak or default passwords, the use of incorrect configurations, and the use of unnecessary ports and services significantly reduce the readiness of new systems to operate effectively on DoD networks.
- Continuity and recovery plans are often lacking for newly fielded systems.
- IA protection against external threats is typically substantially better than protections against internal/insider threats.
- OT&E often yields very limited data on the operational aspects of IA. During many operational test events, the representative IA environment (including firewalls and intrusion detection systems) were not available, inhibiting a full evaluation of those networks and systems.

Exercise assessments and OT&E continue to identify shortcomings in both the information assurance and interoperability of fielded systems. System limitations often 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 to rapidly detect, assess, and respond to network exploitations or attacks.

**FY09 Goals and Planned Assessment Activities**

DOT&E has identified 22 COCOM and Service exercises for assessment in FY09, 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. Eight of the exercises will be for units preparing for deployment to Iraq and Afghanistan. The FY09 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
- Transmitting critical finding to Service leadership

**Recommendations**

- Status of Previous Recommendations. The following are the FY07 recommendations and their status at the end of FY08:
  - FY07 #1: Exercise authorities should permit more realistic network attacks to exercise detection capabilities, and network Continuity of Operations and recovery plans; a Joint Staff recommendation to high-level COCOM and Service authorities would be helpful. SECDEF issued Guidance to the Force to plan for, implement, and regularly exercise the capability to fight through cyber/kinetic attacks that degrade the Global Information Grid. Additionally, the Vice Chairman of the Joint Chiefs of Staff sent a message to Commander, U.S. Joint Forces Command requesting more realistic threat portrayal during exercises. These initiatives should be reflected in FY09 exercise planning.
  - FY07 #2: The Joint Staff and/or U.S. Strategic Command should undertake the development of standard network manning and training templates based on network function, complexity, and required maintenance. There is no ongoing DoD-wide effort to identify the manning baselines, and the associated personnel training and qualification requirements, for managing, administering, and operating networks of different size, complexity, and functionality. This issue has been briefed to and is under the consideration of the IA Senior Leadership panel.
- FY08 Recommendations.
  1. To enhance the value of exercise assessments, exercise authorities for each COCOM and Service should work with appropriate Defense Agencies to incorporate the portrayal of representative nation-state cyber threats during at least one of their major exercises each fiscal year. (Due to security and other concerns, certain aspects may need to be

conducted on segregated networks or as "table-top" events for senior decision-makers.) Additionally:

- National Security Agency, Defense Intelligence Agency, and exercise planners should develop threat assessments and threat-representative exploits to portray realistic cyber threats during selected exercises.
- Exercise planners and assessing organizations should develop exercise plans consistent with other training objectives that exercise the capabilities needed to fight through cyber/kinetic attacks that degrade normal network operations.
- The U.S. Strategic Command Joint Task Force for Global Network Operations should expand participation in all major COCOM exercises where networks are to be subjected to exercise cyber attacks at the nation-state level.

2. The Joint Staff and Services should more strictly enforce adherence to the interoperability certification and re-certification process.

**Table 1. Information Assurance and Interoperability Exercise Events in FY08**

| Exercise Authority | Exercise / Event | Lead OTA | Support OTA |
|---|---|---|---|
| Joint Staff | CWID 08 | JITC | MCOTEA |
| CENTCOM | AOR -1 (OEF) | ATEC | |
| | AOR - 2 (OIF) | ATEC | |
| EUCOM | Austere Challenge 08 | ATEC | JITC |
| | Flexible Leader 08 | ATEC | |
| JFCOM | CJTF – Horn of Africa | JITC | |
| NORTHCOM | Vigilant Shield 08 | AFOTEC | JITC |
| | Ardent Sentry 08 | AFOTEC | MCOTEA, AFIOC |
| PACOM | Terminal Fury 08 | ATEC | JITC |
| SOUTHCOM | Blue Advance 08 | ATEC | |
| | PANAMAX 08 | ATEC | |
| STRATCOM | Bulwark Defender 08 | JITC | |
| | Global Storm 08 | JITC | ATEC, AFIOC, MCOTEA |
| TRANSCOM | Turbo Distribution 08 | JITC | |
| USFK | Key Resolve 08 | ATEC | AFOTEC |
| USA | Unified Endeavor 08-1 | ATEC | JITC, MCOTEA |
| | Unified Endeavor 09-1, Phase 1 | ATEC | JITC |
| | Unified Endeavor 09-1, Phase 2 | ATEC | JITC |
| USN | JTFEX 08-4 | COTF | AFIOC, JITC |

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
USFK – U.S. Forces, Korea
USA – Army
USN – Navy

AOR – Area of Responsibility
CJTF – Commander Joint Task Force
CWID – Coalition Warrior Interoperability Demonstration
JTFEX – Joint Task Force Exercise
OEF – Operation Enduring Freedom
OIF – Operation Iraqi Freedom

ATEC – Army Test and Evaluation Command
AFIOC – Air Force Information Operations Center
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

**Table 2. Planned Information Assurance and Interoperability Assessment Events for FY09**

| Exercise Authority | Exercise / Event | Lead OTA | Support OTA |
|---|---|---|---|
| AFRICOM | CPX 09 | ATEC | JITC |
| CENTCOM | Internal Look 09 | ATEC | |
| EUCOM | Austere Challenge 09 | ATEC | JITC |
| JFCOM | CWID 09 | JITC | AFIOC, ATEC, COTF, MCOTEA |
| NORTHCOM | Vigilant Shield 09 | AFIOC | JITC |
| PACOM | Terminal Fury 09 | ATEC | COTF, MCOTEA |
| | Talisman Saber 09 | ATEC | COTF, MCOTEA |
| SOCOM | Able Warrior 09-2 | MCOTEA | JITC |
| SOUTHCOM | PANAMAX 09 | ATEC | JITC |
| STRATCOM | Global Lightning/Bulwark Defender 09 | JITC | |
| | Global Storm 09 | JITC | |
| TRANSCOM | Turbo Challenge 09 | JITC | |
| USFK | Key Resolve 09 | ATEC | JITC |
| USA | 2nd ID CPX 09 (USFK) | ATEC | |
| USA | Unified Endeavor 09-1 Phase V | ATEC | |
| | Unified Endeavor 09-2 | ATEC | |
| | Unified Endeavor 09-3 Phase I | ATEC | |
| | Unified Endeavor 09-3 Phase II | ATEC | |
| | Unified Endeavor 09-3 Phase V | ATEC | |
| USN | Joint Task Force Exercise 09-2 | COTF | |
| | Joint Task Force Exercise 09-3 | COTF | |
| USAF | Black Demon 09 | AFIOC | |
| USMC | Unified Endeavor 09-1 Phase IV | MCOTEA | |

AFRICOM – African Command
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
USFK – U.S. Forces, Korea
USA – Army
USN – Navy
USAF – Air Force
USMC – Marine Corps

AOR – Area of Responsibility
CJTF – Commander Joint Task Force
CPX – Command Post Exercise
CWID – Coalition Warrior Interoperability Demonstration
JTFEX – Joint Task Force Exercise
OEF – Operation Enduring Freedom
OIF – Operation Iraqi Freedom

ATEC – Army Test and Evaluation Command
AFIOC – Air Force Information Operations Center
COTF – Commander, Operational Test and Evaluation Force
JITC – Joint Interoperability Test Command
MCOTEA – Marine Corps Operational Test and Evaluation Activity