Information Assurance (IA) and Interoperability (IOP)

SUMMARY

Although 16 assessments were planned for FY13, 8 of those were associated with Combatant Command (CCMD) or Service exercises that either were cancelled, reduced in scope, or split into smaller events because of funding cuts and limitations related to sequestration as shown in Figure 1. Nonetheless, the DOT&E Information Assurance (IA) and Interoperability (IOP) Assessment Program completed 12 assessments: 9 of which were conducted at 8 CCMDs and 3 at Service exercises. These were conducted during either exercises or real-world activities and DOT&E was able to analyze these events for trends in context with the prior six years of assessments, as shown in Figure 2.

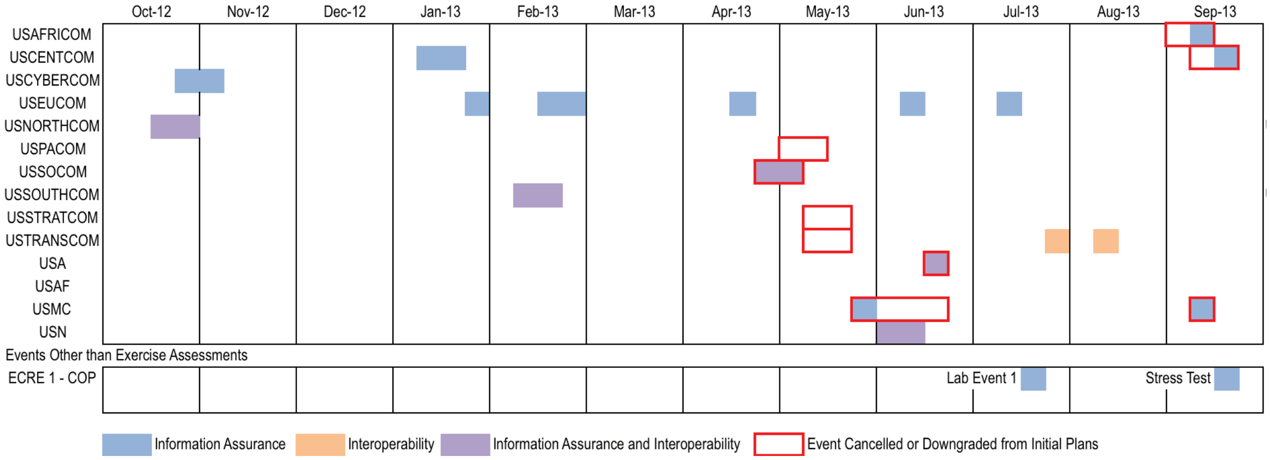

Figure 1: FY13 Exercise Assessments

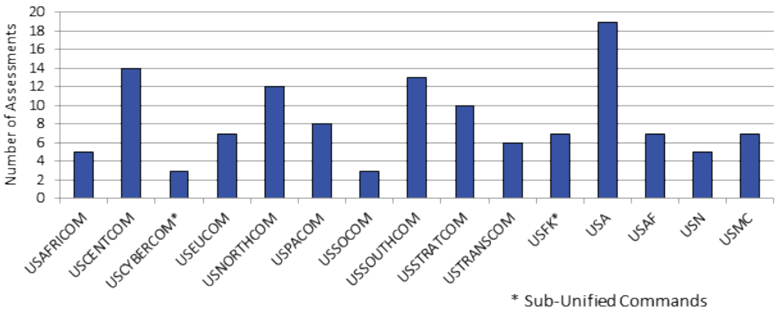

Figure 2: FY07-FY13 Exercise Assessments

USAFRICOM – U.S. Africa Command
USCENTCOM – U.S. Central Command
USCYBERCOM – U.S. Cyber Command
USEUCOM – U.S. European Command
USNORTHCOM – U.S. Northern Command
USPACOM – U.S. Pacific Command
USSOCOM – U.S. Special Operations Command
ECRE – Enterprise Cyber Range Environment

USSOUTHCOM – U.S. Southern Command
USSTRATCOM – U.S. Strategic Command
USTRANSCOM – U.S. Transportation Command
USA – U.S. Army
USAF – U.S. Air Force
USMC – U.S. Marine Corps
USN – U.S. Navy
C2IS – Command, Control, and Intelligence Systems

Most FY13 assessments were at smaller venues than previous years and often included only the lowest tier of computer network defense (local network defenders).[1] At the same time, many assessed commands continued an ongoing transition from direct CCMD management of network resources to an enterprise model of consolidated network defenses – a trend that will continue with the Joint Information Environment (JIE). As a result, the actual Computer Network Defense Service Providers (CNDSP) were not usually assessed during FY13 exercises. To offset this, three events explored new approaches for assessments without a training exercise: (1) an extended Theater Cyber Readiness Campaign assessment, (2) a Cyber Key Terrain

[1] Computer Network Defense (CND) is divided by responsibility into three tiers: Tier 3 (local), Tier 2 (CND Service Providers, e.g., Service and Agency cyber commands), and Tier 1 (Dod-wide, e.g., U S Cyber Command)

methodology assessment, and (3) the IA and IOP Assessment Program also explored making better use of cyber range facilities by sponsoring the Enterprise Cyber Range Environment (ECRE).[2]

Based on FY13 assessments, the demonstrated capabilities of the local network defenses are insufficient to protect against a determined or well-resourced cyber adversary and warfighter missions should be considered "at moderate to high risk" until they can be demonstrated to be resilient in a contested cyber environment. Overall IA (soon to be referred to as "cybersecurity") compliance observed during the FY13 exercise assessments reflected continued and even improved conformance with standards and policies as shown in Figure 3.[3] However, network scans continued to find missing patches and IA vulnerability alerts at rates consistent with previous years.

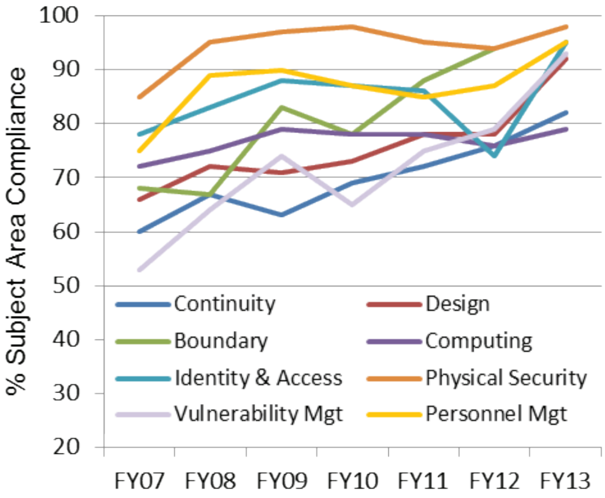

Figure 3: Network Standards Compliance

Red Teams were consistently able to penetrate and exploit networks, but seldom were permitted to conduct disruptive activities – and the lack of exercise participation by upper-tier CNDSPs limited the ability to fully assess the impact of Red Team activities. This lack of participation in IA evaluations must be addressed as it raises questions regarding CNDSP effectiveness in guarding against, recognizing, and responding to attacks. By extension, it also raises questions regarding the approach JIE will implement for computer network defense.

IOP assessments were limited in FY13 for the same reasons as cited earlier, but anecdotal findings confirmed that operators frequently implement workarounds to complete assigned missions and tasks when information systems encounter difficulties exchanging data automatically. These workarounds usually resulted in increased operator workloads, increased errors, and slowed mission performance, but did not affect the accomplishment of the assigned missions and tasks. Less than one third of all fielded systems observed in assessments over the past five years have had current Interoperability certifications. Given the generally effective interoperation of the systems assessed, both certified and uncertified, it is clear the Interoperability certification process provided little to no confidence in system readiness and has not eliminated the need for such workarounds.

Attainment of the milestones from the Chairman, Joint Chiefs of Staff (CJCS) Execute Order (EXORD) to Incorporate Realistic Cyberspace Conditions into Major DoD Exercises of February 2011 remained low. Portrayal of denied, manipulated, or contested cyber conditions was seldom permitted in FY13 assessments, providing little opportunity for the continued development of more sophisticated tactics and procedures. Currently, the Joint Staff intends to allow the EXORD to expire in February 2014 but will replace it with a CJCS Instruction.

Increased emphasis on cybersecurity test planning improved the level of rigor and cyber-threat realism in acquisition tests, but the majority of cybersecurity problems identified during operational testing in FY13 could have been uncovered and resolved in early phases of development and testing. DOT&E and USD(AT&L) are coordinating to update procedures for developmental and operational cybersecurity testing to increase the scope and rigor for an integrated test strategy to improve discovery and correction of vulnerabilities earlier in the acquisition development cycle.

Essential observations for FY13 include:

- DoD is moving towards more centralized and enterprise-based management of cyber capabilities, including the implementation of JIE.
- Local network (proactive) defenses were insufficient to counter the portrayed cyber adversaries.
- Inclusion of upper tier CNDSP participation is essential for both effective training and effective network defense.
- While standards compliance has improved, such compliance is necessary but not sufficient to ensure effective network defense.
- DoD cybersecurity training policies should require participation by all relevant cybersecurity activities/tiers operating in contested cyber conditions with realistic threats.
- The currently evolving tools needed to automate the management and defense of enterprise networks will require ongoing testing and evaluation.
- Cybersecurity testing of acquisition programs must emphasize earlier discovery and remediation of vulnerabilities.

[2] An assessment of Cyber Key Terrain identifies critical components and nodes related to missions of interest, and focuses on the protection and defense of those key components and nodes.

[3] Revised DoD Instruction 8500.01, anticipated release in late 2013.

FY13 ACTIVITIES

In FY13, the five assessing organizations were the Army Test and Evaluation Command; Commander, Operational Test and Evaluation Force; the Marine Corps Operational Test and Evaluation Activity; the Joint Interoperability Test Command; and the Air Force Operational Test and Evaluation Center. These five Operational Test Agencies completed 12 assessments under the DOT&E IA and IOP Assessment Program that included 9 CCMD and 3 Service exercise assessments (see Table 1). Two of the assessments involved units preparing to deploy (or already deployed) to Iraq and Afghanistan.

TABLE 1. INFORMATION ASSURANCE AND INTEROPERABILITY EXERCISE EVENTS IN FY13

ASSESSMENT/EXERCISE AUTHORITY	ASSESSMENT/EXERCISE VENUE	DESIGNATED ASSESSMENT LEAD
U.S. Africa Command	Judicious Response 2013 (Exercise cancelled)	ATEC
	Headquarters Vulnerability Assessment (Multiple events)	ATEC
U.S. Central Command	Marine Forces CENTCOM Site Assessment	ATEC
	Internal Look 2013 (Exercise cancelled)	ATEC
	Headquarters Vulnerability Assessment	ATEC
U.S. Cyber Command	Cyber Flag 2013	ATEC
U.S. European Command	Theater Cyber Readiness Campaign (Multiple events)	ATEC
North American Aerospace Defense Command/U.S. Northern Command	Vigilant Shield 2013	AFOTEC
U.S. Pacific Command	Terminal Fury 2013 (Exercise cancelled)	COTF
U.S. Special Operations Command	Emerald Warrior 2013	ATEC
U.S. Southern Command	Integrated Advance 2013	ATEC
U.S. Strategic Command	Global Lightning 2013 (Exercise cancelled)	JITC
U.S. Transportation Command	Turbo Challenge 2013 (Exercise cancelled)	JITC
	Real World Assessment	JITC
U.S. Army	Warfighter Exercise 13-4	ATEC
U.S. Navy	USS *Harry S. Truman* Sustainment Exercise	COTF
	Bold Quest 2013 (Exercise cancelled)	COTF
U.S. Air Force	Blue Flag 2013 (Exercise cancelled)	AFOTEC
	Ulchi Freedom Guardian 2013 (Deferred to 2014)	AFOTEC
U.S. Marine Corps	Dawn Blitz 2013-2	MCOTEA
	I MEF Site Assessment	MCOTEA

AFOTEC – Air Force Operational Test and Evaluation Center ATEC – Army Test and Evaluation Command CENTCOM – U.S. Central Command
COTF – Commander, Operational Test and Evaluation Force IOW – Information Operations Wing JITC – Joint Interoperability Test Command
MCOTEA – Marine Corps Operational Test and Evaluation Activity MEF – Marine Expeditionary Force

DOT&E and the Operational Test Agencies began an ongoing in-depth analysis on a number of topics germane to the conduct and improvement of IA and IOP assessments including:

- Consolidated assessment program guidance and practices into a handbook-style document
- Revised cybersecurity compliance metrics to attain consistency with the National Institute for Standards Risk Management Framework
- Revised IOP metrics to capture expanded areas of interest and better integrate with IA as part of a holistic cybersecurity assessment
- Revised data collection forms to incorporate lessons learned and capture new areas of interest
- Reviewed IA/cybersecurity compliance inspection and review programs to identify data sharing opportunities
- Designed a scorecard for measuring compliance with guidance to improve training in contested cyber environments
- Developed a Cyber Key Terrain assessment methodology when exercise events are not available
- Developed a scoring mechanism to rate potential exercise venues as well as evaluate the quality of an assessment

Many of the lessons learned during exercise assessments have provided insight on better test methods for systems under acquisition and test. To enhance the cybersecurity for acquisition programs, DOT&E continued to revise and refine the guidance, templates, and process for planning IA testing for acquisition programs. The templates facilitate development and review of Test and Evaluation Master Plans and test plans to ensure that IA is adequately addressed. The templates and new process were applied to reviews of 67 separate Service and DoD systems, including 67 Test and Evaluation Master Plans, 14 operational test plans, and 12 related test documents.

DOT&E IA subject matter experts specifically observed IA tests and reviewed report data for 21 systems that showed the majority of cybersecurity problems identified during operational testing in FY13 could have been uncovered and resolved in early phases of developmental testing. DOT&E and USD(AT&L) are working together to revise and update procedures for developmental and operational cybersecurity testing. The purpose of these revisions is to expand the opportunities to discover and correct vulnerabilities earlier in the acquisition development cycle. This will be accomplished by systematically examining the stated system cybersecurity requirements, analyzing the inherent cybersecurity requirements that arise from the system operating environment, and constructing tests that realistically depict the ways an adversary would attempt to compromise the system under test.

DOT&E conducted site visits in support of cyber assessments for the U.S. Air Force's (USAF) Joint Space Operation Center Mission System and the U.S. Navy's (USN) Joint High Speed Vessel and *Los Angeles/Virginia* submarines. DOT&E has provided active support to assist in the development of cyber testing for systems such as the USN CVN-78 aircraft carrier, USAF Joint Strike Fighter and KC-46 aircraft, and the U.S. Army (USA) M1 ABRAMS tank.

FINDINGS, TRENDS, AND ANALYSIS

Assessment Structure

Ownership, architecture, and command and control relationships governing DoD networks are all in considerable flux. The European-based networks are in transition to a JIE structure, Navy networks are in transition from an outsourced service to a partially outsourced service, and the division of duties between network defense tiers continues to evolve. In addition, the resource constraints from sequestration of DoD funds resulted in fewer and smaller exercises in FY13, constraining the ability of DOT&E assessment teams to observe and assess network defenses.

Most FY13 assessments were at smaller venues and only included the lower tiers of computer network defense. As the Department continues to migrate to more centralized and enterprise network and cybersecurity management models, the majority of key network defense activities are now performed by the upper tier commands, such as the CNDSPs, the Service Cyber Component Commands, or U.S. Cyber Command (USCYBERCOM). Therefore, the focus in FY13 was principally toward local/proactive defenses (standards compliance, patch management, vulnerability management) and not the reactive (detection, remediation) activities conducted at higher layers of network defense. The FY13 assessments were focused on the lower tier defenses, and it was clear that local network (proactive) defenses were insufficient to counter the portrayed cyber adversaries. To be more realistic and effective for both training and assessment, future events should include the upper tier cybersecurity services.

Three of the FY13 assessments explored new approaches for cybersecurity assessments without a training exercise venue: an extended Theater Cyber Readiness Campaign assessment at U.S. European Command and a Cyber Key Terrain methodology assessment at U.S. Africa Command and U.S. Central Command. These assessments were intended to develop consistent assessment approaches for normal operating conditions that would not depend on a scheduled exercise to perform or necessitate harmful effects to operations and networks.

Capability Assessment

While compliance with key cybersecurity standards continued to improve in FY13, assessment teams observed that good fundamental network maintenance, while necessary, was not sufficient to fully protect DoD networks and systems. Local network defenses are insufficient to protect against a determined or well-resourced cyber adversary and warfighter missions should be considered "at moderate to high risk" until they can be demonstrated to be resilient in a contested cyber environment.

Assessments continued to identify the risks posed to operational missions from cyber events, primarily affecting information intensive missions of commanding and controlling forces. The primary mission effects encountered in assessments involved degradations to operational security from compromise of information. IOP problems affecting missions were largely due to the inherent costs associated with the workarounds devised to exchange needed information when automation failed--these costs include the additional personnel and workload required, errors introduced during manual transcriptions, and delays in mission tasks. The risks to operational missions were generally moderate to high when considering the expected severity of the operational effects and the likelihood from portrayed cyber threats, and were generally low when IOP problems were encountered.

Overall, compliance with network standards continues to improve in almost every key area reflecting the continuing efforts across the DoD to implement cybersecurity policies and procedures. Compliance determines whether network defensive measures are in place; however, the observed defensive performance against portrayed threats confirms that these measures can be defeated. Red Teams increasingly circumvented network defenses using default or stolen credentials despite improved compliance with identity management policies. The asymmetric nature of cyber operations permits even a single default or discovered password to lead to rapid exploitation of the network. Further, Red Teams continued to encounter systems with known vulnerabilities that remained unpatched and improper configurations that permitted relatively easy paths for exploitation.

Some fundamental problems appear to be improving. Exercise adversary teams found fewer default or poorly selected passwords, but stolen and default credentials were a principal pathway to intrusion and exploitation activities. Additionally, key network infrastructure components, such as domain controllers, web servers, and printers remained focus areas for surveillance and possible exploitation, often because these components have inconsistent configuration management. Analysis of cybersecurity acquisition testing in FY13 (conducted separate from these exercise assessments) also shows a large body of cybersecurity vulnerabilities, the majority of which derive from either password and software configuration management, missing patches, or network vulnerabilities of systems under test. Many of these fundamental problems go undiscovered until operational testing is conducted late in the acquisition cycle, or discovered during normal fielded operations (such as these exercise assessments).

The Red Teams and CCMD exercise planners emphasized realistically portrayed cyber-adversary activities, but continued to restrict activities needed to create contested conditions that include adversely affecting network resources or mission processes. FY13 assessments increasingly noted that improvements in portrayed threat realism have not been matched by improvements in network defense realism (specifically, the inclusion of upper-tier defensive capabilities).

Assessments of CCMD exercises continue to find a more balanced mix of experience levels for network defenders, but Service exercises remain heavily biased towards lower-skilled personnel. Figure 4 shows the distribution of personnel with beginner, intermediate, and expert skillsets. The difference between the distribution of skill levels at the CCMDs and within the Services likely reflects both the skill and experience requirements levied for assignment of Service personnel to joint tours, and the higher levels of contract support at the CCMD headquarters.

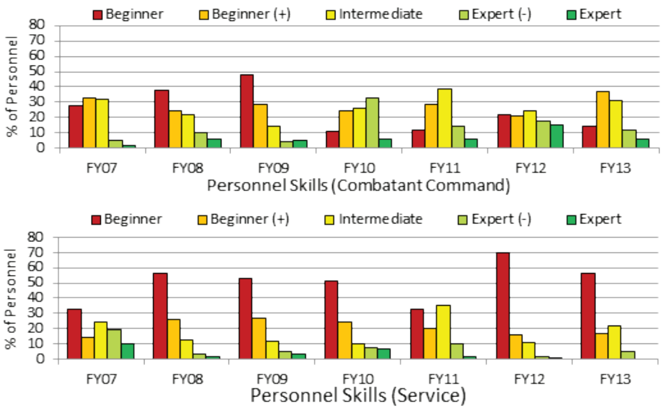

Figure 4: Personnel Skill Levels

Host Base Security System (HBSS) is intended to provide key monitoring and automated reporting support to the future JIE and continuous monitoring solutions for DoD, but in-depth reviews of HBSS in FY12 and FY13 found that a number of problems remain to be resolved with HBSS, including:

- Inconsistencies in the asset management inventories, apparently caused by common configuration errors and hardware. These errors could be exploited to bypass HBSS protections.
- Incomplete or inconsistent information provided by analysis tools to support the investigation of some errors and failed actions. Query tools are also difficult to use.
- Misunderstood system setup rules and interfaces caused by configuration errors.
- Intrusion protection rules that are difficult to access or understand.

Little Interoperability data were gathered in FY13 due to the reduced opportunities for exercise assessments. In those assessments conducted, however, Interoperability issues were noted ranging from minor (e.g., systems freezing but easily rebooted with little-to-no loss of data exchange but minor processing delays) to moderate (e.g., two fires coordination systems locked up due to data transfer backlogs requiring operators to shift to voice communications which took three to five times longer to accomplish). In each case, local operators had developed workarounds, which, while effective in completing the mission tasks, required extra time, extra workload, and personnel, and introduced errors that would not have occurred had the automated data transfers worked properly. Less than one third of all fielded systems observed in assessments over the past five years have had current Interoperability certifications. Given the generally effective interoperation of the systems assessed, both certified and uncertified, it is clear that the Interoperability certification process provided little to no confidence in system readiness and has not eliminated the need for such workarounds.

INFRASTRUCTURE

DOT&E conducted a variety of events to demonstrate and stress the capabilities of the National Cyber Range with support from other ranges and assets to include the Joint Cyberspace Operations Range, the DoD IA Range, Sandia National Laboratories, U.S. Pacific Command/J81, and the Threat Systems Management Office. These events also provided insights on how a DoD Enterprise Cyber Range Environment (ECRE) might work and enabled development of specific environments as part of the ECRE.

The ECRE development effort is a DOT&E-led partnership to build representative mission environments where Red Teams can conduct attacks and demonstrate effects not permitted on operational networks and systems. These environments will be available via the DoD ECRE for use during exercises and in pre- and post-exercise events to demonstrate cyber effects, develop cyber playbooks, and enhance cyber tactics, techniques, and procedures. Each ECRE environment under development was motivated by an earlier exercise assessment where Red Team activities were restricted by operational or training limitations.

The first such environment, ECRE-Command, Control, and Intelligence Systems (C2IS), in development by the Joint Staff J6's Command, Control, Communications, and Computers (C4) Assessment Division, involves the common operating picture and supporting situational awareness systems. The ECRE-C2IS Team completed several phases of risk-reduction activities during late FY13, including integration of a Joint Information Operations Range (JIOR) node to support distributed Red Team and assessment activities. Preliminary events with Red Teams were also executed, providing the first look at the potential effects that a cyber adversary could deliver to the networks and systems of this critical mission area. ECRE-C2IS will support the assessment of the USNORTHCOM exercise Vigilant Shield 2014 in October 2013.

The second environment, ECRE-Command and Control, Battle Management, and Communications (C2BMC), is composed of the command and control elements of the Ballistic Missile Defense System. ECRE-C2BMC capabilities will be provided by the Missile Defense Agency, with augmentation of JIOR nodes. Planning is underway for risk-reduction activities and active Red Teaming. Activities in the missile defense mission area were part of the FY13 U.S. European Command Theater Cyber Readiness Campaign assessment, and ECRE-C2BMC will support follow-on events in FY14.

The third environment, ECRE-AEGIS, focuses on the Aegis Combat Systems and will be developed in four "spirals" or phases during FY14. Collaboration with the Navy Red Team, Wallops Island and Dahlgren test facilities, and Combat Direction Systems Activity Dam Neck began in 4QFY13. Phase 1 activities were conducted in August 2013 and included successful proof-of-concept testing by the Navy Red Team. Phase 2 activities are planned in 1QFY14 to generate initial results regarding the scope and duration of cyber effects. ECRE-AEGIS is expected to support several CCMD assessments in FY14.

Additional ECRE environments are under consideration that will provide realistic data regarding the scope and duration of impacts on critical missions due to cyber attacks. Nonetheless, the management and resourcing of DoD ECRE remains fragmented and inefficient. DOT&E strongly recommends management and resourcing be brought under an Executive Agent.

PARTNERSHIPS AND COORDINATION

DOT&E continued the long-standing partnerships with the Joint Staff and DoD Chief Information Officer (CIO) on the oversight and coordination of the IA and IOP Assessment Program. Metrics and observations generated from these assessments are provided to the DoD CIO for use in enterprise-wide IA assessments and programs. DOT&E coordinates efforts with USD(AT&L), Developmental Test and Evaluation (DT&E) in matters of test and evaluation for acquisition and development of information handling systems. Together with AT&L, DOT&E is reviewing and revising the existing guidelines for cybersecurity testing of acquisition programs. The revised process, once approved, will allow for earlier development of cybersecurity test strategies that are better focused on the operational role of the system under test. This will be accomplished by examining system requirements and intended mission environments early in development and designing developmental and operational tests that cumulatively examine the system.

DOT&E is establishing a standing working group with USCYBERCOM and the National Security Agency to develop and synchronize priorities for Cyber Opposing Force missions consistent with the USCYBERCOM Exercise Support Plan, the Chairman of the Joint Chiefs of Staff training guidance, and DOT&E's CCMD and Service assessment schedule. This group will work to ensure a Cyber Opposing Force has timely ground rules in place for their operations, detailed cyber threat information, and the training and resources to portray representative cyber adversaries. In addition, the working group will track significant vulnerabilities, recommend priorities for development of cyber range environments, and oversee persistent access to the DoD information networks for cyber test teams.

DOT&E worked closely with many members of the intelligence community to improve both the scheduling and portrayal of the representative cyber threats during FY13 exercises. The Defense Intelligence Agency continued to enhance realism during these exercises by helping to write representative cyber threat scenarios and coordinating with Red Teams to ensure they knew adversarial practices and could apply them against DoD networks for training. The Defense Intelligence Agency team, in coordination with other intelligence community members, is building detailed cyber-adversary threat folders to improve overall understanding and portrayal of adversary capabilities.

Recognizing that not all adversary actions and effects are suitable for conduct on live networks, DOT&E continues to support the development of methods and environments to exercise and assess advanced actions on appropriate closed-loop cyber ranges. Cyber ranges such as the DoD JIOR were used in four assessed exercise venues and emphasis will continue for increasing the integration and operational realism of JIOR events associated with assessments in FY14. DOT&E also conducted a variety of events in FY13 to demonstrate and stress the capabilities of the National Cyber Range that included participation of several other cyber range capabilities. The National Cyber Range is now accredited to all classification levels required to support OT&E. The use of other ranges, including the Defense IA Range, and expanded range tools such as persistent range environments is also supported by DOT&E.

DOT&E and the Test Resources Management Center used funding targeted for cyber enhancements to develop advanced cyber-threat assessments, improve the capabilities of cyber Red Teams so they can emulate the advanced threats, develop range environments to demonstrate advanced cyber effects, and create a team of cyber/range/test and evaluation experts to plan and execute rigorous cyber-range events. The Test Resource Management Center's resources are being applied to field the next-generation Regional Service Delivery Points for the JIOR; improvements to traffic generation, instrumentation, and visualization capabilities; creation of persistent cyber environments, and incorporation of Live-Virtual-Constructive capabilities into the cyber ranges. DOT&E has already seen early effects of these improvements, which will be reported on fully in the FY14 DOT&E Annual Report.

DOT&E, in partnership with the Naval Postgraduate School, supports research for improved tools for testing and assessing cybersecurity. Thus far, this has led to the design and development of network test tools, which simulate intrusion and malware symptoms; validation of this tool as a training asset for network operators; and the ongoing development of cause/effect models for use in network event simulations.

REPORTS

Each assessment provided a specific report for the exercise authority (CCMD or Service) detailing results and observations including discovered vulnerabilities. DOT&E provided additional direct feedback to the exercise authorities for problems of high priority. In addition to these exercise assessment reports, DOT&E published six memoranda of findings and initiated research of three additional areas of concern in FY13. Finding memoranda detail specific shortfalls and vulnerabilities that have the potential to significantly degrade operations and warrant senior leadership attention. Shortfalls and vulnerabilities were identified to the responsible leadership and replies were provided to DOT&E detailing mitigation efforts, which then are subject to subsequent re-evaluation and validation in future assessments. During the fiscal year, solutions to prior findings were reviewed or validated in the field where observable.

New findings released in FY13:

- HBSS (released October 2012) – documented discrepancies in the operation of the asset management functions. Response received from the Defense Information Systems Agency.
- Unsecured Chat Capabilities (released October 2012) – documented the use of unsecure collaboration tools in DoD. Awaiting JCS response.
- Network Access Controls (released November 2012) – investigated the use of commonly available devices to compromise DoD networks. Response received from DoD CIO.
- Identity and Access Management (released January 2013) – documented frequently encountered problems with the use of credentials on DoD networks. Response received from USSTRATCOM.
- Adaptive Network Defense (released January 2013) – documented the completion of a joint test at USPACOM to implement a rapidly-deployed virtual secure enclave capability to protect key data and components. Response received from JCS.
- Assessment of DoD IA during Major CCMD and Service Exercises (published April 2013) – documented a detailed follow-up to the April 2012 report of the same title, and addressed classified issues identified in FY12. Response received from DoD CIO.

New research initiated in FY13:

- Defense Connect Online (initiated April 2013) – investigating new vulnerabilities in DoD collaboration tools.
- HBSS (initiated June 2013) – investigating new issues discovered with the use of HBSS on DoD networks.
- Shipboard Systems (initiated July 2012, re-initiated July 2013) – validating original findings and remediations were put into place as a result of research into potential vulnerabilities to afloat systems.

FY14 GOALS AND PLANS

For FY14, the goal of the DOT&E IA and IOP Assessment Program is to complete at least one full assessment of each CCMD and Service. A full assessment is a holistic cybersecurity assessment (IA and IOP components) with the associated mission assurance analysis that focuses on the ability of the training audience to execute critical missions in denied, manipulated, or contested cyber conditions. The FY14 Program has 12 CCMD assessments, 5 Service assessments, and 3 observation-only assessments (See Table 2). The observation-only assessments evaluate specific exercises as potential venues for FY15 and beyond assessments.

For FY14, the goals of DOT&E cybersecurity operational test and evaluation are:

- Update procedures for operational testing to improve the DoD's ability to identify and resolve issues earlier in system development and testing
- Portray representative cyber threats to determine resilience of tested systems

The FY14 detailed plans for DOT&E efforts in cybersecurity operational test and evaluation, and field assessments include:

- Full implementation of the CJCS EXORD (and/or applicable follow-on instructions) to provide training opportunities for CCMDs and Services to execute critical missions in denied, manipulated, or contested cyber conditions.
- Improved realism of the cyber threat levels and effects portrayed during all tests and assessments.
- Increased coordination with USCYBERCOM in scheduling and synchronizing requirements for certified and accredited Red Team assets in support of approved CCMD and Service assessments.
- Improved data collection methodologies to enhance the end-to-end analysis of Cyber Opposing Force activities.
- Expanded capability of DoD JIOR and other cyber range facilities to support field assessments, training events, and tests.
- Implementation of a process to track remediation and verification of corrections for discovered vulnerabilities and shortfalls identified during CCMD and Service assessments.
- Increased completeness of the portrayed DoD cybersecurity defensive capabilities in field assessments and tests by improving participation of upper Tier computer network defense service providers.

TABLE 2. INFORMATION ASSURANCE AND INTEROPERABILITY EXERCISE EVENTS PROPOSED FOR FY14

EXERCISE AUTHORITY	EXERCISE	ASSIGNMENT AGENCY
U.S. Africa Command	Epic Guardian 2014	ATEC
U.S. Central Command	AOR Site Assessment – Special Operations	ATEC
	Internal Look 2014	ATEC
U.S. Cyber Command	Cyber Flag 2014	ATEC
U.S. European Command	EUCOM Theater Cyber Readiness Campaign 2014	ATEC
North American Aerospace Defense Command/U.S. Northern Command	Vigilant Shield 2013	AFOTEC
U.S. Pacific Command	Tempest Wind 2014	COTF
U.S. Special Operations Command	Tempest Wind 2014	ATEC
U.S. Southern Command	JIATF-South Assessment	ATEC
U.S. Strategic Command	Global Lightning 2014	JITC
	Global Thunder 2014	JITC
	Gypsy Juliet 2014 (Observation only)	JITC
U.S. Transportation Command	Turbo Challenge 2014	JITC
U.S. Army	Warfighter Exercise 2014-4	ATEC
U.S. Navy	Valiant Shield 2014	COTF
U.S. Air Force	Ulchi Freedom Guardian 2014 (7th Air Force)	AFOTEC
	Green Flag 2014 (Observation only)	AFOTEC
	Red Flag 2014 (Observation only)	AFOTEC
U.S. Marine Corps	Ulchi Freedom Guardian 2014 (III MEF)	MCOTEA
	Large Scale Exercise 2014 (I MEF)	MCOTEA

AOR – Area of Responsibility AFOTEC – Air Force Operational Test and Evaluation Center ATEC – Army Test and Evaluation Command
COTF – Commander, Operational Test and Evaluation Force JITC – Joint Interoperability Test Command MEF – Marine Expeditionary Force
MCOTEA – Marine Corps Operational Test and Evaluation Activity