Information Assurance (IA) and Interoperability (IOP)

In FY12, the DOT&E Information Assurance (IA) and Interoperability (IOP) Assessment Program performed 20 assessments during Combatant Command (CCMD) and Service-level exercises or real-world activities; 3 of these assessments involved units deployed to the U.S. Central Command (USCENTCOM) area of responsibility. The IA/IOP program conducted reduced-scale assessments at U.S. European Command (USEUCOM) and U.S. Africa Command (USAFRICOM) after their scheduled exercises were cancelled in response to actual operational contingencies. Six individual test and evaluation organizations conducted these assessments, which involved all 10 of the CCMDs and all 4 Services. During the year, DOT&E released five major findings reports, and initiated another nine, pertaining to both IA and IOP. Exercise planners in FY12 made increased use of cyber ranges in support of these exercises.

Summary of Findings

Most exercise assessments and tests involved operations largely against low- and mid-level cyber threats and on networks that were only moderately stressed in terms of loading or network degradation; high-level threats were portrayed infrequently. No exercises were seriously disrupted by adversary activities, or disrupted at any length, because adversary teams were generally not permitted to take actions that could disrupt exercises. In the cases where the adversary team portrayed higher-level threats, exercise training audiences frequently misinterpreted these portrayals as maintenance issues, poor system performance, or anomalies.

Overall, the DOT&E IA/IOP program observed cyber effects caused by unresolved interoperability deficiencies, coupled with low-to-moderate level threats that were sufficient to adversely affect the quality and security of mission critical information in a way that could (and where permitted did) degrade mission accomplishment significantly. Therefore, considering both IA and IOP attributes, the Department has not yet developed sufficiently advanced cyber defensive tactics to counter advanced adversary tactics and to consistently operate in degraded cyber environments.

Interoperability: The FY12 IOP assessments documented interoperability problems involving mission critical systems, but these problems hindered rather than prevented mission accomplishment. This is due primarily to system operators who developed workarounds to preserve the critical mission functions. Even though operators accomplished their missions, the workarounds usually increased operator workload, and often degraded efficiency in completing mission tasks. The assessment teams documented effects on the timeliness, accuracy, and efficiency of operational data handling. Operators frequently viewed interoperability problems as maintenance or design issues and therefore did not report, document, or remediate many of these problems. The majority of systems encountered during assessments were not certified for interoperability.

Information Assurance: The overall IA performance observed during the FY12 exercise assessments remains insufficient to prevent and consistently detect compromise and exploitation of the networks exercised. Although regularly able to penetrate and exploit networks, Red Teams reported modest increases in the required level of effort over previous years. While compliance with network standards continues to improve, the IA/IOP program continued to provide low ratings for certain critical compliance areas. In addition, development of the more sophisticated tactics and procedures necessary to counter a determined or well-resourced cyber adversary remains slow. In exercises involving portrayal of more sophisticated threat profiles, the training audiences usually lacked commensurate defensive tactics. Overall, the implementation of Joint Staff guidance on exercise realism has been slow. Network boundary defenses continued to improve in FY12, to include the presence of host-based intrusion detection tools, improved configuration management of networks and security tools, and the infrastructure supporting the networks. In at least one exercise, good network "housekeeping" effectively deterred adversary efforts. However, DOT&E observed reduced rates of compliance in the use of software and hardware backups; and key practices such as port-and-protocol protections, reliable software baselines, remediation of known vulnerabilities, and effective use of system audit logs.

Partnerships and Coordination

DOT&E continued a number of partnerships directly related to the conduct of IA/IOP assessments. These included:

- Collaborating with the Joint Staff and DoD Deputy Chief Information Officer (CIO) concerning oversight and coordination of the IA and IOP Assessment Program. DOT&E provides metrics and observations generated from these assessments to the DoD CIO for use in enterprise-wide IA assessments and programs.
- Coordinating program efforts with USD(AT&L) and Developmental Test and Evaluation (DT&E) as a means of supporting the acquisition and development of information handling systems.
- Creating a standing memorandum of understanding between DOT&E and U.S. Cyber Command (USCYBERCOM) that directs the establishment and operation of the Cyber Assessment Synchronization Working Group (CASWG), as well as information exchange and collaboration in a variety of areas of interest. The CASWG is developing processes to synchronize planning, execution, and reporting among all cyber assessment activities, and especially those supporting exercise assessments.
- Sharing of information and expertise with the Joint Staff's Joint Deployable Analysis Team continues to enhance assessments.

The partnership collaborated to conduct two assessments in FY12, and further joint assessments are planned for FY13.
- Collaborating with the intelligence community, the National Security Agency, and the Service Information Warfare centers to improve the portrayal of the representative cyber threats during exercises. The Defense Intelligence Agency (DIA) made significant progress in defining advanced and emerging methods of cyber attack, and was instrumental in mapping known adversary activities to the threat portrayals for several FY12 exercises.
- Working with the Naval Postgraduate School to research and develop improved capabilities for network analyses. This partnership includes the design and development of network test tools; instrumentation; training resources and test/evaluation methods; analysis of compliance and performance findings to postulate cause/effect models for use in simulation; and mapping of direct operational effects arising from network performance issues.
- Coordinating with the Defense Information Systems Agency (DISA) to improve and expand the assistance and training available to assessed organizations, including the implementation of a cyber-defense training and assessment suite at several CCMDs.

FY12 ACTIVITIES

In FY12, the six assessing organizations were the Army Test and Evaluation Command; the Navy's Commander, Operational Test and Evaluation Force; the Marine Corps Operational Test and Evaluation Activity; the Joint Interoperability Test Command; the Air Force Operational Test and Evaluation Center; and the Air Force 688th Information Operations Wing. These 6 assessing organizations completed 20 exercises or site assessments under the IA and IOP Assessment Program, and 2 reduced scope assessments at sites where exercise activity was either curtailed or cancelled. These assessments included 13 CCMD and 6 Service exercise assessments (see Table 1). Three assessments involved units deployed in the USCENTCOM area of responsibility.

TABLE 1. INFORMATION ASSURANCE AND INTEROPERABILITY EXERCISE EVENTS IN FY12

EXERCISE AUTHORITY	EXERCISE	ASSESSMENT AGENCY
U.S. Africa Command	Judicious Response 2012 (Exercise Cancelled)	ATEC
U.S. Central Command	AOR Site Assessment #1	ATEC
	AOR Site Assessment #2	ATEC
	AOR Site Assessment #3	ATEC
U.S. Cyber Command	Cyber Flag 2012	ATEC
U.S. European Command	Austere Challenge (Exercise Cancelled)	ATEC
North American Aerospace Defense Command / U.S. Northern Command	Vigilant Shield 2012	688 IOW
	Ardent Sentry 2012	688 IOW & AFOTEC
	Vibrant Response 2012	JITC
U.S. Pacific Command	Terminal Fury 2012	COTF
U.S. Southern Command	PANAMAX 2012	ATEC
U.S. Special Operations Command	Emerald Warrior 2012	ATEC
U.S. Strategic Command	Global Lightning 2012	JITC
U.S. Transportation Command	Assessment During Operations	JITC
U.S. Forces Korea	Key Resolve 2012	ATEC
	Ulchi Freedom Guardian 2012	ATEC
U.S. Army	Full Scope Exercise 2012-4	ATEC
U.S. Navy	Bold Alligator 2012	COTF
U.S. Air Force	Angel Thunder 2012	JITC
	Red Flag 2012-3	688 IOW
U.S. Marine Corps	Ulchi Freedom Guardian 2012 (III MEF)	MCOTEA
	Bold Alligator 2012	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 IOW – Information Operations Wing JITC – Joint Interoperability Test Command
MCOTEA – Marine Corps Operational Test and Evaluation Activity MEF – Marine Expeditionary Force

Several developments in FY12 confirm increasing emphasis across the DoD to prepare to train and operate in a contested cyberspace environment. The Chairman, Joint Chiefs of Staff (CJCS) is preparing additional guidance to amplify the Execute Order (EXORD) issued in FY11 to increase realistic cyberspace conditions in training exercises. Threat portrayal improved during assessed training exercises but with limited progress made towards implementing EXORD requirements. The overall number of instances in which exercise commanders permitted cyber effects to disrupt operations increased, as did the number of sites where these effects were demonstrated; however, the overall effect remains low due to constraints imposed upon Red Teams.

The Defense Intelligence Agency (DIA) Cyber Threat Assessment (CTA) Office continued to make significant progress in defining advanced and emerging methods of cyber attack, and was instrumental in mapping known adversary activities to the threat portrayals for several FY12 exercises. For example, CTA threat assessments for U.S. Pacific Command's (USPACOM) Terminal Fury 2012 contributed to an integrated Red Team employing multiple attack vectors, an opposing force (OPFOR) with a cyber cell that controlled the Red Team and received exfiltrated information, and some of the most realistic cyber play observed to date in an exercise. CTA also has developed a method to assess the shortfalls between the postulated threat and the threat that was actually present in training, which will be a key metric for evaluating implementation of the CJCS EXORD.

To enhance the IA posture of acquisition programs, DOT&E continued to revise and refine the templates and process for assessing the adequacy of IA testing in acquisition Test and Evaluation Master Plans and test plans. These templates facilitate development and review of these documents to ensure that IA is adequately addressed. DOT&E applied the templates and new process to the Test and Evaluation Master Plans for 34 systems, the operational test plans of 13 systems, and related test documents of 8 systems. Additionally, DOT&E IA experts specifically observed IA tests and reviewed data for the following three systems after previously reviewing test documentation:

- Patriot Missile (PAC-3)
- U.S. Navy dry cargo ship (T-AKE)
- U.S. Army Apache Block III helicopter

FINDINGS, TRENDS, AND ANALYSIS

Interoperability

The FY12 assessments found that interoperability issues encountered by the exercise training audience largely hindered, but ultimately did not prevent mission accomplishment. This was primarily because operators developed and executed effective workarounds. The workarounds increased operator workload, and often degraded the efficiency of completing tasks, or degraded timeliness and accuracy of the information generated.

Operators frequently view interoperability problems within systems architectures as maintenance or design issues beyond the control of local authorities. Therefore, many of these problems are not reported, documented, or remediated. More often, local users will develop practices and techniques to work around the lack of a desired/designed automated function. Workarounds include such techniques as:

- Manual transcription of data from one system to another, introducing transcription errors
- Data transfer between systems via portable media, thereby opening both systems to outside malware intrusion
- System re-boot/re-set to trigger update routines, usually resulting in increased delay and latency of operational data

System-to-system interoperability problems remain largely unreported. Over the last two years, slightly less than one-quarter of all systems observed during exercise assessments had been fully certified for interoperability. Of those systems, only two-fifths have ever been previously certified, indicating that almost half of the exercise systems have lapsed in certification or been replaced by uncertified software versions. Configuration management and documentation of observed systems (certified or not) were reported by the system operators to the operational test observers as satisfactory for 9 of every 10 systems. Operators cited system reliability as a problem in almost one-third of all systems reviewed in FY12, an increase over previous years. Several of the findings either reported or under research by DOT&E involve interoperability shortfalls, including:

- AOC Interoperability – software baseline and interoperability certification in the Air and Space Operations Centers lacks centralized configuration management and control. As a result, the Air and Space Operations Centers do not have standard software, and frequently employ locally-produced middleware to accommodate system-to-system interoperation. Furthermore, the version of the Global Command and Control System (GCCS) in use at all of the AOCs had not been fully tested or certified for operational use. (Note: since the release of this finding, the testing and certification of the most recent update for GCCS-Joint is in progress, which includes AOC operational support.)
- Third Party Patching – DoD uses a large number of commercial software suites, ranging from the baseline Windows® Operating System on most desktop computers, Adobe file readers, JAVA script, and other commonly available commercial administrative and business software. DoD does not have a means of central management for updates to these commercial applications, requiring local network authorities to download commercial patches and updates, test, and implement them individually.
- Surveillance Radar Systems – A wide-area surveillance radar system observed during one exercise was found to potentially allow control of the sensor from multiple workstations/roles/accounts within the command and control software that accesses the radar – essentially preventing a stable configuration during operations.

Information Assurance

Red Teams reported increased difficulty in penetrating network defenses; however, results show that with sufficient time, Red Teams routinely penetrated networks and systems with few exceptions. Detection rates of network intrusions remained low, and the ability of network defenders to detect subsequent exploitations of information was minimal.

The CJCS EXORD of February 2011 to Incorporate Realistic Cyberspace Conditions into Major DoD Exercises directs more realistic cyber adversary portrayals in all major CCMD and Service-level exercises. There is little evidence that the milestones cited in the EXORD (such as identification of critical mission tasks and systems) have been completed.

The level of threats portrayed in assessed exercises in FY12 (see Figure 1) remained similar to previous years, with a modest increase in both high-level portrayals and exercises in which no threat was portrayed (usually onsite/non-exercise assessments without Red Teams). While exercise commanders permitted degraded network operations on almost twice as many unclassified network sites than the previous year, the instances of degraded performance on classified networks declined slightly. In FY12, a quarter of all Red Team activities were directly disruptive to networks assessed, a step forward in the implementation of the EXORD guidance. However, in cases where adversary teams portrayed higher-level threats, exercise training audiences were unable to either develop or demonstrate advanced mitigation or tactics in the face of these threats. As a result, the exercise participants' defensive actions were not well-matched to the threats portrayed, and sometimes exacerbated the negative effects of the cyber threat.

Figure 1: Distribution of Threat Depictions

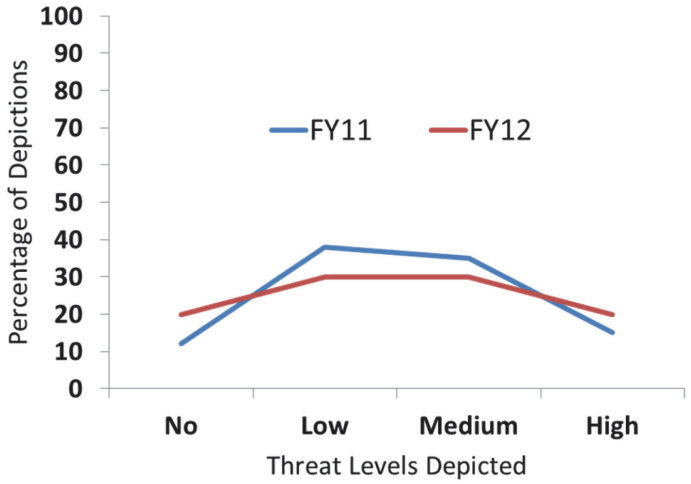

Figure 1: Distribution of threat portrayals in assessed exercises. The majority of threats portrayed in FY12 were low-to-medium capability, and occurred less often than in FY11. A modest increase in high-level threat portrayals was seen at a limited number of exercise sites.

Exercise personnel at times misinterpreted the cyber effects from these more aggressive and disruptive threat portrayals as arising from non-adversary causes such as maintenance shortfalls, system performance problems, or even as artificialities within the exercise construct. As a result, exercise participants either ignored or otherwise did not report significant network events, essentially denying network defenders and leadership critical knowledge of the network status. Additionally, exercise participants perceived the attribution process (confirm whether Red Teams caused the effect) as cumbersome and slow, and in several cases, simply ignored this process, further detracting from the ability to develop a concise and accurate view of the networks under observation.

Most network compliance attributes continue to gradually improve, indicating greater compliance with basic standards (see Figure 2). Network boundary defense compliance continued to improve, including the presence of host-based intrusion detection tools, improved configuration management of networks and security tools, and the overall infrastructure supporting the operational networks. Physical environment, enclave boundary protections, and incident management is improving. The effective use of host-based intrusion detection systems, for example, is increasing.

The ongoing fielding of the Host-Based Security System (HBSS) is improving compliance with having local network protection and intrusion detection; however, the majority of HBSS suites DOT&E observed were found to be incorrectly or ineffectively configured. Enforcement of configuration standards; the deliberate planning for incident responses; and critical network infrastructure practices to include having backup components, supplies, and spares continue to improve. In at least one assessment, a strict enforcement of these basic network requirements resulted in measurably reduced Red Team success. Efforts are also underway at selected CCMDs to document and develop Computer Network Defense playbooks as training and operational tools.

Figure 2: Site Compliance

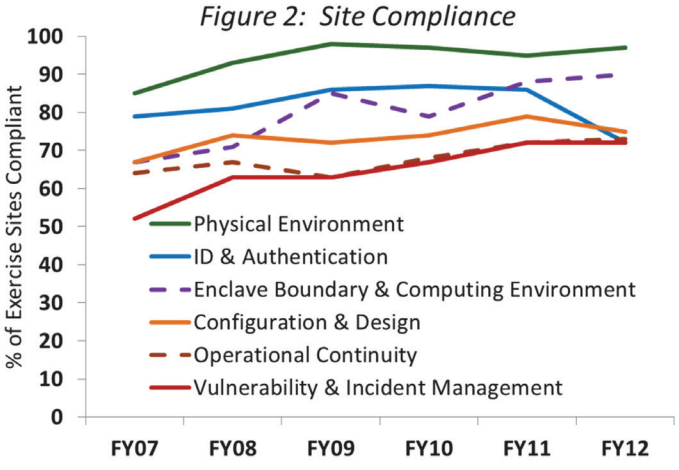

Figure 2: Six-year trend in compliance standards as measured during exercise assessments. Physical environment and enclave protection standards have improved steadily since FY07, but progress in operational network continuity, configuration and design standards, and vulnerability/incident management remain gradual.

DOT&E observed reduced rates of compliance in the use of software and hardware backups and key practices such as port and protocol protections, reliable software baselines, remediation of known vulnerabilities, and effective use of system audit logs. Exercise authorities rarely shift to alternate sites or systems. Most audit logs did not meet the minimum requirements specified, and the identification and remediation of known vulnerabilities has also declined over the last two years. DOT&E also observed that the experience and formal training levels for network defenders, which increased steadily over the last three years, showed a large influx of new or inexperienced personnel in FY12.

Mission Assurance

During the FY12 assessments, the operational testers analyzed the IA and IOP findings to characterize the operational effects, or potential operational effects, on specific missions. Although cyber-adversary activities posed a high risk to critical operations, exercise authorities seldom permitted disruptions to be fully exercised; the priority to achieve other exercise training objectives remains at odds with exercising in an environment with representative cyber adversaries and consequently degraded systems. In those exercises where operational effects were permitted, the mission impacts included:

- Disclosure of friendly force locations and activities to the opposition force, resulting in fewer adversary losses
- Denial of critical network capabilities during periods of high operational tempo
- Delays in the delivery of operational data

Despite the few permitted and observable impacts to actual missions, DOT&E analysis of the vulnerabilities, intrusions, and compliance trends clearly indicates high-risk to operational tasks and Combatant Commander operational missions. DOT&E analysis indicates that without the development of defensive tactics commensurate with the sophistication of our adversaries, large-scale compromise or loss of operational data and operational systems during high-tempo operations cannot be discounted.

REPORTS

Each of these assessments resulted in a specific report for the Exercise Authority (CCMD or Service) detailing problems found during the exercise and detailed observations and recommendations. In addition to these, DOT&E published five memoranda of findings and initiated research on nine additional areas of concern in FY12. Finding memoranda detail specific shortfalls and vulnerabilities that have the potential to significantly degrade operations and warrant senior leadership attention. DOT&E identified the shortfalls and vulnerabilities to the responsible leadership. Service and CCMDs provided replies to DOT&E detailing mitigation efforts, which then are subject to subsequent re-evaluation and validation in future assessments. During the fiscal year, where observable, DOT&E reviewed or validated in the field solutions to prior findings. New findings released or researched in FY12 are listed below.

Released in FY12:

- Air Operations Center (AOC) Interoperability (released November 2011) – documented the lack of a consistent software baseline and interoperability certification in the Air and Space Operations Centers
- Virtual Secure Enclaves (released December 2011) – documented a promising network security experiment at USPACOM
- Third Party Patching (released January 2012) – documented a lack of central management for security patches on commercial software in use within DoD networks
- Active Directory Pass-the-Hash (released March 2012) – documented a classified investigation into a common hacker technique
- Assessment of DoD IA during Major CCMD and Service Exercises (published April 2012) – documented a detailed follow-up to the FY11 Annual Report, specifically addressing classified IA issues

Research Initiated in FY12:

- HBSS discrepancies in asset management (initiated March 2012 and released October 2012) – investigating a potential common misconfiguration of the system that causes inaccurate or inconsistent results
- Event attribution (initiated May 2012) – investigating the manner in which events detected during an exercise are attributed to either Red Team activity or actual cyber incidents
- Shipboard Systems (initiated July 2012) – investigating a possible vulnerability to afloat systems
- Physical Intrusion Devices (initiated July 2012) – investigating the use of a commonly available hacker tool
- Password shortfalls (initiated July 2012) – investigating common password errors exploited by Red Teams
- Unsecured chat systems (initiated July 2012) – investigating the operational effects of using collaboration tools that can be easily intruded/exploited
- Phishing and misuse of secure socket technology (initiated July 2012) – investigating the operational effects of two common hacker techniques
- Physical Security (initiated July 2012) – investigating multiple instances and causes of failures to physically protect network resources and points of access
- Surveillance Radar Systems (initiated September 2012) – documenting a possible control-of-radar interoperability problem

FY13 PLANS AND GOALS

DOT&E's goal is to complete at least one IOP and one IA assessment of each CCMD and Service during the fiscal year, with 15 CCMD and Service exercises already identified for FY13 (see Table 2). One of the planned FY13 assessments will involve units already deployed to the U. S. Central Command (USCENTCOM) areas.

The FY13 IA/IOP Assessment Program will focus on the following goals:

- Supporting and monitoring the three-year implementation of the CJCS EXORD, and continuing to improve the realism of portrayed cyber threats during assessments
- Developing and implementing additional improvements to the methods for gathering and assessing the effects on operational missions
- Increasing coordination with USCYBERCOM, DISA, DoD CIO, and other agencies in the scheduling and conduct of assessments
- Continuing to expand the use of the DoD Joint Information Operations Range (JIOR) and other range/test facilities in support of exercise assessments
- Continuing to refine the mission assurance analysis afforded by the IA and IOP findings

TABLE 2. INFORMATION ASSURANCE AND INTEROPERABILITY EXERCISE EVENTS PROPOSED FOR FY13

EXERCISE AUTHORITY	EXERCISE	ASSIGNMENT AGENCY
U.S. Africa Command	Judicious Response 2013	ATEC
U.S. Central Command	AOR Site Assessment	ATEC
	Internal Look 2013	ATEC
U.S. Cyber Command	Cyber Flag 2013	ATEC
U.S. European Command	AOR Site Assessment	ATEC
North American Aerospace Defense Command / U.S. Northern Command	Vigilant Shield 2013	AFOTEC
U.S. Pacific Command	Terminal Fury 2013	COTF
U.S. Southern Command	Integrated Advance 2013	ATEC
U.S. Special Operations Command	Emerald Warrior 2013	ATEC
U.S. Strategic Command	Global Lightning 2013	JITC
U.S. Transportation Command	Turbo Challenge 2013	JITC
U.S. Army	Warfighter 13-4	ATEC
U.S. Navy	Aircraft Carrier Battle Group (CVBG) Assessment	COTF
U.S. Air Force	Blue Flag 2013	AFOTEC
U.S. Marine Corps	II Marine Expeditionary Force	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
MCOTEA – Marine Corps Operational Test and Evaluation Activity

INFRASTRUCTURE OBSERVATIONS

While exercise commanders permitted degraded network operations on almost twice as many unclassified network sites than the previous year, the instances of degraded performance on classified networks declined slightly. Exercise authorities remain cautious about permitting advanced threat depictions or advanced network effects that may endanger other exercise objectives, or be inappropriate for conduct on live networks.

The use of cyber ranges and laboratories increased in FY12, with four exercises incorporating ranges to support exercise conduct: RED FLAG 2012, CYBERFLAG 2012, TERMINAL FURY 2012, and WARFIGHTER 2012-4. For RED FLAG and CYBERFLAG, the use of the cyber range was integral to the exercise, whereas during the TERMINAL FURY and WARFIGHTER exercises, cyber range use supplemented and enhanced the training scenarios but was not central to the exercises. In all four instances, the use of the ranges permitted more advanced threat and network activities.

The CJCS EXORD of February 2011 directed more realistic cyber adversary portrayals in all major CCMD and Service-level exercises, but did not specify all of the necessary resources to accomplish this tasking. Expanded use of range facilities has been demonstrated to both enhance and expand the ability to depict wider varieties of cyber activities. Furthermore, many DoD networks have transitioned from direct CCMD management and oversight to "ownership" by consolidated cyber service providers or Service component cyber commanders.

The networks supporting USAFRICOM and USEUCOM, for example, are now consolidated under the Joint Enterprise Network (JEN) for the theater and under the control and management by the Army Signal Brigade in that theater. A number of Air Force networks are similarly consolidating.

All of these consolidations are consistent with the Department's plans for a Joint Information Enterprise, but this has further complicated the tasks of planning and executing realistic assessments. In recent exercises, the assessing agency either experienced critical delays or was unable to obtain approved ground rules, authorizations, or support for cyber adversary activities during the exercise. This was largely due to the cyber component's inability to support the additional activities required by the exercise, or the lack of sufficient agreements with the supported commander to make such commitments on behalf of the Combatant Commander. As DoD continues to consolidate cyber resources, it will be critical for these agencies to control sufficient resources to support exercises to the degree required by the EXORD. Additionally, the demand for "offline" capabilities, such as training, experimentation, development, and test ranges will increase.

DOT&E continues to support the development of methods and environments to exercise and assess advanced actions on appropriate closed-loop cyber ranges. CCMDs used cyber ranges such as the JIOR in four assessed exercise venues, and emphasis will continue for increasing the integration and operational realism of JIOR events associated with DOT&E's IA/IOP assessments in FY13. DOT&E sponsored a distributed cyber-range experiment in July 2012, where the JIOR was used to connect the National Cyber Range (NCR) with other cyber labs, targets, and attackers. NCR capabilities offer substantial increases in network scaling and substantial reductions in the time required for cyber research, development, training, and testing.

At DOT&E's initiative to enhance the operational realism and threat portrayal in exercises and range environments, DoD championed investments to mature the environments and capabilities needed for testing and training with advanced cyber adversaries. The need for this capability is highlighted by the findings contained in the DOT&E classified report dated April 2012. DOT&E recommended integrating four facilities into an enterprise cyber range to speed implementation of the CJCS EXORD, as well as to meet Section 933 requirements for infrastructure to support the rapid acquisition of cyber warfare capabilities.