Cybersecurity

SUMMARY

DOT&E cybersecurity efforts in FY14 included 16 Combatant Command (CCMD) and Service assessments completed as part of the Cybersecurity Assessment Program, 21 cybersecurity operational test and evaluation (OT&E) events of acquisition systems, and continued efforts to enhance assessment capabilities via cyber-range events. During this year's CCMD exercises and acquisition program operational tests, cyber Opposition Forces (OPFOR) portraying adversaries with beginner or intermediate cyber capabilities were able to demonstrate that many DOD missions are currently at risk from cyber adversaries. CCMD and Service authorities have yet to consistently show that critical missions can be assured in scenarios where an intermediate or advanced cyber adversary contests these missions.

During the Turbo Challenge 14 exercise, a combination of skilled local defenders and security-conscious network users and administrators denied the Cyber OPFOR's attempts to impact missions on the U.S. Transportation Command's network. This is one of the few times a CCMD quickly detected and effectively responded to thwart an attack by an intermediate-level cyber adversary. During this assessment, the U.S. Transportation Command demonstrated the following key security tenets:

- Implementation and enforcement of strong passwords and password storage requirements
- Hardening of outward-facing servers
- Consistent review of network logs using automated scripts
- Effective incident response and reporting processes.

Notwithstanding this infrequent success, the continued development of advanced cyber intrusion techniques makes it likely that determined cyber adversaries can acquire a foothold in most DOD networks, and could be in a position to degrade important DOD missions when and if they chose to. It is therefore critical that DOD network defenders, and operators of systems residing on DOD networks, learn to 'fight through' cyber attacks, just as they are trained to fight through more conventional, kinetic attacks.

DOD continued to improve compliance with policies intended to improve cybersecurity, such as ensuring known software patches are installed on time. Consequently, during FY14 DOT&E assessments, Red Teams report that some beginner- and intermediate-level network intrusion exploits did not work as frequently as they have in the past. However, fundamental vulnerabilities continue to persist in most networks, and processes to ensure accountability for security policy violations have not matured.

Exercise authorities permitted more realistic OPFOR activities on operational networks in FY14 than during previous years, but tended to limit activities to acquiring network accesses and exfiltration of information, rather than more disruptive activities such as denial of service attacks. While these limits are understandable due to constraints associated with operational networks, operationally realistic assessments require realistic cyber effects. Without realistic cyber effects, the training audience may have a false sense of security that their missions were not subject to degradation, and the operators and network defenders miss the opportunity to detect and respond to realistic cyber attacks. To address this requirement, DOD needs improved methods and range environments to better characterize and simulate cyber effects for both assessments and training.

In FY14, DOT&E began examining CCMDs' ability to sustain critical missions when subjected to realistic cyber threats. These efforts focus on missions deemed most critical by the CCMDs, and will help increase the visibility and realism of cybersecurity assessments.

DOD initiatives such as the Joint Information Environment (JIE) and the Cyber Mission Force are intended to address some of the inherent challenges with securing DOD networks. DOT&E will examine the effectiveness of new Cyber Protection Teams during future assessments with CCMDs and Services, and will fully test the JIE as it is implemented.

During FY14, DOT&E refocused cybersecurity assessments to help CCMDs and Services reduce the number of persistent cybersecurity vulnerabilities that DOT&E has reported on in previous years. Assessments now include a "fix" phase outside of the formal assessment, during which a DOT&E-sponsored team will advise CCMD and Service personnel on the implications of existing vulnerabilities, ways to address critical cybersecurity vulnerabilities, and points of contact for further assistance.

At the request of U.S. Pacific Command and several other CCMDs, DOT&E has begun executing more frequent cyber assessments, including "fix" phases, to help improve the commands' cybersecurity posture and assess the impacts of emerging cyber threats.

During FY14, DOT&E increased the interaction between cyber Red Teams and network defenders following assessments to help improve defender awareness of the signs and optimal responses to cyber intrusions. DOT&E sponsored the development of 'cyber playbooks' and battle drills during which network defenders can practice enhanced tactics, techniques, and procedures (TTPs).

Realistic cybersecurity assessments require operationally representative participation by network defenders. 'Tier 2' network defenders, which provide regional network defense, provide critical capabilities that augment the local network defenders' ability to detect and react to network intrusions. During FY14, Tier 2 network defenders provided more active

support to DOT&E assessments, although more consistent Tier 2 involvement is required in the future.

In FY14, DOT&E revised and published procedures for cybersecurity OT&E of acquisition programs, providing specific measures and standards for conducting cybersecurity tests. Cybersecurity OT&E will continue to focus on identifying significant cybersecurity vulnerabilities, and characterizing the impact of the vulnerabilities on operational missions. DOT&E identified critical cybersecurity vulnerabilities in most of the acquisition programs that were operationally tested during FY14.

During FY14, the demand for resources and skilled cybersecurity personnel needed to support operations, training, and assessment increased across the DOD. Cyber experts were needed in greater numbers to develop cyber-secure capabilities; to defend networks and systems; to provide cyber Red Teams to support training, assessments, and tests; to plan, conduct, and analyze tests and assessments; and to create ranges and range environments to support the activities discussed in this section. Demand has begun to exceed the capacity of existing personnel able to portray cyber threats, and projected FY15 personnel needs for cybersecurity tests and assessments, as well as training for the Cyber Mission Force personnel in support of U.S. Cyber Command, may not be met unless critical resource shortfalls are addressed.

During FY14, leadership at U.S. Strategic Command, U.S. Cyber Command, and U.S. Pacific Command approved Standing Ground Rules for a Persistent Cyber Opposing Force (PCO). These ground rules, proposed by DOT&E, permit year-round operations by the cyber OPFOR to enable a more representative portrayal of potential cyber adversaries. U.S. Northern Command also agreed to a PCO beginning in FY15. The PCO construct will allow heavily-tasked Red Team assets to support more assessments by optimizing Red Team targeting boards and aggressing more targets throughout the year. Results of the PCO are also expected to help set initial conditions for cybersecurity OT&E.

To improve DOD's cybersecurity posture, DOT&E recommends the CCMDs and Services do the following:

- Demonstrate fight-through capabilities and resiliency for all critical missions; these demonstrations should include realistic Cyber OPFOR play and active involvement by Tier 2 computer network defense service providers.
- Require higher levels of cybersecurity accountability for networks and systems needed for critical missions.
- Routinely include the effects of a representative cyber OPFOR in training exercises, as opposed to training in the unlikely benign cyber environment.
- Emphasize network defense fundamentals
  - Implementation and enforcement of strong passwords and storage requirements
  - Hardening of outward-facing servers
  - Consistent review of logs at all tiers
- Exercise and improve incident response and reporting processes.

FY14 ACTIVITIES

Cybersecurity Assessment Program Events

In FY14, DOT&E, in conjunction with the Army Test and Evaluation Command; the 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 completed 15 cybersecurity assessments. The assessments were of nine CCMD and three Service exercises, and of three visits to operational sites not during an exercise (see Table 1).

DOT&E's Cybersecurity Assessment Program included planning and conduct of events, both during large-scale training exercises and at operational sites during events other than a training exercise. DOT&E also conducted Theater Cyber Readiness Campaign (TCRC) assessments, which comprised a series of smaller assessment events focused on specific problems and topics of interest to improve cybersecurity. These sub-events assessed vulnerabilities identified during prior assessments and the impacts of emerging cyber threats. Each TCRC phase culminated in a capstone assessment event—usually a major exercise—where all elements of the TCRC could be simultaneously assessed. DOT&E has conducted TCRC activities at three CCMDs to date, and will expand these efforts to other CCMDs in the future.

Persistent Cyber Opposing Force (PCO)

During FY14, leadership at U.S. Strategic Command, U.S. Cyber Command, and U.S. Pacific Command approved Standing Ground Rules, proposed by DOT&E, for a Persistent Cyber OPFOR (PCO). The rules permit year-round operations by the cyber OPFOR to enable a more representative portrayal of potential cyber adversaries. U.S. Northern Command also agreed to a PCO beginning in FY15. The PCO will allow heavily-tasked Red Teams to support more assessments by optimizing Red Team targeting boards and aggressing more targets throughout the year. Results of the PCO are also expected to help set initial conditions for cybersecurity OT&E of acquisition programs.

Although the PCO construct may—through efficiencies—reduce the OPFOR workload for a given event, these efficiencies are not expected to offset the growth in demand for cyber experts.

Improvement of Cyber Threat Assessments

DOT&E has partnered with multiple DOD organizations to form teams possessing cyber, T&E, cyber range, and other expertise to support cybersecurity assessments, including:

Exercise Support Team. The Defense Intelligence Agency Exercise Support Team developed detailed threat folders to improve the understanding and portrayal of cyber-adversary

capabilities, and also supported the design and execution of exercise scenarios.

Standing Test, Assessment, and Rehearsal Team (START). The START helped ensure the right talent sets were integrated into DOT&E-sponsored assessment activities. In FY14, the START supported a series of cyber-range events (Project C) that stressed range capabilities and environments, while also affording new Cyber Protection Teams the opportunity to defend against cyber attacks on realistic networks. U.S. Cyber Command partnered with DOT&E on these cyber-range events, and is employing the results, which included a draft Cyber Protection Team (CPT) tactics guide, to help identify the appropriate training curriculum for the 68 CPTs, refine CPT tactics, and identify metrics to assess CPT performance. CPT personnel were appreciative of these training opportunities, and DOT&E will continue to look for opportunities to engage with CPTs and provide CPT assessment results to U.S. Cyber Command.

DOD Enterprise Cyber-Range Environment (DECRE). The DECRE continued to mature its cyber-range capabilities, but at a slower pace than desired by U.S. Cyber Command, the training community, and the Research, Development, Test, and Evaluation community. Major accomplishments in FY14 by the DECRE components include:

- The Test Resources Management Center (TRMC) fielded the cloud-based Regional Service Delivery Point for enhanced range capability and connectivity.
- The Joint Staff J6 created several cyber environments in which to examine cyber effects not suitable for operational networks.
- The TRMC's National Cyber Range became fully operational and is now looking at ways to expand capacity to meet the growing demand for range events.

All of these DECRE accomplishments are positive and noteworthy, but the demand for repeatable, routine, and distributed events exceeds current capabilities, and demand is expected to increase significantly across the Future Years Defense Program.

Partnerships and Collaboration. Several Research and Development organizations have made existing lab environments available and performed important assessments to characterize the effects of cyber attacks. Mission areas examined included:

- Ballistic Missile Defense – DOT&E partnered with the Missile Defense Agency (MDA) to plan and execute four events of increasing complexity and realism to examine potential cyber vulnerabilities.
- Aegis – DOT&E partnered with Navy Red Team, Wallops Island and Dahlgren test facilities, and Combat Direction Systems Activity (Dam Neck) to characterize and understand vulnerabilities focused on the Aegis Combat Systems. Events provided information on the scope and duration of cyber effects to inform Program Office development.
- Command, Control, and Intelligence Systems – DOT&E partnered with the Joint Staff J6 Command, Control, Communications, and Computers Assessment Division to create an environment to examine cybersecurity aspects of the common operating picture and situational awareness systems. Events identified and characterized cyber effects to be introduced into training exercises. Continuing efforts will expand the systems and environment to explore a wider variety of cyber effects.

Both the MDA and the Navy have identified ways to improve cybersecurity for their respective programs through these assessment activities.

The Naval Postgraduate School developed a Malicious Activity Simulation Tool (MAST), which is ready for testing in realistic network environments. DOT&E is overseeing the efforts to test this capability on a cyber range to confirm readiness to support training and assessment of network personnel.

Several National Labs (Sandia National Labs, Johns Hopkins Applied Physics Lab, and MIT Lincoln Labs) delivered or are developing prototypes of new instrumentation and visualization capabilities, new products for traffic generation, and new ways to automate or virtualize network environments and activities. These new capabilities will help make cyber-range environments more operationally realistic, and will also help optimize the employment of range capabilities in repeatable and distributed events.

The Army's Threat Systems Management Office (TSMO) played a leading role in the planning and execution of many DOT&E-sponsored cyber-range experiments, identification and acquisition of new Red Team capabilities, testing and fielding of cyber-range Regional Service Delivery Points, and management and operation of the PCO. TSMO and the other Service Red Teams continued to provide Cyber OPFOR support to many of the FY14 exercise assessments, as well as acquisition testing. Other Service Red Teams also provided critical support in portraying cyber adversaries in exercise, tests, and range events.

TABLE 1. CYBERSECURITY ASSESSMENT PROGRAM EVENTS IN FY14		
EXERCISE AUTHORITY	**EVENT**	**ASSESSMENT AGENCY**
U.S. Africa Command	Epic Guardian 2014 (exercise cancelled, conducted as Site Visit)	ATEC
U.S. Central Command	Site Visit – Special Operations Command Central	ATEC
U.S. Cyber Command	Cyber Flag 2014	ATEC
U.S. European Command	No Assessment Opportunity	ATEC
U.S. Northern Command	Vigilant Shield 2014	AFOTEC
U.S. Pacific Command	Cyber Readiness Campaign Event – Physical Security	START
	Cyber Readiness Campaign Event – Network Hygiene	
	Cyber Readiness Campaign Event – Knowledge Management	
U.S. Southern Command	Site Visit – Joint Interagency Task Force South	ATEC
U.S. Special Operations Command	Tempest Wind 2014	ATEC
U.S. Strategic Command	Global Thunder 2014	JITC
	Global Lightning 2014	JITC
U.S. Transportation Command	Turbo Challenge 2014	JITC
U.S. Army	Warfighter 2014-4	ATEC
U.S. Navy	Valiant Shield 2014	COTF
U.S. Air Force	No Assessment Opportunity	AFOTEC
U.S. Marine Corps	Ulchi Freedom Guardian 2014	MCOTEA

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
START – Standing Test, Assessment, and Rehearsal Team

Cybersecurity OT&E of Acquisition Programs

In FY14, DOT&E approved cybersecurity test plans for 82 Service and DOD systems, including 62 Test and Evaluation Master Plans, 26 operational test plans, and 25 related test documents. DOT&E cybersecurity subject matter experts observed cybersecurity tests and reviewed test data for 21 systems across the warfare domains.

In August 2014, DOT&E issued updated procedures for OT&E of cybersecurity in acquisition programs. The procedures specify the information needed for planning, conducting, and reporting cybersecurity operational testing that includes a cooperative vulnerability and penetration assessment, and an adversarial assessment. The purpose of the cooperative assessment is to identify the cybersecurity vulnerabilities of a system in cooperation with the program manager and to allow the program to fix them. The adversarial assessment then evaluates the ability of a unit equipped with the system to support assigned missions in the expected operational environment in the presence of a realistic cyber threat.

FINDINGS, TRENDS, AND ANALYSIS

Assessment Structure

FY14 continued the FY13 trend of fewer exercises available or suitable for assessment; the impetus for this in FY13 was the sequester, and reductions in exercise funds continued into FY14 (see Figure 1). The assessments outside of an exercise reflect both the declining number of large-scale exercises and the implementation of focused opportunities to find, fix, and verify. Service-level assessment remained at a level of one per Service.

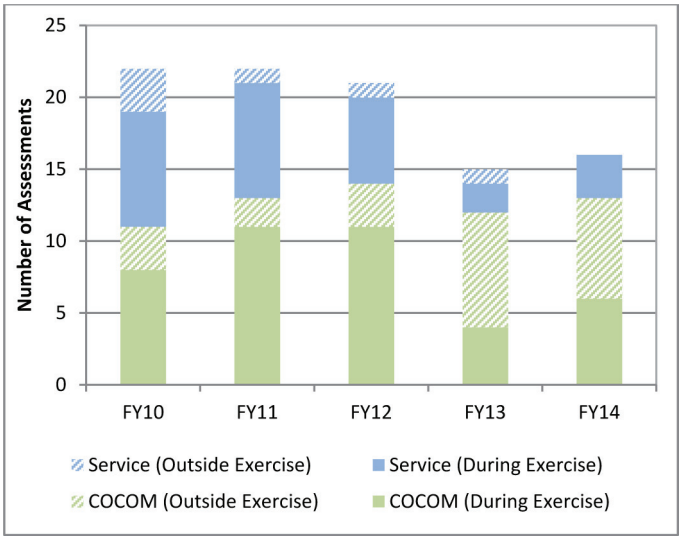

Figure 1. Cybersecurity Assessments FY10 – FY14

As in previous years, the most common adversary cyber activity permitted and portrayed during FY14 exercises was the compromise and exfiltration of critical operational information. The exercise authority's desire not to affect exercise operations usually prevented the opposing force from using the compromised information to influence operations. These limitations minimized the value of cybersecurity actions for training and assessment. In several exercises, exercise authorities allowed Red Teams to conduct some level of denial of service and data manipulation. This is a welcome move towards improving threat realism and the creation of observable mission effects.

FY14 assessments increasingly included active participation of the local network defenders and the next higher layer of network defense, the Tier 2 computer network defense service providers. The increased participation is a notable improvement over that observed in previous years, and enables assessment of both the local/proactive defenses (standards compliance, patch management, vulnerability management) and the defensive activities conducted at higher echelons that involve the detection, reaction, and response to cyber threats. Furthermore, realistic participation by network defenders is required for an adequate assessment of the ability of CCMDs and Service components to sustain critical missions when under cyber attack.

Assessment Findings

Red Teams portraying a Cyber OPFOR successfully accessed target networks primarily through vulnerable web services and social engineering (phishing). Similar to FY13, Red Teams routinely expanded access across networks using stolen credentials. The asymmetric nature of cyber operations allows even a single default or weak password to lead to rapid access and exploitation of the network. This is particularly true when the password belongs to an individual with elevated privileges. FY14 assessments revealed numerous violations of DOD password security policies, which indicates the policies are either too difficult to implement, too hard to enforce, or both.

On the other hand, compliance with relevant network security standards exceeded 85 percent overall, and compared to FY13, was higher in all areas except security design and configuration, and identification and authentication (passwords). Compliance assessments determine whether network defensive measures are in place. The generally poor defensive performance against dedicated attacks by Red Teams shows that a network is only as secure as its weakest link. Unless compliance levels approach 100 percent, it is likely a dedicated cyber adversary will succeed in accessing a network. Hence it is critical that network users and defenders learn to fight through and accomplish missions in the face of network security breaches.

In FY14, certain areas of network defense improved over previous years. Regional (Tier 2) computer network defense service providers, which provide key support to the local defenders, participated in half of the assessed exercises. Protective defense, in the forms of phishing discovery and perimeter defense configurations, prevented several attempted Red Team incursions. These successes reflect improved personnel awareness to recognize and report phishing emails, better filters for identifying and blocking phishing emails, and implementation of settings to block common intrusion techniques used in these emails. Defenses would be further improved by hardening outward-facing servers and limiting the amount of sensitive information available on public portals.

Some network defenders demonstrated the ability to detect intrusions by reviewing logs of network and sensor activity, and initiating actions to counter the adversary presence on the network. In over half of the FY14 assessments, local network defenders initiated these detections and responses, and coordinated the response with regional computer network defenders. Such coordinated responses, when executed well, can protect critical mission systems from cyber attacks.

In many cases, however, the response actions were not quick enough to preclude an intermediate or advanced cyber adversary from pivoting to another foothold or escalating privileges within the compromised network. Additionally,

some responses were to reboot or reload software for systems believed to be compromised or in a degraded mode. Depending on the operational phase of the exercise, rebooting or reloading software denies users mission-critical services, and does not contribute to the commander's ability to fight through a cyber attack. Reloading software can also result in the loss of previously installed software patches, making systems more susceptible to cyber attack.

Although many of the elements of network protection and defense were observed in FY14 exercises, the lack of mature and well-rehearsed procedures often precluded effective integration of network defense capabilities, placing missions at risk. DOT&E assessed that at least one mission in each exercise assessment was at high risk because of observed cyber activities, including:

- Loss of operational security resulting from the compromise of sensitive information
- Data manipulation
- Denial of service

Several CCMDs have initiated development of Cyber Playbooks that are intended to achieve more accurate and timely execution of responses to cyber attacks. To encourage these efforts, and to evaluate their effectiveness, DOT&E initiated planning with three CCMDs to begin a focused examination of the CCMD's ability to sustain important missions when subjected to realistic cyber stress. These efforts will result in multi-year Cyber Assessment Master Plans (CAMPs) centered on the missions deemed most critical by the CCMDs.

Execution of CAMPs will support implementation of the Chairman of the Joint Chiefs of Staff Execute Order, published in February 2011, and re-emphasized by the Secretary in December 2012, which required routine training and validation of procedures that enable execution of critical missions in contested cyber environments. To date, DOT&E has yet to observe a mission demonstration in an advanced cyber-threat environment.

DOT&E found significant vulnerabilities on nearly every acquisition program that underwent cybersecurity OT&E in FY14. Program managers worked to resolve vulnerabilities found from cybersecurity testing in prior years, but FY14 testing revealed new vulnerabilities. Corrections to past vulnerabilities have required modifications to system architecture; hardware, firmware, and configurations; system software; training; and operational procedures. As in FY13, significant vulnerabilities found during OT&E could have been found and/or remedied during earlier phases of development. Nearly all the vulnerabilities were discoverable with novice- and intermediate-level cyber threat techniques. The cyber assessment teams did not need to apply advanced cyber threat capabilities during operational testing.

DOT&E found that some programs had not adequately planned for cybersecurity testing. This resulted in insufficient time to perform adequate cooperative testing, implement fixes, and achieve successful adversarial testing results. It also negatively impacted the ability of cyber teams to plan and execute their test activities across different programs.

REPORTS

For the Cybersecurity Assessment Program, DOT&E issued an assessment report for each exercise or site visit that discussed observations, findings, and discovered vulnerabilities. DOT&E also issued separate reports to DOD, CCMD, and Service leadership highlighting high-priority observations. For OT&E of acquisition programs, DOT&E reported the cybersecurity test results as an integrated part of operational effectiveness, suitability, and survivability.

DOT&E also published five memoranda of findings in areas of concern in FY14. Finding memoranda detail specific problems that need senior leadership attention. DOT&E addressed the finding memoranda to the responsible leadership for action. DOT&E will evaluate corrective actions in future assessments.

New finding memoranda published in FY14 were:

- Defense Connect Online (Released November 2013). This was a follow-on to a September 2010 finding that reported means by which the DOD chat/collaboration system could be compromised. It reported on new findings as well as the efficacy of prior remediation. DISA has responded to this report noting corrections that will be made to the system in question.
- Host-Based Security System (Released April 2014). This was a follow-on to an October 2012 finding that reported shortfalls in how the DOD network security tool was providing inventory data. It reported on new findings of how the tool could be exploited. DISA/CIO have responded to this report noting the actions that will be taken to correct the finding.
- Electronic Security of Special Handling Documents (Released April 2014). This finding reported shortfalls regarding how sensitive Alternate Control Measure programs were being handled on classified networks. The Joint Staff, DOD CIO, and USD(I) have provided a coordinated response describing corrective measures that have or will be taken to address this finding.
- Shipboard Datalinks (Released June 2014). This finding reported on issues identified with off-ship datalink security. The Navy has responded with specific actions that are being taken to address the finding.
- Assessment of DOD Cybersecurity during Major Combatant Command and Service Exercises and Major Program Acquisitions (released September 2014). This detailed report provided classified observations and analysis concerning common vulnerabilities and issues uncovered during major exercises and acquisition tests. No response was required.

FY15 GOALS AND PLANS

A major goal of the Cybersecurity Assessment Program in FY15 is to assist the CCMDs and Services in improving their cybersecurity postures by finding cybersecurity problems, providing information to fix problems, and verifying the status of implemented fixes to previously discovered problems. An additional goal for cybersecurity OT&E is to implement the new test procedures to improve rigor and consistency of cybersecurity testing for acquisition programs.

Specific FY15 goals include:

- Publish finding memoranda to recommend solutions to significant cybersecurity problems that could have an impact on DOD missions.
- Include a "fix" phase in each of the planned assessments of nine large-scale training exercises, four operational site visits outside of exercises, and four cyber readiness campaigns having multiple events (see Table 2).
- Expand the Standing Ground Rule authorities for PCO operations to additional CCMDs.
- Ensure availability of certified and properly trained and equipped Red Teams to provide representative Cyber OPFOR support to OT&E and exercise assessments.
- Improve realism of the cyber threat levels and effects portrayed during all tests and assessments.
- Expand DOD cyber-range environments to support demonstration of advanced cyber effects, and development and verification of cybersecurity solutions.
- Publish a Handbook for the Cybersecurity Assessment Program to update the procedures, expectations, and requirements for cybersecurity assessments of CCMDs and Services.
- Work with DOD test organizations to plan more robust cybersecurity testing during OT&E, including participation by cyber defenders and the creation of mission effects.
- Provide technical recommendations to programs and acquisitions organizations based on the data gathered from cybersecurity assessments during OT&E.

TABLE 2. CYBERSECURITY ASSESSMENTS PROPOSED FOR FY15

EXERCISE AUTHORITY	EVENT	ASSESSMENT AGENCY
U.S. Africa Command	Judicious Response 2015	ATEC
U.S. Central Command	Site Visit – Air Forces Central Command	ATEC
	Site Visit – Marine Corps Forces Central Command	ATEC/MCOTEA
U.S. Cyber Command	Cyber Guard Exercises	JITC
U.S. European Command	Austere Challenge 2015	ATEC
	Cyber Readiness Campaign Events	ATEC
North American Aerospace Defense Command/U.S. Northern Command	Vigilant Shield 2015 Cyber Readiness Campaign Events	AFOTEC
U.S. Pacific Command	Cyber Readiness Campaign Events	START, AFOTEC, ATEC
U.S. Southern Command	Integrated Advance 2015	ATEC
U.S. Special Operations Command	To Be Identified	MCOTEA
U.S. Strategic Command	Global Lightning 2015	JITC
	Cyber Readiness Campaign Events	JITC
U.S. Transportation Command	Turbo Challenge 2015	JITC
U.S. Army	Warfighter 2015-4	ATEC
U.S. Navy	Joint Task Force Exercise – USS *Roosevelt*	COTF
U.S. Air Force	Site Visit – U.S. Pacific Air Forces	AFOTEC
U.S. Marine Corps	Site Visit II – Marine Expeditionary Force	MCOTEA

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
START – Standing Test, Assessment, and Rehearsal Team