DOT&E Cybersecurity Procedures

10 April 2015

Walter Dodson, Kevin Eveker, Anil Joglekar, Sourav Mandal,

William Robbins, Phillip Webb, and Kevin Westburg

Shawn Whetstone, Project Leader

Background

- **Cyber domain touches all military domains including land, sea, air, and space**

- **Cybersecurity presents a major potential threat to the DoD**
  - "….a networked world -- a world in which oceans are crossed at the speed of light -- presents challenges to American security that our nation has never before confronted" - Defense Secretary Chuck Hagel (28 March 2014)

- **A review of cybersecurity in operational testing over the past several years revealed a lack of data, mission effects, and adversarial cyber testing as required by the DOT&E guidance**
  - DOT&E therefore developed the 1 August 2014 revised procedures for operational test and evaluation

Goal: Improve DoD Cybersecurity Posture

- **Results from threat-representative cyber testing during OT&E should be feeding into DoD processes in ways that spur action**
  - Inform acquisitions decision makers with respect to program milestones
  - Improve DoD Defensive Posture through improved Tactics, Techniques, and Procedures
    - » Improve detection tools and training for cyber response
    - » Improve collaboration between local defenders and network service providers
  - Inform Chief Information Officer (CIO) if assessment finds sufficiently poor security posture to revoke Authority to Operate (ATO)

- **The revised DOT&E procedures are desired for ensuring consistent, comprehensive, and threat representative cybersecurity OT&E for oversight programs**
  - Be thorough, comprehensive, and consistent in reviewing and approving TEMP and Test Plans
  - Integrate cyber into the DOT&E assessment of system effectiveness
  - Provide education and training to IDA, DOT&E, OTA, and program office staff
    - » Provide seminars, tutorials, courses, etc.
    - » Organize periodic discussion group between OTAs, net defenders, and adversary teams

Procedures Summary

- **New procedures supersede previously issued 2009 DOT&E guidance and two subsequent clarification memos**
  - Rectifies insufficient data collection and adversarial cyber testing, and incomplete evaluation of mission effects
- **Retains a two-phase approach:**
  - Cooperative, *comprehensive* assessment to identify vulnerabilities
  - *Threat-representative* adversarial assessment focused on mission effects and cyber defender responses
- **More specific direction on the minimum data OTAs should collect**
  - Supports independent analysis by DOT&E
- **DOT&E will use the results of the cybersecurity OT&E, in part, to determine system effectiveness, suitability, and survivability**

Scope

- **The procedures apply to all oversight programs that send or receive digital information, e.g.:**
  - Direct connections to external networks
  - Connections to host platforms, including specialized connections or protocols
  - Wireless or radio frequency connections
  - Physical ports (e.g. USB), removable data cards
  - Mission planning systems
  - Specialized data buses (e.g. 1553)
  - Maintenance laptops and equipment
- **Any systems with two-way data transfer capabilities to external networks must perform both phases of cybersecurity testing**
- **DOT&E will evaluate the level of test required for other systems on a case-by-case basis**
  - Need information on system architecture with data paths and protocols

Scope (cont.)

- **The need for threat-representative adversarial cyber testing is independent of any requirements for certification and accreditation**
  - Receipt of an Authority to Operate (ATO) does not obviate the need for cybersecurity testing as part of OT&E
- **Cyber defenders (local and upper echelons) should participate in OT&E to support detect, react, and restore data collection**
  - Testers can prompt restore activities if no detection occurs
- **Programs processing data above the secret level should follow DOT&E procedures to the extent possible**

Phase 1: Cooperative Vulnerability and Penetration Assessment

- **Comprehensive assessment to identify all vulnerabilities in the operational context**
- **Cooperative with all stakeholders, including program office, system administrators, and developers**
- **Should be conducted in an operationally representative way to the extent possible – introducing the system into the operational environment often adds vulnerabilities:**
  - Unprotected data paths to networks and other systems
  - Misconfigured cyber defense systems
  - Inadequate physical security
  - Deficient operator Tactics, Techniques, and Procedures
- **The operational environment introduces defensive capabilities as well for many systems, providing an early look at their effectiveness**

Phase 2: Adversarial Assessment

- **Non-cooperative assessment of system performance conducted by the OTA in the presence of a threat-representative cyber adversary**

- **An NSA-certified adversarial team must portray the threat**
  - Must be accredited by USSTRATCOM to operate non-cooperatively on live networks, as per CJCSM 6510.03, 28 February 2013
  - Certification also assures minimum competency

- **Threat portrayal should be representative and system-specific**
  - Testing should permit sufficient time for adversarial activities, including reconnaissance
  - Adversarial team should be permitted to execute non-destructive cyber attacks
  - Adversarial activities should exhibit the same range of capability that the threat would, up to and including system-specific exploits and attacks through enterprise assets

Phase 2: Adversarial Assessment (cont.)

- **Compared to the prior phase, focus is on mission accomplishment, not comprehensiveness**
  - Once the adversarial team finds an entry point, they will attempt to induce mission effects instead of looking for more vulnerabilities
- **The OTA will need to collect data on adversarial team activities, cyber defense activities, and mission effects**
  - System operators should be conducting representative missions
  - Cyber defenders (local and upper echelons) should participate in OT to support Detect, React, and Restore data collection

Timing and Data Sharing

- **The timing of the two phases will vary by program, but should occur sequentially in the context of planned operational test events**
- **Programs are encouraged to schedule time between phases to fix vulnerabilities that are discovered in Phase 1**
- **A real cyber adversary will spend significant time doing reconnaissance on system under test prior to attack**
  - The adversarial team should use data as necessary from Phase 1 to replace this long-term reconnaissance, or to ensure that all critical vulnerabilities are examined

Mandatory Minimum Data Elements
Attachments A, B, and C of DOT&E Memo

- **Revised DOT&E guidance lists minimum data sets to be collected for both phases of cybersecurity OT**

- **Cooperative Vulnerability and Penetration Assessment:**
  - Selected compliance baseline metrics
  - Cyber vulnerabilities with DISA severity codes
  - Penetration/exploitation techniques

- **Adversarial Assessment:**
  - Adversarial activities
  - Times to detect
  - Defense activities
  - System restoration activities
  - Mission effects

Mission Effects

- **Mission effects parameters will be system specific, but should be quantitative measures of system effectiveness**
- **Should include performance parameters already being used to assess effectiveness**
- **Where direct measurement not possible, OTAs should describe a strategy using Subject Matter Experts (SMEs) to connect exploitations to mission effects**
  - Explain what SMEs the OTA will use and how they will be used
  - Estimate reduction (minor, major, severe) in measures of effectiveness

How to Evaluate Cybersecurity OT&E

- **Understand the system and its cyber operational environment**
  - System architecture, typical users, and missions
  - What the cyber threat can and might do
  - What cyber defenders can and should do
  - Tools used by cyber defenders

- **Understand the test**
  - Insider and outsider threat portrayal
  - How cyber defense performance and mission effects will be evaluated
    - » Cooperative assessments: putative impacts
    - » Adversarial assessments: direct measurement (extent possible)
  - Test design and limitations
  - Data to be collected to support evaluation

- **During the test**
  - Is the test design being followed? New or unforeseen limitations?
    - » New system components discovered on-site?
    - » System components unexpectedly placed off-limits?
    - » Adversarial assessments: cyber defenders and adversarial team playing realistically?
  - Are the required data being collected for Phase 1 or Phase 2?
    - » Including minimum data in DOT&E guidance

Summary

- **Revised DOT&E procedures retain the same, basic two-phased approach to cybersecurity testing in OT&E as previous guidance**
- **Applies to all oversight programs that send or receive digital information, including through physical means**
- **Greater specificity with respect to:**
  - Cooperative vulnerability assessment and penetration testing phase activities
  - Adversarial testing phase activities
  - Minimum data to be collected in both phases
- **Emphasis on mission effects in the adversarial phase, either through direct demonstration or through a well-thought-out analytical exercise**
- **Measurement of cyber defender responses in adversarial phase**