



OPERATIONAL TEST  
AND EVALUATION

OFFICE OF THE SECRETARY OF DEFENSE  
1700 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1700

FEB 01 2013

MEMORANDUM FOR COMMANDER, ARMY TEST AND EVALUATION COMMAND  
DIRECTOR, MARINE CORPS OPERATIONAL TEST AND  
EVALUATION ACTIVITY  
COMMANDER, OPERATIONAL TEST AND EVALUATION  
FORCE  
COMMANDER, AIR FORCE OPERATIONAL TEST AND  
EVALUATION CENTER  
COMMANDER, JOINT INTEROPERABILITY TEST CENTER

SUBJECT: Test and Evaluation of Information Assurance in Acquisition Programs

DOT&E has provided detailed guidance for the test and evaluation of information assurance in acquisition programs and I recently reviewed the implementation of this guidance in FY12 across a number of test reports.<sup>1</sup> I have attached a copy of that review. While we have collectively improved information assurance testing and evaluation, my review identified a number of areas where we can further improve, as follows:

- Independent Penetration Testing – Due to limited test durations, sharing system information and interconnections between the cooperative cyber vulnerability assessment teams (usually a “Blue Team”) and the independent cyber penetration/exploitation teams (usually a “Red Team”) is acceptable. However, shared information should not include specific vulnerabilities or system shortfalls. The effort of the cyber penetration/exploitation team should go beyond merely validating prior findings, and focus on examining the system under test in an operational and threat representative event. Additionally, separate teams preferably should perform vulnerability assessments and penetration/exploitation assessments to enhance independence and opportunities for assessing protect, detect, react and respond components. Finally, the correction of vulnerabilities discovered in the cooperative assessments should be an entrance criterion for subsequent penetration/exploitation testing.
- Network Defense Analysis – The test environment should encompass those network defense elements (including trained personnel, standard tools, and normal network defense procedures) that may not be locally resident and are increasingly provided at higher tiers by other activities. The test should quantitatively examine not only the inherent system/network protections for the system under test, but also the network defense ability to detect penetration or

---

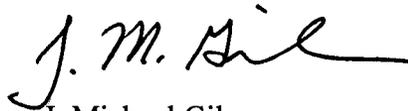
<sup>1</sup> Director, Operational Test and Evaluation, *Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs*, 21 January 2009; *Clarification of Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs*, 4 November 2010.



exploitation, react to those events (either procedurally or automatically), and restore the system to full capability following the event. Where appropriate, continuity of operations should be demonstrated or assessed for enterprise system programs; weapons system programs should coordinate with my office to confirm the requirement for continuity of operations testing.

- Operational Effects Analysis – Testing should include an assessment of operational risk presented by vulnerabilities and shortfalls exploited by a representative threat, and the most direct way to assess that risk is to demonstrate and record relevant operational effects. When operational threat representative effects cannot be conducted on live-networks, alternate evaluation approaches (including the use of cyber range facilities) should be employed and included in the test planning.

We must routinely review information assurance test and evaluation procedures and outcomes as the cyber environment in the Department evolves. I request your support in continuing to improve these information assurance tests to be not only as rigorous as every other test you conduct, but as rigorous and challenging as the cyber threats these systems will confront.



J. Michael Gilmore  
Director

Attachment:  
As stated



---

# **FY12 Overarching Assessment of Information Assurance During Operational Test and Evaluation**

**17 January 2013**

---

Attachment



# Purpose

---

- **Provide an initial assessment of FY12 information assurance testing during OT&E**
- **The objective was to assess information assurance testing for consistency in implementation, commonality of vulnerabilities, and identify improvements**
- **Data from 14 oversight systems that had penetration testing undertaken were obtained from OED research staff**
- **These systems did not go through the DOT&E TEMP and Test Plan checklist reviews first implemented during late FY11**

---

*Acronyms on this slide: Operational Test and Evaluation (OT&E), Operational Evaluation Division (OED), Test and Evaluation Master Plan (TEMP).*



# Background

---

- **DOT&E information assurance assessment procedure is given in the memorandum dated 21 January 2009 and clarification memorandum dated 4 November 2010**
  - **Assessment procedure is defined by:**
    - Step 1: Determine applicability of DOT&E information assurance procedures
    - Step 2: Initial review
    - Step 3: Risk assessment
    - Step 4: Cooperative operational vulnerability evaluation
    - Step 5: Independent realistic penetration testing to assess PDRR
    - Step 6: Continuity of operations evaluation
  - **Primarily Steps 4, 5, and 6 constitute the operational assessment portion of the information assurance assessment process**
    - Steps 1, 2, and 3 are done during certification and accreditation and developmental test phase
  - **DOT&E and AT&L/DT&E are currently jointly reviewing this policy for potential updates and enhancements**
- 

Acronyms on this slide: Protect, Detect, React, and Restore (PDRR), Acquisition, Technology, and Logistics (AT&L)/Developmental Test and Evaluation (DT&E).



# OT&E Assessment Teams

Organization	Cooperative Vulnerability Assessment (Step 4)	Independent Penetration Assessment (Step 5)
U.S. Army	1 <sup>st</sup> IOC, ARL-SLAD	TSMO
U.S. Navy	NIOC, COTF	NIOC, COTF
U.S. Air Force	92 <sup>nd</sup> IOS	92 <sup>nd</sup> IOS
U.S. Marine Corps	MCIAAT	MCIAAT

- **Inconsistency in how Services address cooperative vulnerability assessment (Step 4) and independent penetration assessment (Step 5)**
- **Potential for lessened independence between Steps 4 and 5**
- **Need to improve consistency across Services**

Acronyms on this slide: Information Operations Command (IOC), Army Research Laboratory-Survivability/Lethality analysis Directorate (ARL-SLAD), Threat Systems Management Office (TSMO), Navy Information Operations Command (NIOC), Commander Operational Test and Evaluation Force (COTF), Information Operations Squadron (IOS), Marine Corps Information Assurance Assessment Team (MCIAAT), Operational Test and Evaluation (OT&E).



# Systems Used in Assessment

<b>Army</b>	AB3 WIN-T JTRS BCS-F PAC-3 Gray Eagle GCSS-A DCGS-A	Apache Block III Helicopter Warfighter Information Network-Tactical Joint Tactical Radio System Manpack Battle Control System-Fixed Patriot Gray Eagle UAV Global Combat Support System-Army Distributed Common Ground System-Army
<b>Air Force</b>	GPS-SAASM  ISPAN	Global Positioning System-Selective Availability Anti-spoofing Mode  Integrated Strategic Planning and Analysis Network
<b>Navy</b>	DCGS-N T-AKE AEGIS NMT	Distributed Common Ground System-Navy Dry Cargo/Ammunition Ships ARGIS Weapon System Navy Multiband Terminal
<b>Marines</b>	None reviewed for this study	



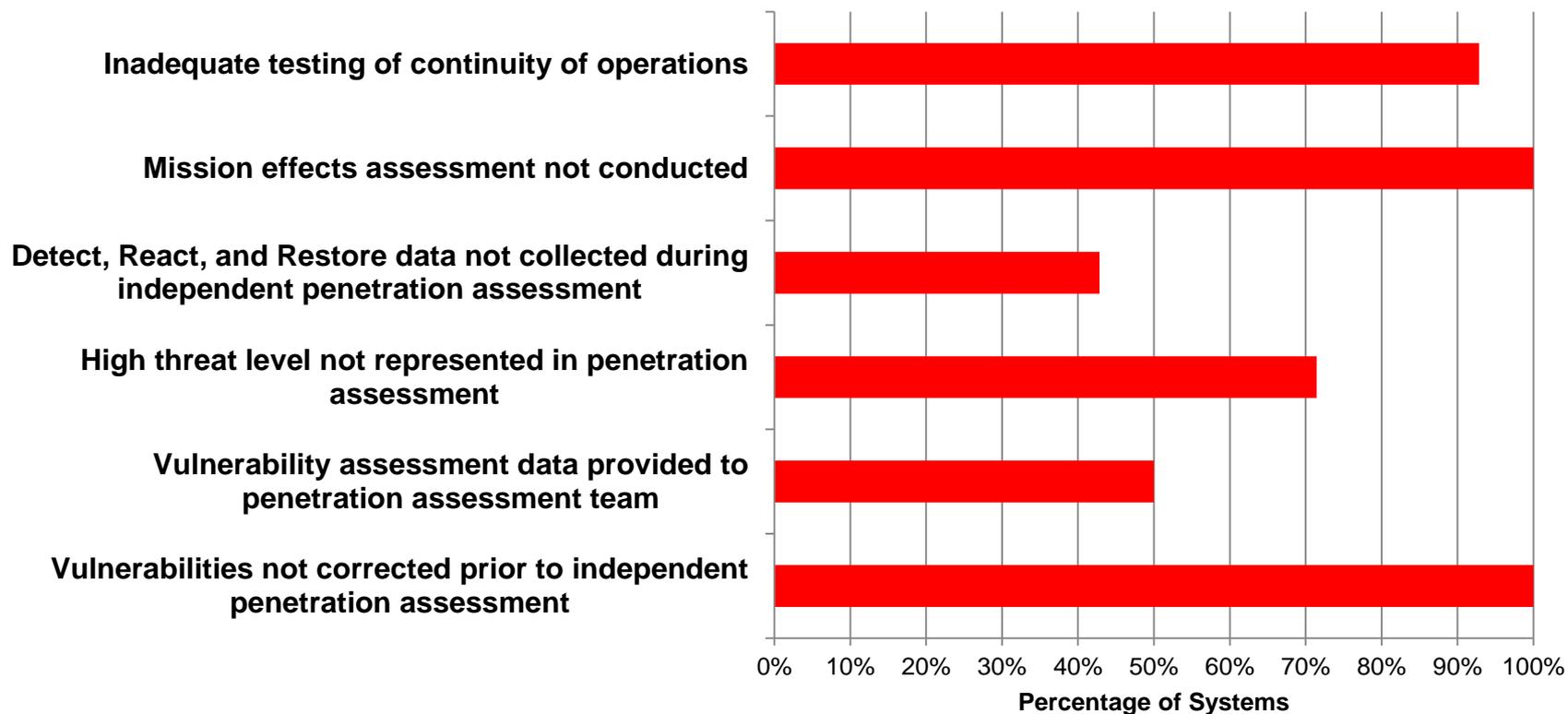
# Test Conduct Assessment

---

- **Cooperative vulnerability assessment (Step 4) testing generally conforms to DOT&E expectations, but independent penetration assessment (Step 5) generally does not**
- **Vulnerability findings were not corrected before penetration testing in any of the systems reviewed**
- **Penetration assessment testing did not have participation of trained network defenders**



# Test Conduct Deficiencies





# Vulnerability Assessment Methodology

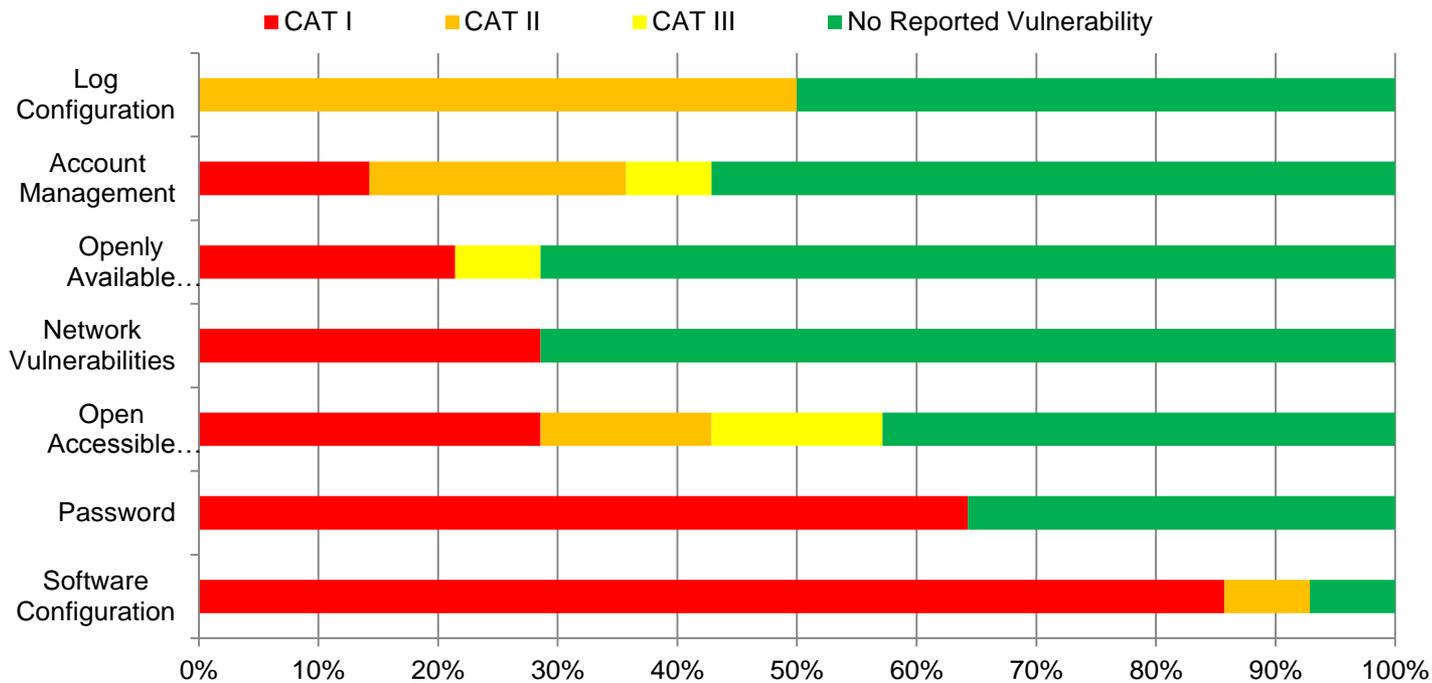
---

- **Identified vulnerabilities from 14 systems**
  - **Vulnerabilities were categorized using Defense Information Systems Agency categories as:**
    - CAT I – Allows an attacker immediate access into a machine and allow super-user access
    - CAT II – Provides information which have a high potential of giving access to an intruder
    - CAT III – Provides information that potentially could lead to compromise.
  - **Individual vulnerabilities collapsed into seven common categories**
    - Open Source Intelligence
    - Password Management
    - Log Configuration
    - Open Accessible Physical Ports
    - Software Configuration
    - Network Vulnerabilities
    - Account Management
-





# Observed Information Assurance Deficiencies





# Conclusions

---

- **Cooperative vulnerability assessments (Step 4) show most systems have easy-to-exploit vulnerabilities**
  - **Inconsistent and inadequate independent penetration assessment (Step 5) execution among Services**
  - **Failure to correct vulnerabilities limits the value of the independent penetration assessment**
  - **Detect and React data are lacking**
  - **Information on mission effects is lacking due to not being allowed to exploit data and effect operations**
  - **Continuity of operations evaluation (Step 6) generally lacking**
-



# Recommendations

---

- **Improve consistency and adequacy of assessments**
    - Require Detect and React data to be collected for all systems
    - Require separate teams for cooperative vulnerability and threat representative independent penetration assessments
  - **Improve operational realism of independent penetration testing**
    - Provide penetration testers with limited or no system and network data to ensure appropriate threat realism, even if more time is required to conduct test
    - Require full cyber defense capability to participate during penetration testing to measure detection ability
    - Require information assurance testing as a concurrent part of operational testing and permit exploitation to determine mission effects
  - **Revise current DOT&E information assurance memorandum**
    - Introduce criterion that known vulnerabilities be corrected before penetration testing
    - Clarify that continuity of operations testing only applies to enterprise systems and not to individual weapon systems
-