OPERATIONAL TEST
AND EVALUATION

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

JAN 2 1 2009

MEMORANDUM FOR DIRECTOR, NATIONAL SECURITY AGENCY
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR INFORMATION AND IDENTITY ASSURANCE
DIRECTOR, ARMY TEST AND EVALUATION OFFICE
DIRECTOR, NAVY TEST AND EVALUATION AND TECHNOLOGY REQUIREMENTS (N912)
DIRECTOR, AIR FORCE TEST AND EVALUATION
DEPUTY DIRECTOR, DEVELOPMENTAL TEST AND EVALUATION, SYSTEMS & SOFTWARE ENGINEERING, OUSD(AT&L)
COMMANDER, ARMY TEST AND EVALUATION COMMAND
COMMANDER, AIR FORCE OPERATIONAL TEST AND EVALUATION CENTER
COMMANDER, OPERATIONAL TEST AND EVALUATION FORCE
DIRECTOR, MARINE CORPS OPERATIONAL TEST AND EVALUATION AGENCY
COMMANDER, JOINT INTEROPERABILITY TEST COMMAND

SUBJECT: Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs

The attached provides the general procedures for evaluation of information assurance (IA) during the operational test and evaluation (OT&E) of Department of Defense (DoD) acquisition programs. Implementation of these procedures will improve test rigor and better inform acquisition and fielding decisions. DOT&E will consider the adherence to these procedures when assessing the adequacy of Test and Evaluation Master Plans (TEMPs) and Test Plans submitted for approval. This document supersedes the Director, Operational Test and Evaluation (DOT&E) Policy for OT&E of IA in Acquisition Programs, dated November 21, 2006.

Charles E McQueary

Dr. Charles E. McQueary
Director

cc:
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION
INTEGRATION
DIRECTOR, TEST AND EVALUATION, JOINT FORCES COMMAND
DIRECTOR, OPERATIONAL TEST AND EVALUATION DIRECTORATE, SPECIAL
OPERATIONS COMMAND

PROCEDURES FOR OPERATIONAL TEST AND EVALUATION (OT&E) OF INFORMATION ASSURANCE (IA) IN ACQUISITION PROGRAMS

1. Purpose

This document describes the procedures for the evaluation of Information Assurance (IA) during Operational Test and Evaluation (OT&E) for Department of Defense (DoD) acquisition programs.

2. Background

DoD Directive (DoDD) 5000.1, DoD Instruction (DoDI) 5000.02, DoDI 8580.1, and the Defense Acquisition Guidebook (DAG) provide acquisition policy and procedures. The overarching DoD IA policy is documented in DoDD 8500.01E and DoDI 8500.2. DoDI 8580.1, *Information Assurance in the Defense Acquisition System,* states that program managers shall ensure that IA is fully integrated into all phases of the acquisition, including initial design, development, testing, fielding, and operation. Additionally, all Mission Critical (MC) and Mission Essential (ME) systems must have an appropriate IA strategy that will be reviewed prior to all acquisition milestone decisions, program decisions, and acquisition contract awards. The Department of Defense IA Certification and Accreditation Process (DIACAP) is outlined in DoDI 8510.01.

3. OT&E IA Procedures Update

This document describes Director, Operational Test and Evaluation (DOT&E) procedures for ensuring that DoD information systems provide assured information to the warfighter. These procedures supersede those outlined in the DOT&E policy for OT&E of IA in acquisition programs dated November 21, 2006.

4. Applicability and Scope

These procedures apply to all systems on the Office of the Secretary of Defense (OSD) Test and Evaluation (T&E) Oversight list for OT&E. Operational Test Agencies (OTAs) are encouraged to apply these procedures to non-oversight systems as well. OT&E of systems with Sensitive Compartmented Information (SCI) shall be assessed in accordance with Intelligence Community Directive 503 dated September 15, 2008.

5. Procedures

a. The focus of this document is to evaluate, in a realistic operational environment,[1] an acquisition system's (or system-equipped unit's) IA capabilities to include its ability to detect and react to penetrations and exploitations[2] and to protect and restore data and information.

b. The Test and Evaluation Master Plan (TEMP) must contain an OT&E strategy for IA evaluation in an operational environment, to include systems and networks to be operated by representative end users and system/network administrators. The TEMP shall identify all IA test and evaluation resources required to execute the IA portion of OT&E, to include funding sources and responsible organizations, and shall reference the appropriate threat documentation[3] and the

[1] Operational environment encompasses physical areas and factors (of the air, land, maritime, and space domains) and the information environment. Included within these are the adversary, friendly, and neutral systems that are relevant to a specific joint operation. (Source JP-3-0)

[2] Penetration testing is designed to evaluate the relative vulnerability of the system to hostile attacks. Penetration testers often try to obtain unauthorized privileges (especially attempts to obtain "root" or "superuser" privileges) by exploiting flaws in the system design or implementation (Source: CJCSM 6510.01).

[3] Defense Intelligence Agency, (U) "Information Operations Capstone Threat Assessment." DI-1577-37-07, April 2007, future updates and other documents as appropriate.

procedures described in this document. DOT&E / OTAs will use all available IA-related data from certification, accreditation, and developmental testing to assess the risk of the system entering operational testing.

c. DOT&E and the appropriate OTA shall ensure that IA measures support an evaluation of system effectiveness, suitability, and survivability. If evaluation in an operational environment is deemed to incur unacceptable operational risks, alternative evaluation strategies shall be outlined in the TEMP and the test plan approved for adequacy by DOT&E.

d. Operational Test Plans must include end-to-end IA strategies, including the links to other systems that accept, use, or provide data/information to the system being evaluated. Measures/metrics must evaluate a system in terms of its operational capabilities. Table 1 provides a suggested framework for IA evaluation of a system's operational effectiveness and suitability. OTAs may suggest alternative measures suitable for systems under test. DOT&E will assess the adequacy of metrics specified in the operational test plan to resolve issues for the system-under-test.

Table 1. Suggested Framework for IA Evaluation

Overarching Issue	Do the system's IA capabilities support the system's effectiveness, suitability, and survivability as well as support the Commander's mission accomplishment?
Issue 1	How well do the system's IA capabilities protect the Commander's/user's required data/information?
Measure/Metric 1	- Level of effort (e.g. time) required by the penetration team to achieve penetrations, accounting for system information made available. - Comparison of time to penetrate a system/network with the system mission duration, accounting for system information made available. - Number of attempts that failed to escalate privileges over the total number of attempts. - Adequacy of network scanning and patch management - Adequacy of configuration management - Effectiveness of firewall - Effectiveness of access control list - Impact of vulnerabilities and exploitations
Issue 2	Will the system's IA detection measures support the ability of the commander/user to identify specific attacks?
Measure/Metric 2	- Total number of events/incidents detected in the System-Under-Test (SUT) - Time taken to analyze detected events/incidents in the SUT - Elapsed time between when a penetration was made and when the network defenders detected the penetration in the SUT - Number of successful detections over the total number of penetrations/exploitations - Effectiveness of intrusion detection systems (IDS) - Adequacy of audit logging, including review and analysis
Issue 3	Will the system facilitate the Commander's/user's ability to react to detected penetrations and exploitations?
Measure/Metric 3	- Number of successful reactions over the total number of detected penetrations and exploitations attempted - Time taken by systems/security administrators to react to each incident - Courses of action to support system's mission operation/performance
Issue 4	Will the system facilitate the Commander's/user's ability to restore data/information?
Measure/Metric 4	- Elapsed time between when a penetration was made and when network defenders fully restored the system/network to a trusted state - Time to restore the system's support of operations after initiating restoration plan - Number of instances where data/information were successfully restored over the total number of instances where data/information needed to be restored - Assessment of COOP adequacy against information attacks

e. For Mission Assurance Category (MAC[4]) I and II Classified systems undergoing system/maintenance upgrades, the level of IA testing will be approved by DOT&E on a case-by-case basis.

f. A six-step process for implementation of these procedures is described below. OTAs shall leverage data from the Certification and Accreditation (C&A) and/or Developmental Test and Evaluation (DT&E) wherever feasible. The six steps are:

Step 1: Determination of Applicability of DOT&E IA Procedures
Step 2: Initial IA Review
Step 3: OT&E IA Risk Assessment
Step 4: Operational IA Vulnerability Evaluation
Step 5: Protection, Detection, Reaction, and Restoration Operational Evaluation
Step 6: Continuity of Operations (COOP) Evaluation

Step 1. Determination of Applicability of DOT&E IA Procedures: As the first step, determine whether the candidate acquisition program requires a specific IA evaluation in accordance with this document. In general, the following table can be used for this purpose.

Table 2. Required Application of DOT&E IA Procedures

Acquisition Programs under DOT&E oversight	Apply DOT&E IA Procedures
All Major Automated Information System (MAIS) programs	Yes
Major Defense Acquisition Programs (MDAP), Platform IT (refer to DoDD 8500.01E) products/weapons systems (Mission Critical (MC) or Non-MC) that have interconnections to external information systems or networks	Yes
MDAP, Platform IT products/weapons systems (MC or Non-MC) that DO NOT have interconnections to external information systems or networks	No

Step 2. Initial IA Review: Through Step 1 above, the OTA, with DOT&E concurrence, will determine whether the acquisition system requires IA evaluation. For programs requiring evaluation, DOT&E / OTAs will validate that the applicable MAC, Confidentiality Level (CL), and IA Controls have been assigned and documented in the appropriate IA strategy, certification and accreditation documentation, Joint Capabilities Integration and Development System (JCIDS) document, and the TEMP. The OTA will coordinate with the program manager to integrate IA DT&E and OT&E test requirements, including resource requirements, into the TEMP.

Step 3. OT&E IA Risk Assessment: DOT&E / OTAs will use IA DT&E data to assess residual risks prior to proceeding to Steps 4 and 5. This will be based on the status of the system's IA Controls implementation. Table 3 provides IA Controls significant to OT&E. An Interim Approval to Operate (IATO) or Approval to Operate (ATO) signed by the Designated Accrediting Authority is the required entrance criterion for OT&E. For MAC III systems assigned a CL of Public, further OT&E of IA will not be required unless DOT&E identifies specific concerns. For MAC I and II systems and Sensitive or Classified MAC III systems, the

[4] DoDI 8500.2 defines MAC levels (I, II, or III), and these reflect the mission criticality of the system availability and integrity, level I being the most critical and level III being the least critical.

OTA shall follow Steps 4 and 5. DOT&E will review the OTA Test Plans, to ensure that adequate evaluation of protection, detection, reaction, and restoration functions will be conducted in Steps 4 and 5, and to confirm the adequacy of the integration and resourcing of the IA related OT&E events. Step 3 completion is a prerequisite to Steps 4 and 5.

Table 3. Significant IA Controls and Concerns Relevant to Protect, Detect, React, and Restore Capabilities to be Reviewed during Step 3

	Significant IA Controls and Concerns
PROTECT	Individual identification and authentication (IA controls from the Identification and Authentication subject area) Account management process Application of security configuration or implementation guides Virus protection implementation Defense mechanisms (e.g., Firewall, Intrusion Detection System) deployed at the enclave boundary (IA controls from the Enclave Boundary Defense subject area) Physical access control (IA controls from the Physical and Environmental subject area) Defined IA roles and responsibilities: Training for IA roles and responsibilities Comprehensive vulnerability management process (IA controls from the Vulnerability and Incident Management subject area)
DETECT	Audit trail, monitoring, analysis, and reporting Audit trail records review Host-based Intrusion Detection System
REACT	Disaster Plan Continuity of Operations Plan and Contingency Plan Incident Response Plan
RESTORE/COOP	Transaction roll back and journaling Data backup procedures Trusted recovery procedures Protection of backup and restoration assets

Step 4. Operational IA Vulnerability Evaluation: Working with the intended user's information assurance/network security staff, the OTA will conduct an overt, cooperative, and comprehensive vulnerability assessment in an operational environment. DOT&E / OTAs will use the results from this step to determine if the system is ready for Step 5. The following are guidelines for executing Step 4:

- Use technical and non-technical methodologies to evaluate
  - Configuration management and system IA tools
  - New equipment and IA training
  - IA incident response
  - Patch management and network access controls
- Leverage as much production-representative DT data as possible
- Evaluate the system's inherited controls as identified in the C&A process
- Identify protect, detect, react, and restore capabilities and limitations
- Provide vulnerability evaluation results and recommendations to materiel developers, as appropriate

Step 5. Protection, Detection, Reaction, and Restoration Operational Evaluation: Step 5 should address the protect, detect, react, and restore issues presented in Table 1, for all MAC I systems and Classified/Sensitive MAC II/MAC III systems. The following are the characteristics of Step 5 evaluation[5]:

- An independent (from the developer) and comprehensive evaluation of protect, detect, react, and restore capabilities of the system and the operational vulnerabilities and shortfalls discovered during Step 4, to include their exploitation potential, and their mission impact. This will be conducted in a realistic, system-of-systems, operational environment approved for adequacy by DOT&E.

- Due to limited test durations at OT&E, system information and interconnections may be provided to the penetration/exploitation test team to facilitate the IA evaluation, instead of the test team having to discover the required information/interconnections as part of the evaluation.

- Evaluate the systems' ability to facilitate user and system/network administrator detection of and reaction to penetrations and exploitations. This will support the determination of how well the system's IA measures support mission accomplishment.

- Leverage incident handling reports prescribed in CJCSI 6510.01 regarding detect, react, and respond functions. Findings shall address operational impact.

Step 6. Continuity of Operations (COOP) Evaluation: COOP and contingency plans will be evaluated for all MAC I systems in the context of mission accomplishment in case of an information attack or system failure/malfunction. Steps 5 and 6 may be performed concurrently.

6. Definitions.

Definitions are the same as those provided in DoDD 5000.1, DoDI 5000.02, CJCSI 6212.01D, CJCSI 3170.01F, and DoDI 8510.01.

7. Documentation.

DOT&E will include IA evaluations to support assessment of applicable oversight programs in the DOT&E Annual Report and Beyond Low-Rate Initial Production (BLRIP) report(s) to the Secretary of Defense and Congress, as well as Full Fielding Decision Reviews.

8. Effective Date.

The procedures outlined in this document are effective immediately and will be incorporated in future revisions and updates to DoDD 5000.1, DoDI 5000.02, DoDI 8580.1, the Defense Acquisition Guidebook, and OUSD(AT&L) system assurance guidance (www.acq.osd.mil/sse/ssa).

Dr. Charles E. McQueary
Director, Operational Test and Evaluation

[5] Systems that use the Defense Information Systems Network (DISN) shall ensure that DISN vulnerabilities are mitigated using CJCSI 6211.02C.