Cybersecurity OT&E – Guidance

General Guidance

The TEMP should describe a test and evaluation strategy for cybersecurity that uses relevant data from all sources and includes testing production representative systems in an operationally representative environment. Data sources may include, but are not limited to, information security assessments, inspections, component and subsystem level tests, and system of system tests. As needed, the TEMP can provide details on the cybersecurity test and evaluation strategy in Appendix E.

The purpose of testing cybersecurity during operational testing is to assess the ability of the system to enable operators to execute critical missions and tasks in the expected operational environment. Testing of cybersecurity during OT&E includes the representative users and an operationally representative environment that may include hardware, software (including embedded software and firmware), operators, maintainers, operational cyber/network defense, end users, network and system administrators, help desk, training, support documentation, Tactics, Techniques, and Procedures, cyber threats, and other systems that exchange information with the system under test.

In the memorandum, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs" (April 3, 2018), henceforth referred to as DOT&E 2018, DOT&E specifies that OTAs should evaluate cybersecurity in OT&E via two assessments: a Cooperative Penetration and Vulnerability Assessment (CVPA) and an Adversarial Assessment (AA). The OTA should design the CVPA and AA to identify cyber vulnerabilities, examine attack paths, evaluate operational cyber defense capabilities, and establish the operational mission effects (loss of critical operational capability) in a cyber threat environment while conducting operational missions.

A CVPA characterizes the cybersecurity and resilience of a system in an operational context and provides reconnaissance information about the system in support of the tests providing information for the AA. If possible, the OTA should conduct the events providing data for the CVPA far enough in advance of the AA to enable mitigation of vulnerabilities before proceeding to the AA, but close enough to remain a relevant input to AA planning. The CVPA requires information from events that include an operationally and production representative system unless specific differences are defined and approved by DOT&E prior to execution. The events can be a standalone test events, a series of events (separate from or embedded in other tests), or an operational component of integrated test.

The AA characterizes the operational effects to critical missions caused by threat-representative cyber activity against a unit training and equipped with a system, as well as the effectiveness of defensive capabilities. The AA requires information from events that include a production-representative and operationally configured system with representative operators, users, and cyber defenders, an operational network configuration, and representative missions. Missions can include military, business, command and control, and cyber tasks. The AA events

should include third party or external defenders including those responsible for defending networks connecting to the system under test. The scope of defensive capabilities and extent of defender roles should match the operational deployment and concept of operations for the system. The AA requires information from events conducted in concert with other operational testing, but might require closed environments, cyber ranges, or other operationally representative tools to demonstrate mission effects. OTAs will ensure verification, validation, and accreditation of these closed environments, cyber ranges, or tools according to Service standards.

For information systems that manage financial/fiscal/business activities or funds, OTAs should conduct a Cyber Economic Vulnerability Assessment (CEVA), see the DOT&E memorandum, "Cyber Economic Vulnerability Assessments (CEVA)" dated January 21, 2015.

Cybersecurity Information for the Body of the TEMP

The TEMP describes the cybersecurity OT&E strategy in the following paragraphs:

- Paragraph 1.3. System Description. Describe the operational configuration and the concept of operations for deployment and operation of the system. Specify and identify the cyber defense responsibilities of the system users, any dedicated system cyber defenders, and the cyber defenders supporting the networks and enclaves on which the system will connect and operate. Identify whether the system has specialized components such as cross-domain solutions, industrial control systems, non-internet data transfers, and data transfer via alternate media such as radio frequency and data links.
- Paragraph 1.3.4. System Threat Assessment. Describe the cyber portion of the complete threat environment in which the system will operate. An advanced cyber threat is appropriate for all systems. Reference the applicable available threat documents, including but not limited to the most recent Defense Intelligence Agency Computer Network Operations Capstone Threat Assessment and component-validated threat documents for the system.
- Paragraph 2.5. Integrated Test Program Schedule. Show on the Integrated Program Test Schedule all events (tests, inspections, cyber table tops, demonstrations, etc.) that will provide information for the CVPA, AA, and, if required, the CEVA (Figure 2.1).
- Paragraph 3.3.2. Developmental Test Events. Identify any developmental and integrated test events that will provide data to support the OT&E assessments, identify the OTA for the event, and confirm plans to obtain DOT&E approval of (1) any specific differences from an operationally and production representative system, and the (2) the operational test plan for the integrated event.
- Paragraph 3.5. Operational Evaluation Approach. Describe the strategy for using the cybersecurity results to inform the overall evaluation of operational effectiveness, suitability, and survivability. Confirm that the OT&E strategy and design will examine operational resilience, including the key attributes of prevent, mitigate, and recover.

- Paragraph 3.5.1 Operational Test Events and Objectives. Describe the strategy (single event, multiple events, etc.) for providing the information needed for the CVPA, the AA, and, if required, the CEVA. List the critical issues and measures for cybersecurity.
- Paragraph 3.5.1.1 Events Supporting the Cooperative Vulnerability and Penetration Assessment. For each event providing information for the CVPA, provide the schedule, identify the involved organizations, list the complete set of limitations and constraints with implications for the assessments, describe the architecture of the system under test including anticipated differences from an operationally and production representative system, describe the operational environment, identify activities (e.g., system and network scans, penetration tests, access control checks, physical inspections, personnel interviews, and reviews of system architecture), and describe expected information (which portions of the information in Attachment B of DOT&E 2018). If planning multiple events, then confirm that the set of events combined will provide the complete set of information in Attachment B of DOT&E 2018.
- Paragraph 3.5.1.2 Events Support the Adversarial Assessment. For each event providing information for the AA, provide the schedule, identify the involved organizations, list the complete set of limitations and constraints with implications to the assessments, describe the architecture of the system under test including any anticipated differences from an operationally and production representative system, describe the operational environment, identify activities (e.g., attacks to create observable mission effects, assessment of mission effects using closed environments, cyber ranges, or other tools, "white cards,", etc.), and describe expected information (which portions of Attachment C of DOT&E 2018). If planning multiple events, then confirm that the set of events will provide the complete set of information in Attachment C of DOT&E 2018.
- Paragraph 3.5.1.3 Cyber Economic Vulnerability Assessment (if required). Identify the test teams that will support the CEVA; this should include both a cyber team and an accounting firm. Name the system and economic subject matter experts who will assist in the Cyber Economic Threat Analysis and assess the mission effects of exploitation, and discuss their qualifications for these roles.
- Paragraph 3.5.1.4. Cybersecurity Test Architecture. Either include the diagrams or provide references to available documents that provide diagrams (e.g., DoD Architectural Framework, system specifications, etc.) with the following information:
  - Major sub-systems (e.g., guidance and communication)
  - Connections between the subsystems including their protocols (e.g., target identification receives input from both Link 16 and the fire control radar via a 1553 data bus)
  - External connections, direct (e.g., NIPRNet, SIPRNet, or JWICS) or indirect (e.g., maintenance laptop, Mission Planning System data transfer devices)

  - Physical access points (e.g., operator consoles) and removable media ports (e.g., USB ports, CD/DVD drives)
  - Other systems to which the system will connect (e.g., SATCOM)

- Paragraph 3.5.2.1. Cybersecurity Critical Issues. Identify the critical issues affected by cybersecurity and describe the cybersecurity evaluation criteria.
- Paragraph 3.5.4 Test Limitations. Identify common restrictions that apply to all test events and discuss how these restrictions affect the efficacy or realism of the CVPA, AA, or CEVA (e.g., safety restrictions on altering system data during operations) and any associated mitigations (e.g., white cards, validated laboratory environment).
- Paragraph 4.2.5 Resources for Cybersecurity Tests. Identify resources required to conduct the tests providing information for the CVPA, AA, and CEVA to include funding, organizations, participants (system operators, inherent cyber defenders, external cyber defenders, test teams, etc), test assets (tools, software, data collection, closed environments, cyber ranges, etc.), and related efforts such as verification, validation, and accreditation efforts. Specifically identify capabilities that the cyber teams do not already possess and must develop (attack tools for non-Internet Protocol buses, threat-representative attack capability against specialized components such as cross-domain solutions) and any system-specific capability (closed environments, cyber ranges, or other tools).

Cybersecurity OT&E Information for Appendix E

Appendix E provides an opportunity for expanded discussion of details not already stated in the body of the TEMP. Detailed system architectures and diagrams are an example of the type of information for the appendix. The TEMP only needs a cybersecurity appendix if the main body does not provide references for or includes all needed information.

Examples

TBD

References

Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, DOT&E, 3 April 2018

Cyber Economic Vulnerability Assessments (CEVA), DOT&E, 21 January 2015

Cybersecurity Test and Evaluation Guidebook, DoD, 1 July 2015

Operational Test Conditions for Cross Domain Solutions, 1 August 2016