OPERATIONAL TEST
AND EVALUATION

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

APR 0 3 2018

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

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

References: (a) Director, Operational Test and Evaluation (DOT&E) Memorandum, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," August 1, 2014
(b) Joint Staff J6 guidebook, "Cyber Survivability Endorsement Implementation Guide," Version 1.01
(c) DOT&E Memorandum, "Cybersecurity Operational Test and Evaluation Priorities and Improvements," July 27, 2016
(d) Chairman of the Joint Chiefs of Staff Manual 6510.03, "Department of Defense Cyber Red Team Certification and Accreditation," February 28, 2013
(e) DOT&E Memorandum, "Cyber Economic Vulnerability Assessments," January 21, 2015

This memorandum provides policies and procedures for the test and evaluation of cybersecurity as part of all operational test and evaluation (OT&E) of systems and capabilities in the Department of Defense (DOD). This memorandum supersedes reference (a) and includes processes and procedures from references (b) through (e) for assessing cybersecurity within OT&E. DOT&E will routinely review and update this policy as needed to reflect changes in test and evaluation technology and capabilities.

Background

The DOD acquisition process should deliver weapons systems, platforms and networks that are both secure and resilient in all aspects of the expected operational environment, including cyber.[1] The purpose of testing cybersecurity during OT&E is to assess the ability of the system to enable operators to execute critical missions and tasks in the expected operational

[1] Per DOD Instruction 8500.01, "Cybersecurity," dated March 14, 2014, operational resilience requires three conditions to be met: information resources are trustworthy; missions are ready for information resources degradation or loss; and network operations have the means to prevail in the face of adverse events.

environment. DOT&E will consider adherence to the guidance contained in this memorandum and cited references when reviewing and assessing the adequacy of cybersecurity in all operational tests.

Applicability

Any electronic data exchange (however brief and regardless of format, means of transmission, or physical "air-gap") provides an opportunity for a cyber threat to deny, degrade, disrupt, destroy, deceive, or manipulate information critical to military operations. Therefore, while the procedures in this memorandum apply to all system acquisition programs under DOT&E oversight, Operational Test Agencies (OTAs) should also apply them to all systems requiring cybersecurity in OT&E. The OTAs may tailor these procedures specifically to support the evaluation of weapons, platforms, networks and other systems that handle or transfer data.

DOT&E requires testing of cybersecurity during OT&E to include the representative users and an operationally representative environment. This 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 (TTPs), cyber threats, and other systems that input or exchange_information with the system under test, as applicable. When conducting OT&E, OTAs should evaluate cybersecurity defenses (inherent as well as external), identify vulnerabilities, characterize the mission effects from exploitation of cyber vulnerabilities, and evaluate the resilience of the system to support critical mission functions.

Certification, Accreditation, and/or Authorization processes should inform OT&E, but are not substitutes for OT&E, and completion of these processes may be necessary prior to the conduct of OT&E.

With prior DOT&E approval, OTAs may deviate from the procedures in this memorandum in order to meet the specific needs for testing unique weapon systems, platforms, and networks. OTAs should tailor operational test plans as needed_for DOT&E review and approval.

Procedures

OTAs should evaluate cybersecurity in OT&E via two assessments: a Cooperative Vulnerability and Penetration Assessment (CVPA) and an Adversarial Assessment (AA). The CVPA and AA should be designed 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. The OTA, with DOT&E review and approval, should integrate developmental and operational testing where possible to assure sufficient data is obtained to meet OT&E objectives/measures. CVPA and AA results will inform the OTA's overall evaluation of operational effectiveness, suitability and survivability.

OTAs should ensure that cybersecurity assessments also examine the cyber defenders' employment of automated cybersecurity defenses (e.g., the Host Based Security System, or other intrusion detection/prevention systems), and should to the greatest extent practical use automated test and data collection tools.

OTAs should design OT&E to examine operational resilience, including key attributes such as:[2]

- Prevent: The ability to protect critical mission functions from cyber threats.

- Mitigate: The ability to detect and respond to cyber-attacks, and assess resilience to survive attacks and complete critical missions and tasks.

- Recover: The resilience to recover from cyber-attacks and prepare mission systems.

Prior to Test

Attachment A contains cybersecurity–unique factors OTAs should consider when preparing for OT&E. Test preparation should identify critical missions and review risks to those critical missions in a contested cyber environment. OTAs should review key program documentation, such as Program Protection Plans, System Engineering Plans, and threat documents such as the Validated Online Lifecycle Threat to identify cybersecurity information relevant to planning OT&E. OTAs should also review risks introduced by the system supply chain to critical missions. OTAs should review and consider data from developmental test events (such as the Cooperative Vulnerability Identification and Adversarial Cybersecurity Developmental Test and Evaluation) and any integrated tests previously conducted. When designing OT&E, OTAs should also consider the following factors in determining the scope of cyber assessments:

- Operational context. Identify the missions supported, mission load (if networked), the operators, the cyber defensive capabilities and support (including third party cybersecurity defenders and physical security), and the means by which the OTA can obtain cybersecurity defense data within those contexts.

- System extent. Identify risks to critical missions from the system supply chain as well as external (or "plug in") capabilities and determine whether they should be assessed as part of the system "attack surface." This may include maintenance peripherals, mission loaders, and other similar devices. Obtain current physical and logical system and network diagrams from the program office.

- System-unique attributes. Review system architectures and operating processes to identify system and network attributes that may enable attack vectors for the system under test (SUT). Identify all key performance parameters and operational

[2] Formerly "Protect, Detect, React, and Restore," key attributes are described in reference (b).

requirements (such as Cyber Survivability Endorsement requirements) that require verification per reference (b) or the capability documentation.

- Specialized components. Identify components such as cross-domain solutions, industrial controls, non-internet data transfers, and data transfer via alternate media such as radio frequency and data links. OTAs will find additional guidance via reference (c).

Cooperative Vulnerability and Penetration Assessment (CVPA)

The CVPA uses data taken from cooperative cybersecurity test events to characterize the cybersecurity and resilience of a system in an operational context and provide reconnaissance of the system in support of the AA.

The CVPA should be conducted as early in the operational test cycle as possible, and should be integrated with developmental tests as applicable. DOT&E will approve in writing the cybersecurity test plans as part of or as an appendix to the overall system test plan.

If possible, the OTA should conduct these events 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. Program office representatives, including developer support, are encouraged to participate during the CVPA to observe and characterize vulnerabilities, potential exploits, and follow-on fixes. The CVPA requires an operationally and production representative system unless specific differences are defined and approved by DOT&E prior to CVPA execution. Attachment B lists the minimum data required from a CVPA._If conducted on a live/operational network, cyber teams must conform to the guidance provided via reference (d).

CVPA data and tests include system and network scans, vulnerability validation, penetration tests, access control checks, physical inspection, personnel interviews, and reviews of system architecture and components to characterize the cybersecurity defensive status of a system as deployed and operated in the operational environment, including any third party or external defenders.[3] The OTA should identify relevant cyber hygiene metrics (including Risk Management Framework controls) as applicable. Following the CVPA, the Program and OTA may review the potential mission effects for inclusion in the test report. The CVPA report should document the system configuration as observed, all test events executed (including both failed and successful events), observations, findings, and results. CVPA results should be provided to DOT&E, the Services, relevant authorizing officials, involved program offices and cyber teams conducting additional testing as soon as possible and no later than 30 days after completion of the last CVPA test event.

The CVPA can be a standalone test event, a series of events (separate from or embedded in other tests), or an operational component of integrated test. To the extent possible, CVPA tests should be integrated with other test events, including (where approved) developmental tests.

[3] For CVPAs, OTAs should ensure that the systems' internal and external defenders are available, but OTAs may need to limit active defender actions to maintain the cooperative nature of the assessment. Additionally, OTAs must gather all relevant detection and relevant passive defense data (e.g., logs, trouble tickets, etc).

DOT&E will approve the selected approach as part of the test strategy in the Test and Evaluation Master Plan (TEMP) and the operational test plan.

Adversarial Assessment (AA)

The purpose of the AA is to characterize the operational effects to critical missions caused by threat-representative cyber activity against a unit trained and equipped with a system, as well as the effectiveness of defensive capabilities.[4] During the AA, the adversary team should focus attacks on disrupting the critical missions. If an opposing force commander is part of the test structure, the OTA should synchronize the AA activities with that commander. OT&E should examine relevant insider, nearsider, and outsider threat postures.[5] Personnel or equipment safety considerations could constrain the OTA's ability to demonstrate these mission effects. In these limited circumstances, and with prior DOT&E approval, OT&E may use closed environments, cyber ranges, or other validated and operationally representative tools to demonstrate mission effects. OTAs will ensure complete verification, validation, and accreditation (VV&A) of these closed environments, cyber ranges, or other validated and operationally representative tools according to Service VV&A standards. Attachment C lists the minimum data required from the AA.

The OTA should conduct the AA on a production-representative and operationally configured system, and identify any test/system deviations for review and approval by DOT&E prior to test. The use of cyber teams to attack the system must conform to the requirements of reference (d) and cyber attacks should be carried to their conclusion or the limitations of the cyber team's capabilities. Where possible, the OTA should assess the efficacy of any vulnerability mitigations not previously examined in prior tests. For systems processing financial data, mission effects should be determined via the guidance on Cyber Economic Vulnerability Assessments provided in reference (e).

Where limitations due to operations or safety arise, or in the interest of time, the OTA may provide system access to the AA team via "white card" insertion to enable required test activities and data collection in the time available.[6] In limited situations, and with DOT&E pre-approval, OTAs may inject "white cards," with the assistance of trusted agents, to stimulate and collect mission effects data.

The term "adversarial" describes only the focus of the assessment – how an adversary could exploit the system. The OTA, program office, user subject matter experts, and supporting agencies should work together in the design of the AA, use of trusted agents, and system

[4] For all systems, an advanced threat is the appropriate level of cyber threat. Missions for systems under test can include military, business, command and control, and cyber tasks.

[5] These postures are defined in reference to the SUT, but not necessarily the network or enclave on which the system resides. Therefore, "insider" = a system user who is authorized both physical and logical access to the SUT (Note: remote insider = a system user not authorized physical access, but authorized logical access, such as a remote administrator); nearsider = a user authorized physical access to the system, but not authorized logical access to the SUT; outsider = someone not authorized either physical or logical access to the SUT.

[6] A "white card" is a simulated event in an operational test. OTAs may use "white card" simulations if the cyber team cannot access the system externally to enable nearsider and insider evaluations, while preserving as much operational realism as possible.

accesses. The AA should include representative operators, users, and cyber defenders; an operational network configuration, with a representative mission; and expected network traffic/mission load.

The OTA should arrange the participation of any third party or external defenders, including those responsible for defending networks connecting to the system under test, and identify the extent of defender involvement, data collection requirements, and passive or active measures that the defenders should take. Defender observations and activities could include validation of procedures and supporting defensive capabilities required for successful mission accomplishment. The scope of these defensive capabilities and the extent of defender roles during operational testing should match the operational deployment and concept of operations for the system. Data collection should support evaluation of cyber responses, mission effects, and operational continuity plans. The OTA should confirm that resilience and continuity plans include protecting backups and failovers against compromise to enable restoration to a secure state as applicable.

Roles and Responsibilities

- DOT&E shall:
  - Provide and update guidance and procedures for integration of cybersecurity within OT&E;
  - Review and approve adequacy of OT&E (including both cybersecurity phases, CVPA and AA) planning in TEMPs and OT&E Test Plans (including both CVPA and AA) for systems under oversight;
  - Monitor OT&E planning and observe OT&E execution to determine adequacy; and
  - Review and approve proposals for alternate data sources and procedural deviations from those described in this memorandum.

- OTAs shall:
  - Obtain all necessary program documentation to support OT&E, (including but not limited to) system architectures, network diagrams, systems engineering plans, program protection plans, user manuals, training materials, tactics guides and procedures, certification and accreditation artifacts, results of previous testing, technical specifications, and any unique or proprietary materials from weapons/platform/network system program offices;
  - Provide all necessary documentation and references to DOT&E;
  - Design, plan, manage, and execute OT&E;
  - Provide a test concept brief to DOT&E 180 days in advance of test execution;
  - Write OT&E Test Plans that include cybersecurity objectives, measures, activities, and test resources and provide them for DOT&E review and approval no later than 60 days prior to test;
  - Update DOT&E representatives routinely on test conduct, findings, and issues; and
  - Provide data from Attachments B and C to this memorandum to DOT&E as soon as practical, but no later than, 30 days after completion of each CVPA and/or AA.

- Program Managers should:
    - Attempt to schedule CVPAs far enough in advance of the AA to enable mitigation of vulnerabilities before proceeding to the AA;
    - Resource/fund all cybersecurity test events;
    - Provide TEMPs (that include planning for CVPAs and AAs) to the OTAs and DOT&E for review and approval;
    - Obtain approval to connect/operate for the SUT prior to the final Operational Test Readiness Review (OTRR);
    - Provide production and operationally representative system and networks supporting OT&E;
    - Ensure representative/trained operators are available for OT&E;
    - Collaborate fully with the OTAs to plan and execute CVPAs and AAs; and
    - Provide all necessary program documentation to the OTA and DOT&E (including but not limited to) system architectures, network diagrams, systems engineering plans, program protection plans, user manuals, training materials, tactics guides and procedures, certification and accreditation artifacts, results of previous testing, technical specifications, and any unique or proprietary materials.

Test Documentation

TEMP

The DOT&E TEMP Guidebook (http://www.dote.osd.mil/tempguide/index.html) provides guidance for cybersecurity content in the TEMP. The TEMP should define a test and evaluation strategy that includes cybersecurity, uses relevant data from all available sources, and includes testing 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. The program office and OTA should integrate cybersecurity testing into the overall evaluation planning and schedules. The TEMP should identify resources required to execute CVPAs and AAs and include funding, organizations, test assets, and threat documentation. The TEMP should also 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 be fielded, and how the accomplishment of these responsibilities will be tested.

The TEMP should describe how the systems engineering analysis and results (conducted early in the acquisition process) were used to identify and assess mission critical tasks in a cyber contested environment. The TEMP should also describe how this analysis considered the role of system operators to ensure critical mission tasks in a cyber degraded environment. The results of this analysis should inform the T&E strategy in the TEMP as well as developmental and operational test designs.

Operational Test Plan

Attachment D provides cyber requirements for the content of an OT&E test plan. OT&E test plans should contain details of how the OTA will test to provide the required cybersecurity data, including resources, schedule, OTA-specific test and data collection tools, and data to be collected. The OTA should consider requirements such as the use of embedded cyber team observers, trusted agents, data collectors, instrumentation/data collection systems, and cyber defenders in the OT&E test plan. The OT&E test plan should identify the test environment, and all known test limitations, along with their implications and mitigations. Test plans should also require system restoration and the removal of all malware, sensors, and other modifications that were implemented in support of cybersecurity testing at the end of the test.

Test Data

OTAs should authenticate/validate data as needed and provide data from Attachments B and C of this memorandum to DOT&E as soon as practical, but no later than, 30 days after completion of the CVPA or AA. When OT&E identifies problems that may require system modifications, retesting, or re-accreditation – or identifies risks to other systems – the OTA should provide the data as soon as possible to the Services, cybersecurity service providers, military commanders, relevant authorizing officials, involved program offices and other test agencies, as appropriate. OTAs should describe the circumstances of the test, list any limitations and constraints (and associated effects on the assessment), fully describe the cyber-attacks and defensive actions, and discuss all observed and assessed mission effects.

Robert F. Behler
Director

Attachments:
A – Pre-OT&E Considerations
B – Cooperative Vulnerability and Penetration Assessment Data Requirements
C – Adversarial Assessment Data Requirements
D – Operational Test Plan Cybersecurity Content

cc:
Secretaries of the Military Departments
Under Secretary of Defense for Research and Engineering
Under Secretary of Defense for Acquisition and Sustainment
Commander, U.S. Cyber Command
Director, Cost Assessment and Program Evaluation
Department of Defense Chief Information Officer
Assistant Secretary of the Army for Acquisition, Logistics, and Technology
Assistant Secretary of the Navy for Research, Development, and Acquisition
Assistant Secretary of the Air Force (Acquisition)
Director, Joint Chiefs of Staff
Director, National Security Agency
Director, Defense Information Systems Agency
Director, Defense Intelligence Agency
Director, Missile Defense Agency
Director, Army Test and Evaluation Office
Director, Navy Test and Evaluation and Technology Requirements (OPNAV N94)
Director, Test & Evaluation, Headquarters U. S. Air Force
Assistant Commandant of the Marine Corps
Commander, Joint Force Headquarters, DOD Information Networks

Attachment A
Pre-Operational Test and Evaluation (OT&E) Considerations

The Operational Test Agency (OTA) should consider the following cybersecurity–unique factors when planning for/prior to commencing OT&E.

Planning

- Is there a Director, Operational Test and Evaluation (DOT&E)-approved test plan?
- Has the program incorporated cybersecurity requirements from the Cybersecurity Strategy and Program Protection Plan?
- Has the planning incorporated the results of prior tests or assessments?
- Has the program obtained an Authority to Operate?
- Has the program provided all relevant documentation and developmental risk assessments to describe potential effects to critical missions from the system supply chain?
- Has the program provided the OTA with the most current updated system and network architecture?
- Does the test plan include monitoring of cyber defender actions and defender data collection, and evaluation of all defensive capabilities?
- Does the test plan include a means to collect data on mission effects?
- Are current or planned cyber threat tools identified and made available for employment?
- Have the Cyber Rules Of Engagement been identified and agreed upon by appropriate organizations?

Developmental Test & Evaluation

- Will any proposed integrated testing (including cybersecurity) planned to provide operational test data during developmental tests be provided to DOT&E for approval prior to commencement of operational test?
- If the program conducted a Cooperative Vulnerability Identification or Adversarial Cybersecurity Developmental Test and Evaluation, has it provided the results to the OTA?
- Does the program have any unmitigated Defense Information Systems Agency Category 1 vulnerabilities?
- If the program conducted a cyber table top, concept rehearsal, or similar analysis, has it provided the results to DOT&E, the OTA, and teams supporting both the Cooperative Vulnerability and Penetration Assessment and Adversarial Assessment?

Resources

- Will operational cyber defenders be in place and participating?
- Are all other resources required for cybersecurity testing available and in place?
  - Correct software version(s)?
  - All external interfaces and data sources/exchanges?
  - System-unique equipment?
  - Test team resources such as accounts, workspace, and reference materials?
  - Infrastructure, assets and personnel?

Attachment B
Cooperative Vulnerability and Penetration Assessment (CVPA) Data Requirements

The following table lists the minimum data required for a CVPA.

CVPA Data Requirements		
Evaluation Area	**Information**	**Notes**
Test Conduct	• Provide schedule, locations, involved organizations, and complete set of limitations and constraints.	
System Under Test (SUT) Configuration	• Describe the SUT and the operational network to include configuration, addresses, etc. • Identify system protection mechanisms (example: firewall, Intrusion Detection/Prevention Systems).	• If the test team observes any differences in the SUT from the system architecture used in planning, identify these as well as any changes made during the CVPA to support later Adversarial Assessment (AA) testing.
Vulnerability and Exposure Identification - Scans	• Enumerate cyber vulnerabilities, exposures, and patching status. • Data should describe the nature of the vulnerability/exposure, where found (portions of the SUT, network, etc.).	• List tools, versions, and settings used to complete scans.
Penetration Test	• For all discovered and known vulnerabilities and exposures, determine the extent of achieved access. • Report all explored vulnerabilities and exposures with achieved access. • Report on all automated cybersecurity tools that captured information on exploits.	• Penetration test results provide basis for developing potential attack vectors that the AA can continue to explore mission effects. Review of exploit data can determine the detectability of the exploit or attack.

Attachment C
Adversarial Assessment (AA) Data Requirements

The following table lists the minimum data required for an AA.

AA Data Requirements		
Evaluation Area	**Information**	**Notes**
Test Conduct	• Provide schedule, locations, involved organizations, and all limitations and constraints.	
System Under Test (SUT) Configuration	• Describe the SUT and the operational network to include configuration, addresses, etc.	• Identify any observed differences from the system architecture used for test planning as well as any changes made during the AA.
Attack Vector Data	• Record and report data on the results of all attack activities. • For each activity, report address, port/protocol, time line, privilege level, tool used, target and source system.	• Coordinate the reporting format of the data with Director, Operational Test and Evaluation (DOT&E). • Data collection logic is provided via the DOT&E classified extranet.
System Protection	• Report on those attacks that succeed and the specific system configurations or causes.	• Identify the root cause if known for attack success.
System Monitoring, Analysis, and Detection	• Organization (who/how detected/not detected) • Detected activity • Mode of Detection (automated, manual, user-reported) • Tool Data (name, type, version) • Timelines	
System Response	• Organization • Activity prompting response (detection, white card, false alarm, etc.)	• The Operational Test Agency should collect data on response and restoral actions. • Multiple organizations might have individual

	• Reaction (e.g., incident report, block access, remove system) • Restoration (operational, cyber, continuity of operations (COOP)) • Time response action initiated • Time response action completed • Outcome of response action (adversary access removed, malware removed, response action failed) • Evaluation of whether backup systems are impacted by compromises of primary systems, and responses of both systems • White cards used, if any.	response actions to a particular event and the OTA should collect all measures for each. • One organization might have multiple reactions to a particular event (e.g., incident report to higher-tier org., followed by an Internet Protocol block at the direction of the higher-tier org.) • *Operational Restore* refers to the recovery of affected system functions • *COOP is the* implementation of an alternate capability using a different system or process. • *Cyber Restore* refers to the complete removal of the adversary from the affected system.
Mission Effects	• Report observed or estimated mission effects due to either attack vectors or defensive response and how those effects influenced mission critical functions. • Where direct measurement is not feasible, estimate effects, e.g., via Subject Matter Experts, cyber ranges, or simulations. Report white cards used, if any.	• Should include performance parameters already being used to assess system effectiveness. • Adverse effects could include specific mission-critical tasks or mission/system functions.

Attachment D
Cybersecurity Content for Operational Test Plans

Item	Description
Test and Evaluation Master Plan (TEMP) Linkage	The test plan should be consistent with the approved TEMP
Architecture	The test plan should define the architecture of the system(s) under test. Specific system information should encompass: • Major subsystems within the scope of test or their interfaces to other components or systems • Interconnections between major subsystems (e.g., data bus links), external connections (e.g., networks), and any physical access points (e.g., USB ports, drives, peripherals, and other media)
Operational Environment	Identify the cyber-attack surface for the system(s) under test. Also, specify and describe the cyber environment for the system(s) under test. Description should include: • Locations, cybersecurity roles, for end users, system/network administrators, maintenance teams • Specific mission threads and tasks addressed in the test plan • The location and anticipated roles of all cyber defenders, and Cybersecurity Service Providers supporting system operation • The threats, techniques, and objectives that the Red Team will portray during the test • Potential safety risks during testing.
Time and Resources	Provide the schedule of test events and resources. Description should: • Show dates and locations for both phases of cybersecurity testing. The Cooperative Vulnerability and Penetration Assessment (CVPA) should be scheduled far enough in advance of the Adversarial Assessment (AA) to enable mitigation of vulnerabilities identified in the CVPA prior to the beginning of the AA. • Identify specific operational users. • Identify the cyber defense agencies/personnel. • Identify the cyber teams arranged to perform test functions. • Identify other test resources such as cyber ranges or specific tools. • Identify any authorizations required to conduct the test.
CVPA	Describe the planned CVPA execution. Describe how the test team will scan and conduct penetration tests. • Describe deviations to the operational configuration and environment as described in the TEMP, and their impact. • Describe anticipated CVPA limitations and how they could affect the test.

	• Describe how the test will collect cybersecurity metrics in accordance with Attachment B. • Specify the data collection methods. These may include: o Automated scanning/exploitation tools o Physical inspection o Personnel interviews o Document reviews • Provide data collection forms and other documents. • Describe specific test and data collection tools and versions. • Describe any limitations or variations and how they will affect the test.
AA	Describe the planned AA execution. • Describe the threat (and validation of the threat) that the adversarial team portray. • List the objectives the adversarial team will pursue and, as available, the attack vectors • Describe any periods of enumeration or "free play" that will occur. • Describe how the test will incorporate the CVPA results. • Describe any limitations or variations and how they will affect the test. The test plan should address: o White cards where necessary. o Cyber range use. • Identify the cyber defenders for the system(s) and identify how the test will gather defense data from those activities. • Provide data collection plans in accordance with Attachment C. • Identify any automated tools for the test. • Identify the methods to determine mission effects. • Provide data collection forms, and other documents. • Describe deviations to the operational configuration and environment as described in the TEMP, and their impact.