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

OPERATIONAL TEST
AND EVALUATION

February 14, 2025

MEMORANDUM FOR U.S. CYBER COMMAND (CYBERCOM)
COMMANDER, ARMY TEST AND EVALUATION COMMAND
COMMANDER, AIR FORCE OPERATIONAL TEST AND EVALUATION CENTER
DIRECTOR, MARINE CORPS OPERATIONAL TEST AND EVALUATION ACTIVITY
DIRECTOR, OPERATIONAL TEST AND EVALUATION FORCE
COMMANDER, JOINT INTEROPERABILITY TEST COMMAND
BALLISTIC MISSILE DEFENSE OPERATIONAL TEST AGENCY

SUBJECT: Cyber Operational Test and Evaluation Guidebook

On December 9, 2024, we published DoD Manual (DoDM) 5000.99, *Realistic Full Spectrum Survivability and Lethality Testing,* which in turn canceled both Director of Operational Test and Evaluation Memoranda "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," April 3, 2018, and "Cyber Economic Vulnerability Assessments," January 21, 2015. Attached to this memorandum is the follow-on guidance that supersedes the canceled memoranda and will serve as interim guidance until the release of the forthcoming joint Developmental Test and Evaluation (T&E) and Operational Test and Evaluation (OT&E) Cyber Guidance.

The Cyber Operational Test and Evaluation Guidebook expands on the policies outlined in DoD Instruction 5000.98, *Operational Test and Evaluation and Live Fire Test and Evaluation,* DoDM 5000.96, *Operational and Live Fire Test and Evaluation of Software,* and DoD Manual (DoDM) 5000.99, *Realistic Full Spectrum Survivability and Lethality Testing,* with key guidance for details and procedures. It outlines necessary testing to inform full spectrum survivability and lethality assessments of DoD systems throughout their operations and sustainment due to advances in adversary kinetic and non-kinetic threats, tactics, techniques, and procedures.

Conducting adequate and effective cybersecurity OT&E is crucial to inform evaluations of operational effectiveness, suitability, and survivability of DoD systems and underscores the importance of OT&E in assessing a system's operational resilience. For programs listed on the OT&E Oversight List, adherence to the Cyber Operational Test and Evaluation Guidebook will be a key factor in evaluating the adequacy of T&E strategies and plans.

DOT&E will consider adherence to this cybersecurity guidance, and cited references, as an essential part of comprehensive full spectrum survivability and lethality assessments when reviewing and assessing adequacy of all operational tests.

Dr. Raymond D. O'Toole, Jr.
Director (Acting)

Attachment:
Cyber Operational Test and Evaluation Guidebook

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

Department of Defense

Cyber Operational Test and Evaluation Guidebook

Version 1.0
31 January 2025

This Guidebook will be rescinded upon the publication of joint Development Test (DT) Operational Test (OT) cyber guidance.

Executive Summary

The Cyber Operational Test and Evaluation Guidebook amplifies the policies outlined in Department of Defense (DoD) Instruction (DoDI) 5000.98 and DoD Manual (DoDM) 5000.99 with key guidance for details and procedures. It outlines the necessary cyber testing to inform evaluations of operational effectiveness, suitability, and survivability of systems under test (SUTs) and underscores the importance of operational test and evaluation (OT&E) in assessing a system's survivability and its capacity to prevent, mitigate, recover from, and adapt to adverse cyber-events. This guidebook supersedes, incorporates, and expands on guidance found within the rescinded Director of Operational Test and Evaluation (DOT&E) Memoranda "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs" (April 3, 2018) and "Cyber Economic Vulnerability Assessments," (January 21, 2015) and will serve as interim guidance until the release of the forthcoming joint developmental test and evaluation (DT&E) and OT&E guidance. The intent of this document is to fill the void of the rescinded memoranda. Forthcoming guidance will address specific application of the Adaptive Acquisition Framework (AAF) pathways to operational test (OT) events. Note: A forthcoming cyber developmental test (DT) DoDM and cyber DT guidebook is set to be released later in 2025 which will provide policy and guidance for cyber DT and pre-OT and will be referenced within this guidebook.

This guidebook's appendices include guidance and checklists designed for Operational Test Agencies (OTAs) and Operational Test Organizations (OTOs) to use in the planning of cyber T&E events. These appendices cover the following:

- Pre-OT considerations
- Cyber content of OT plans
- Cooperative vulnerability and penetration assessment (CVPA) data requirements
- Adversarial assessment (AA) data requirements
- Cyber economic vulnerability assessment (CEVA) requirements

The purpose of cyber OT&E is to assess the ability of the system in the projected operational environment to remain mission ready and safe to operate in a contested cyberspace and to enable operators to execute critical missions and tasks in the multi-domain operational environment. Conducting adequate and effective cyber OT&E is crucial for ensuring the operational cyber survivability of DoD systems. For programs listed on the Test and Evaluation (T&E) Oversight List for OT, adherence to this guidebook will be a key factor in evaluating the adequacy of T&E strategies and plans. Programs not under DOT&E oversight will also benefit from following this guidance. Following and incorporating this guidance into planning, scheduling, executing, and reporting OT&E, should meet the intent of the DOT&E's policies. DOT&E will consider adherence to this guidance and cited references when reviewing and assessing the adequacy of cyber testing in all operational tests.

Questions and issues regarding the content and format of this document or technical issues involving test and evaluation, please email the DOT&E Pillar 3 mailbox with subject line: Cyber OT&E Guidebook at osd.dote.pillar-3@mail.mil.

Table of Contents

1 General Information

This guidance supersedes, incorporates, and expands on guidance provided by both DOT&E Memoranda "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs" (April 3, 2018) and "Cyber Economic Vulnerability Assessments" (January 21, 2015) for assessing cyber survivability within OT&E. DOT&E will routinely review and update this guidebook as needed to reflect changes in T&E technology and capabilities, and the needs of the user community.

This version of the guidebook provides guidance on how to implement cyber OT&E directives codified in DoDI 5000.98, DoDM 5000.99, and previously released DOT&E memoranda. This guidebook will be rescinded upon the publication of joint DT –OT guidance. It is necessary to complete DT and pre-OT activities prior to beginning the activities provided in this guidebook. For DT and pre-OT guidance and considerations reference the "Cyber DT&E Guidebook" (February 10, 2020), the forthcoming cyber DT DoDM, and the forthcoming cyber DT guidebook.

1.1 Introduction

This guidebook supports DoDM 5000.99, Realistic Full Spectrum Survivability and Lethality Testing, in describing *how to* perform data-driven, mission-impact-based analysis and assessment methods for iterative cyber OT&E used throughout an acquisition's entire life cycle, regardless of the chosen AAF pathway.[1] Appendix G of this guidebook provides references to relevant cyber T&E content from multiple policies to describe implementation. For details, the reader is encouraged to go directly to source documents. Footnoted references assist with understanding the source of a specific statement. This guidebook specifically supports and references:

- DoDI 5000.98, Operational Test and Evaluation and Live Fire Test and Evaluation
- DoDM 5000.96, Operational and Live Fire Test and Evaluation of Software
- DoDM 5000.99, Realistic Full Spectrum Survivability and Lethality Testing
- DoDM 5000.100, Test and Evaluation Master Plans and Test and Evaluation Strategies
- DoDM 5000.102, Modeling and Simulation Verification, Validation, and Accreditation for Operational Test and Evaluation and Live Fire Test and Evaluation
- DoD Test and Evaluation Enterprise Guidebook

Cyber T&E is iterative and starts as early as possible and should integrate as many data sources as available. This guidebook recognizes that cyber OT&E and the Risk Management Framework (RMF) processes may be complementary. RMF is a necessary process to support gaining and retaining an authorization to operate (ATO) but does not replace cyber OT&E. Assessment and authorization processes should inform OT&E, but are not substitutes for OT&E,

[1] DoDI 5000.02, "The Operation of the of the Adaptive Acquisition Framework," January 2020.

and completion of these processes may be necessary prior to conducting OT&E. OT&E results and findings should inform and be rolled back into the RMF continuous monitoring phase.

1.2 Applicability

The procedures in this guidebook apply to all DoD acquisition programs and systems including, but not limited to:

- Defense business systems
- Weapon systems
- Industrial control systems
- Supervisory control and data acquisition systems
- Acquisition programs
- National security systems
- Non-developmental items
- Hull, mechanical, and electrical systems

DOT&E requires cyber testing during OT&E to include both the representative users and an operationally representative environment. Representative users encompass a wide range of personnel who interact with the SUT during its operational use. This includes operators, cyber and network defenders, maintainers, end users, network and system administrators, help desk personnel, and any other individuals whose roles involve direct interaction with the SUT. An operationally representative environment may include the hardware; software; operational cyber/network defense; tactics, techniques, and procedures (TTP); and other systems that input or exchange information with the SUT under a cyber threat. For OT&E to be more efficient and effective, OTAs should have access to and build upon data from DT&E to better understand the system and help minimize rework. During OT&E, the OTAs/OTOs should collect data to:

- Identify vulnerabilities.
- Evaluate cyber defenses.
- Evaluate system integration into the DoD cyber warfighting enterprise.
- Demonstrate and characterize effects to the missions the system is being fielded to support (mission effects) from exploitation of cyber vulnerabilities.
- Evaluate the resilience of the system to execute critical functions.

With prior DOT&E approval of a tailored test plan, OTAs may deviate from the procedures in this guidebook to meet the specific needs for testing unique weapon systems, platforms, and networks. DOT&E will consider adherence to this guidance and cited references when reviewing and assessing the adequacy of cyber testing in all OT events.

1.3 Audience

Iterative cyber OT&E requires multiple stakeholders working collaboratively. This guidebook provides guidance specifically directed to T&E stakeholders in OTAs, OTOs, and to program managers (a program's acquisition, contract, and cyber personnel) for activities enabling cyber OT&E. It also considers the roles of senior decision makers, program executives,

oversight organizations, authorizing officials, requirement sponsors, warfighters, system development and test teams, and industry partners in the execution of adequate cyber OT&E.

1.4 Terminology

The Services/Components/Agencies and other organizations involved in cyber OT&E may use different terms for the people or teams discussed in this guidebook. The actions described in this document are more important than the titles of those performing the activities.

A key term used in this guidebook when discussing cyber OT&E activities is stakeholders, which generally include the following organizations and personnel:

- DOT&E
- The Executive Director of Developmental Test, Evaluation, and Assessments, within the Office of the Under Secretary of Defense for Research and Engineering
- DoD Service/Components/Agency decision authorities
- Requirement sponsors
- Combatant commands, mission owners, warfighters
- Program management offices
- Cyber T&E organizations
    - Chief Developmental Tester, Lead Developmental Test Organizations
    - OTAs/OTOs
- Authorizing officials

Another key term, SUT, refers to a subcomponent, component, subsystem, system, or system-of-systems to include the network environment, end users, administrators, cyber defenders, and cyber threats, depending upon the context of the cyber OT&E event. For OT, the boundary/scope of testing may extend beyond the SUT to include maintenance laptops, system(s) supporting the test which enable access to the SUT from external networks, or other systems not within the program's accreditation boundary.

This guidebook uses the terminology of prevent, mitigate, and recover/adapt for consistency with the key attributes as described in the "Cyber Survivability Endorsement Implementation Guide" and the "Manual for the Joint Capabilities Integration and Development System."[2,3]

[2] Cyber Survivability Endorsement Implementation Guide (CSE IG), version 3.0, July 2022, Joint Staff J6.

[3] Manual for the Joint Capabilities Integration and Development System, October 30, 2021, Joint Staff J8.

2 Roles and Responsibilities

The following cyber-test-specific actions provide guidance to OT&E stakeholders regarding expected actions to facilitate cyber OT&E.

DOT&E:

- Provides and updates guidance and procedures for integration of cyber threats within OT&E.
- Reviews and approves adequacy of OT&E (including both cyber assessments, CVPA and AA) planning in Test and Evaluation Master Plans (TEMPs)/T&E Strategies and OT&E test plans (including both CVPA and AA) for systems under oversight.
- Monitors OT&E planning and observes OT&E execution to determine adequacy.
- Reviews and approves proposals for alternate data sources and procedural deviations from those described in this guidebook or the TEMP/T&E Strategy.

OTAs/OTOs:

- 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, any supply chain-relevant information, 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.
- Consider providing an early concept brief to DOT&E 360 days in advance of test execution.
- Provide a test concept brief to DOT&E 180 days in advance of test execution.
- Write OT&E test plans that include cyber testing 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.
- Provide data from Appendix C and Appendix D of this guidebook to DOT&E as soon as practical, but no later than 30 days after completion of each CVPA and/or AA.
- Serve as a member of the cyber working group (CyWG) and participate in the following:
    - Defining cyber OT&E requirements and resources for inclusion in requests for proposal (RFPs), contracts, and other agreements.
    - Reviewing and assessing system developer contractor cyber test plans.
    - Supporting cyber OT&E planning, preparation, and coordination activities.
    - Supporting efforts to conduct critical, vulnerability, and supply chain analyses.

  - Providing cyber OT&E inputs to inform the program's acquisition strategy.
  - Providing cyber OT&E inputs to the development of the TEMP/T&E strategy.

Program managers:

- Consider scheduling CVPAs far enough in advance of the AA to enable mitigation of vulnerabilities before proceeding to the AA, when possible and doing so does not affect the system configuration.
- Resource/fund all cyber OT&E events.
- Author and provide TEMPs (that include planning for CVPAs and AAs) to the OTAs and DOT&E for review and approval.
- Obtain the authority to connect/ATO, as required, for the SUT prior to the final operational test readiness review.
- Provide and coordinate production and operationally representative system and networks supporting OT&E.
- Ensure representative/trained users (as defined as Section 1.2 of this guidebook) are available for OT&E.
- Collaborate fully with the OTAs to plan and execute CVPAs and AAs.
- 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, any supply chain-relevant information, and any unique or proprietary materials.

The CyWG:

- For a complete list of CyWG roles and responsibilities reference forthcoming cyber DT DoDM and the cyber DT guidebook.
- Cyber OT&E specific responsibilities include:
  - Provide cyber subject matter experts (SMEs) to support cyber OT&E.
  - Characterize the attack space.
  - Coordinate with appropriate intelligence resources.

3 Approaches to Testing

3.1 Agile Development Strategy and OT&E

For programs executing an Agile deployment strategy, incremental cyber OT&E in the operational or production environment is essential to ensuring systems exposed to operational threats are cyber survivable throughout the system maturation and Agile deployment process. Iterative and incremental cyber OT&E should occur as soon as possible following the deployment of new capabilities that potentially increase the attack surface. Agile cyber OT&E should focus on validating the effectiveness of remediations and mitigations to previously identified vulnerabilities and identifying new vulnerabilities and potential mission impacts present in the operational environment. Cyber testing should be conducted on the system in the state(s) in which it was incrementally deployed, regardless of the intended end state and status of system defenders. DoDM 5000.96 contains information on how to conduct T&E for Agile software development programs.

3.2 Recommended Approaches to Integrated Cyber T&E

The CyWG should consider integrating test events to meet the objectives of multiple stakeholders, maximize testing opportunities, align with the program's AAF pathway schedule, generate shared data, and save resources. For OT&E, a key consideration in any integrated test is confirming system maturity and if test conditions are sufficiently representative of operational conditions to enable using the data to meet OT&E needs. As part of the CyWG, OT&E representatives have access to the test schedule and should consider all tests as opportunities to gather data for OT&E needs. Consider the following when looking to use integrated cyber test events for OT&E purposes:

- Do programmatic documents such as the RFP, statement of work, or statement of objectives need language to enable using integrated approaches to cyber T&E for OT&E?
- Do opportunities exist where a test provides the conditions necessary for OT&E?
- Have OT&E stakeholders reviewed all proposed test events to determine feasibility of shared data to meet their needs?
- Do agreements on data management and sharing exist to enable sharing of data?
- Do OT&E stakeholders agree an event will provide information to meet their needs?

The CyWG should consider planning for any of the below described approaches to integrated Cyber T&E.

3.2.1 Integrated Government-Contractor Testing

Use of contractor testing data can inform operational evaluation if it otherwise meets the conditions necessary for OT&E and can be independently observed/validated, but it does not replace acceptance or OT.

3.2.2 Concurrent Functional-Cyber T&E

Cyber testing should be concurrent with functional testing as much as it is both safe and practical to determine the true mission effects that may result from cyber shortfalls and inform effectiveness, suitability, and survivability determinations.

3.2.3 Integrated Government Cyber DT-OT

Coordination for common test objectives and events help to integrate testing into a continuous (rather than segregated) process. This can be achieved if the SUT is sufficiently production representative or the equivalent based on the acquisition pathway (e.g., Middle Tier of Acquisition uses a prototype), and test events are conducted with real-world operators in the: (1) operational environment and/or (2) sufficiently realistic emulated environment. Such potential integration should be addressed in the TEMP/T&E Strategy and include verification, validation, and accreditation (VV&A) as necessary in compliance with DoDM 5000.102 to establish by the competent authority that an emulated environment is sufficiently realistic. Integrated DT-OT does not replace or eliminate the need for dedicated OT&E and initial operational test and evaluation (IOT&E).

3.2.4 Iterative Cyber T&E

Cyber T&E will start as early as feasible in system development and iterate throughout the system life cycle in response to changes in both the system itself and the conditions in which the system operates to collect data to inform survivability assessments. The CyWG should coordinate with all stakeholders to establish information needs that allow the iterations to build upon one another while minimizing unnecessary repetition. OTAs/OTOs should seek to perform iterative cyber T&E as resources, tasking, and time allows.

4 Cyber Test Procedures

4.1 Overview

OTAs should execute cyber testing in OT&E in two stages: a CVPA and an 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 contested cyberspace while conducting operational missions. The CVPA is an assessment that uses data taken from cooperative cyber test events to characterize the cyber survivability of a system in an operational context and provides reconnaissance of the system in support of the AA. The purpose of the AA is to demonstrate and 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 and the ability to integrate the system into enterprise DoD cyber monitoring, reporting, and response processes.[4] The OTA, with DOT&E review and approval, should integrate DT and OT where possible to assure sufficient data is efficiently obtained to meet OT&E objectives/measures. CVPA and AA results will inform the OTA's overall evaluation of operational effectiveness, suitability, and survivability. More information on CVPAs and AAs can be found below and in Appendix C and Appendix D of this guidebook. Additionally, for financial and business systems that have the potential risk of economic exploitation, OTAs/OTOs must perform a CEVA. More information on CEVAs can be found in Appendix E of this guidebook. Additionally, DoDM 5000.96 provides policy for OT&E and live fire test and evaluation (LFT&E) for software-intensive systems or software embedded in systems.

OTAs should ensure that cyber assessments also examine the cyber defenders' employment of automated cyber defenses (e.g., firewalls and intrusion detection/prevention systems), ability to share data and report incidents to Service- or DoD-level cyber defenders and should to the greatest extent practical use automated test and data collection tools.

OTAs should design OT&E to examine survivability, using the cyber survivability pillars:[5]

- **Prevent:** Design requirements to identify, protect and harden weapon system's functions from adversary cybersecurity threats (to anticipate most likely and greatest risk).
- **Mitigate:** Design requirements to detect and respond to cyber-events making it through defenses; enabling cyber operational resiliency (to complete the mission).
- **Recover:** Design requirements to recover to a "known good" condition after a cyber-event; at a minimum, restore sufficient capability (to fight another day).
- **Adapt:** Enables a sustained capability to adapt to changes in adversary threat and

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

[5] Cyber Survivability Endorsement Implementation Guide (CSE IG), version 3.0, July 2022, Joint Staff J6.

vulnerabilities (to win this war and the next) through processes such as DevOps.

4.2 Prepare

Appendix A of this guidebook contains cyber-unique factors OTAs should consider when preparing for OT&E. As parts of the CyWG the OTAs should acquire the necessary data to inform cyber OT events. During test preparation, OTAs should identify critical missions from sources such as concept of operations (CONOPS) and capabilities documents and review risks to those both safety critical systems and critical missions in contested cyberspace. OTAs should review key program documentation, such as Program Protection Plans, System Engineering Plans, and threat documents such as the Validated Online Lifecycle Threat and other finished intelligence products to identify cyber information relevant to planning OT&E. Other industry standard resources identifying adversary threat TTP and known cyber vulnerabilities in software, hardware, firmware, etc. such as the MITRE ATT&CK knowledge base and Common Vulnerabilities and Exposures database should be reviewed.[6] OTAs should also review all available documentation and associated risks introduced by the system's supply chain to critical missions. This may include a supply chain risk assessment conducted by a cyber test team or Mission Based Cyber Risk Assessment (MBCRA). OTAs should also review and consider data from developmental test events and previously conducted integrated test events. When designing OT&E, OTAs should also consider the following factors in determining the scope of cyber assessments:

- **Operational context:** Identify the missions supported, network capacity, the operators, the cyber defensive capabilities and support (including physical security, assigned Cybersecurity Service Provider, and correct Service-specific incident reporting chain), and the means by which the OTAs can obtain cyber 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 SUT. Identify all key performance parameters and operational requirements (such as Cyber Survivability Endorsement requirements) that require verification or 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.

[6] MITRE ATT&CK, https://attack.mitre.org/

4.2.1 Threat Assessments

Starting at program inception, acquisition programs request from the Intelligence Community and use finished intelligence and counterintelligence threat products to guide risk-based program management, system engineering, operational trade-off, and systems authorization decisions, and scope test planning. These threat products contextualize the threat to the system in contested cyberspace and guide engineering efforts to design the system to operate in the expected threat environment. Intelligence assessments and reporting should be updated regularly as adversary capabilities evolve over time. While cyber OT&E teams should use baseline intelligence products and artifacts to begin test planning, they require updated intelligence products related to the expected threat within the expected operational environment when conducting operational testing. The focal point for requesting updated intelligence is the CyWG. In addition, the MITRE ATT&CK Knowledge Base is an industry standard used as a resource for understanding observed adversary TTP in contested cyberspace.

4.2.2 Mission-Based Cyber Risk Assessments (MBCRAs)

Programs should confirm that systems can perform critical functions to complete supported missions within required timeframes when faced with representative threats. MBCRA is an analytical, iterative process that identifies, estimates, assesses, and prioritizes the risks of cyber effects to DoD operational missions. MBCRAs provide a means to understand the SUT, identify the system's critical functions and supporting critical data, understand potential attack paths and risks, identify required test resources, and generate the cyberspace attack scenarios needed to support DoDI 5000.89, DoDI 5000.98, DoDM 5000.99, and forthcoming cyber DT DoDM directed scenario-based testing. The program management office may utilize the systems security working group or CyWG to plan, conduct, or update MBCRAs throughout the acquisition life cycle and includes representatives of the user community, the system designers, and cyber technicians with familiarity in using threat representative attacks, at a minimum.

In preparation for Cyber OT&E, programs should conduct an MBCRA or update the latest version of existing MBCRA products to reflect changes in system design, operating environment, threats, and cyber test results, as well as ensure their scope includes all areas that will be tested during OT&E. As there are multiple MBCRA methodologies, programs may choose the MBCRA methodology that meets the program's specific needs as long as the MBCRA methodology adheres to the DoD MBCRA guidance and considerations in the forthcoming cyber DT DoDM and cyber DT guidebook.

4.3 Test Documentation

The strategy for cyber T&E should be documented in the TEMP. Additionally, cyber content should be included in operational test plans to enable adequate testing.

4.3.1 TEMP/T&E Strategy

DoDM 5000.100 "Test and Evaluation Master Plans and Test and Evaluation Strategies" and the DOT&E TEMP Guidebook provide policy and guidance for cyber content in the TEMP.[7] The TEMP/T&E Strategy should use relevant data from all available sources and include 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-systems tests. The program office and OTAs should integrate cyber testing into the overall evaluation planning and schedules. The TEMP/T&E Strategy should identify resources required to execute CVPAs and AAs and include funding, organizations, test assets, and threat documentation. The TEMP/T&E Strategy 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/T&E Strategy 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 contested cyberspace. The TEMP/T&E Strategy 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.

4.3.2 Operational Test Plan

Appendix B of this guidebook provides cyber requirements for the content of an OT&E test plan. OT&E test plans should contain details of how the OTAs will test to provide the required cyber data, including resources, schedule, OTA-specific test and data collection tools, and data to be collected. The OTAs 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, consider the supply chain, 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 cyber testing at the end of the test. Test plans should be coordinated and approved in accordance with organizational standard operating procedures.

4.3.3 Test Data

OTAs should authenticate/validate data as needed and provide data from Appendix C and Appendix D 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 OTAs 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.

[7] DOT&E TEMP Guidebook 3.1, January 2017.

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.

4.4 Execute

4.4.1 CVPAs

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

If possible, the OTAs may 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. When possible, the CVPA should not be cojoined with the AA, to allow sufficient time separation between the CVPA and AA for the program manager to consider and implement system remediations. During the CVPA, OTAs should examine relevant insider, nearsider, and outsider threat postures. Program office representatives, including developer support, are encouraged to participate in the CVPA to observe and characterize vulnerabilities, potential exploits, and follow-on fixes. CVPAs should also include operational users and cyber defenders. The CVPA requires a system that is operationally and production representative, or the system that is available at the time of OT, depending on the acquisition pathway. Any specific differences must be defined and approved by DOT&E before CVPA execution. Appendix C of this guidebook lists the minimum data required from a CVPA. If conducted on a live/operational network, cyber teams must conform to the guidance within DoDI 8585.01.

CVPA data and tests include system and network scans, vulnerability validation, penetration tests, mission effects if any occur from penetration testing, defender detections of these activities and information regarding what actions would be queued (but not executed in the CVPA in order to continue penetration testing), access control checks, physical inspection, personnel interviews, consider the supply chain, and reviews of the system-of-systems and the system architecture and components to characterize the cyber defensive status of a system as deployed and operated in the operational environment, including any third party or external defenders.[8] The OTAs should identify relevant cyber hygiene metrics (including RMF controls) as applicable. Data from RMF activities and reports should be incorporated and utilized whenever possible to minimize duplication of effort. Following the CVPA, the program office and OTA should review implications for potential mission effects for inclusion in test reporting. The CVPA data should document the system configuration as observed, all test events executed (including both failed and successful events), observations, findings, detections, and results. CVPA results should be provided to DOT&E, the Services, relevant authorizing officials,

[8] 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).

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 OTA should review mitigations to the SUT that were implemented to correct CVPA findings and inform DOT&E on how – if at all – the SUT configuration has been altered.

The CVPA can be a standalone 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) DT events. DOT&E will approve the selected approach as part of the test strategy in the TEMP and the operational test plan.

4.4.2 AAs

During the AA, the adversarial team (threat stimulus) should focus attacks on disrupting the critical missions to create both safety critical and cyber effects so that the OTAs can collect data on resulting mission performance. If an opposing force commander is part of the test structure, the OTAs should synchronize the AA activities with that commander. During the AA, OTAs should examine relevant insider, nearsider, and outsider threat postures, to include the effects of a compromised insider or enterprise host network. In 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 VV&A of these closed environments, cyber ranges, or other validated and operationally representative tools according to Service VV&A standards. Appendix D of this guidebook lists the minimum data required from the AA.

The OTAs should conduct the AA on a production-representative and operationally configured system, or the system available during operational testing based on the acquisition pathway. They should identify any test or system deviations for review and approval by DOT&E before the test. The use of cyber teams to attack the system must conform to DoDI 8585.01, and attacks should be carried out according to the rules of engagement and scope defined in planning (which may be to their conclusion or the limitations of the cyber team's capabilities). Where possible, the OTAs 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 procedures on CEVAs provided in Appendix E of this guidebook.

Where limitations due to operations or safety arise, or in the interest of time, the OTAs may provide system access to the AA team via "white card" insertion to enable required test activities and data collection in the time available.[9] 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.

[9] 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.

The term "adversarial" describes only the focus of the assessment – how an adversary could exploit the system. The OTA, program office, user SMEs, and supporting agencies should work together in the design of the AA, use of trusted agents, and system 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 OTAs should arrange the participation of any third party or external defenders, including those responsible for defending networks connecting to the SUT, and identify the extent of defender involvement, data collection requirements, and passive or active measures that the defenders should take. In most cases where a system is hosted on a DoD enterprise network, network defenders such as a cybersecurity service provider should already be providing day-to-day monitoring and response, and so no special measures beyond coordinating data collection should be necessary. 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 OT should match the operational deployment and CONOPS for the system. Data collection should support evaluation of cyber responses, operational mission effects from cyber aggression as well as from defensive responses, and operational continuity plans. The OTAs should confirm that resilience and continuity plans include protecting backups and failovers against compromise to enable restoration to a secure state as applicable.

Appendix A Pre OT Considerations

The OTAs should consider the following cyber-unique factors when planning for/prior to commencing OT&E.

Planning

- Is there a DOT&E-approved test plan?
- Has the OTA/OTO incorporated cyber 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 ATO (if required)?
- 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 OTA/OTO reviewed 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 testing/assessment of supply chain?
- Does the test plan include testing/assessment of artificial intelligence of machine learning as applicable?
- 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?
- Has the OTA/OTO identified the cyber rules of engagement and reached agreement with appropriate organizations?

DT&E Results

- Has DOT&E reviewed integrated test plans for test data relevant for operational evaluation?
- Has DOT&E reviewed any unresolved cyber DT&E findings or cyber deficiencies?
- If the program conducted an MBCRA, has it provided the results to DOT&E, the OTA, and teams supporting both the CVPA and AA?

Resources

- Will operational cyber defenders be in place and participating?
- Are all other resources required for cyber 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?

Appendix B Cyber Content of Operational Test Plans

The following table lists the minimum content for operational test plans.

Item	Description
TEMP Linkage	Review the test plan to ensure consistency with the approved TEMP, and document differences that may require review and/or approval.
Architecture	Test Plan should describe the architecture of the system (or system-of-systems) to include: • Major subsystems within the scope of test or their interfaces to other components or systems • Interconnections between major subsystems (e.g., Ethernet links, data bus links), external connections (e.g., NIPRNet, SIPRNet), and physical access points (e.g., USB ports, drives, peripherals, and other media) • System and test boundaries
Operational Environment	Identify the cyber-attack surface for the SUT(s). Also, specify and describe the operational (cyber) environment of the system described? Descriptions should include: • Locations, cyber roles, for end users, system/network administrators, and maintenance teams • Specific mission threads and tasks addressed in the test plan. • The location and anticipated roles of all cyber defenders (local and non-local), and cybersecurity services supporting system operation • The threats, techniques, and objectives that the Red Team will portray during the test and the cyber threat actions to be portrayed • Potential safety risks during testing
Time and Resources	A schedule of test events and required resources should include: • The dates and location for both phases of the cyber testing • Specific operational users • The cyber defense agencies/personnel • The cyber teams arranged to perform test functions • Other test resources such as cyber ranges or specific tools • Any authorizations required to conduct the test
CVPA	Describe the planned CVPA execution: • The cyber team should review the system architecture, CONOPS, configuration, policies, and prior known vulnerabilities as part of the CVPA preparation. • Describe how the data and metrics will be documented in accordance with Appendix C of this guidebook. – Cyber vulnerabilities – Attack vectors planned to include starting points, criterion for success, tools planned, time and location data • Specify data collection methods, which may include: – Automated scanning/exploitation tools – Physical inspection – Personnel interviews – Document reviews • Describe anticipated deviations from the operational configuration and potential implications for test adequacy. • Describe anticipated CVPA limitations and how they could affect the test.

Item	Description
AA	Describe the planned AA execution: • Describe the validated threat that will be portrayed for the test to include intended attack vectors and intended mission effects/objectives. • Describe any limitations or variations anticipated and how they will affect the test, including white cards or cyber range use. • Describe any periods of enumeration or "free play" that will occur. • Describe how the test will incorporate the CVPA results. • Identify anticipated operational cyber defenders for the system(s) and how data will be gathered from those activities/organizations, including: – Local users and administrators – Command-level administrators and defenders – Cybersecurity service organizations • Provide data collection plans in accordance with Appendix D of this guidebook. • Identify any mission effects determined by either direct measurement or by independent assessment using SMEs. • Identify any automated tools for the test.

Appendix C 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, personnel, and complete set of limitations and constraints.	
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 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 solutions. • 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.
Defender Detections	• For all scanning and penetration testing, determine which actions defenders saw and what actions would normally be queued in response.	• Do not execute defensive responses in this phase of testing so as not to interfere with the extent of the exposure characterization.
Mission Effects	• Collect all data from any incidental mission effects that come about during scanning, penetration testing, or even just operating in an operationally representative manner.	• As this is an OT&E event, collection of mission effects data by exception is always desirable.

Appendix D 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, personnel, and all limitations and constraints.	
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, timeline, privilege level, tool used, target and source system.	• Coordinate the reporting format of the data with 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.). • Reaction (e.g., incident report, block access, remove system). • Restoration (operational, cyber, continuity of operations). • 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	• The OTA should collect data on response and restoral actions. • Multiple organizations might have individual response actions to a particular event and the OTAs should collect all measures for each. • One organization might have multiple reactions to a particular event (e.g., incident report to higher- tier organization, followed by an Internet Protocol block at the direction of the higher-tier organization). • *Operational restore* refers to the recovery of affected system functions. • *Continuity of operations* is the implementation of an alternate capability using a different system or

AA Data Requirements		
Evaluation Area	**Information**	**Notes**
	compromises of primary systems, and responses of both systems. • White cards used, if any.	process. • *Cyber restore* refers to the complete removal of the adversary from the affected system.
Mission Effects	• Report demonstrated and 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 SMEs, 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. • It is recommended to collect other mission performance observations even if not caused by cyber aggression or defense.

Appendix E CEVAs

For financial or business systems, cyber threats present a risk of economic exploitation of information systems whose functions include financial management, payments, allotments, and fiscal transfers. A CEVA is an operational assessment that evaluates the economic losses and mission effects resulting from cyber exploits that include identity theft, wage theft, counterfeiting, forgery, terrorist financing, embezzlement, money laundering, corruption, bribery, and other fraudulent activities.

A CEVA consists of three stages, shown in Figure E-1 and described in Table E-1:

- Economic-based cyber tabletop
- CVPA (Section 4.4.1)
- AA (Section 4.4.2)

A CEVA working group will design and execute the three stages and should include all CyWG personnel and all additional roles related to financial systems including:

- Technical penetration testers that have requisite experience in exploitation of associated operating systems, applications, databases, web applications, and other components related to financial systems to provide attack vectors into the system.
- Intelligence analysts to provide threat intelligence from cyber intrusions into commercial industries (e.g., reports from Mandiant, Verizon, and Kaspersky), similar or related systems, and which economic information is exploitable to achieve cyber economic effects.
- System administrators, users, and maintainers to provide insight on roles, responsibilities, and procedures related to business operations, enterprise-wide system management, accounting, and finance.
- Auditors with functional knowledge of government business processes capable of analyzing large amounts of economic and financial data, threat intelligence data, and cyber-attack trends data to identify targets of economic exploitation and associated economic effects.

A CEVA should include the tabletop exercise in order to inform economic and financial considerations for both the CVPA and then the AA. A CEVA should not require an independent testing event separate from the existing CVPA and AA. However, CEVA results following the three aforementioned phases can inform an external audit.

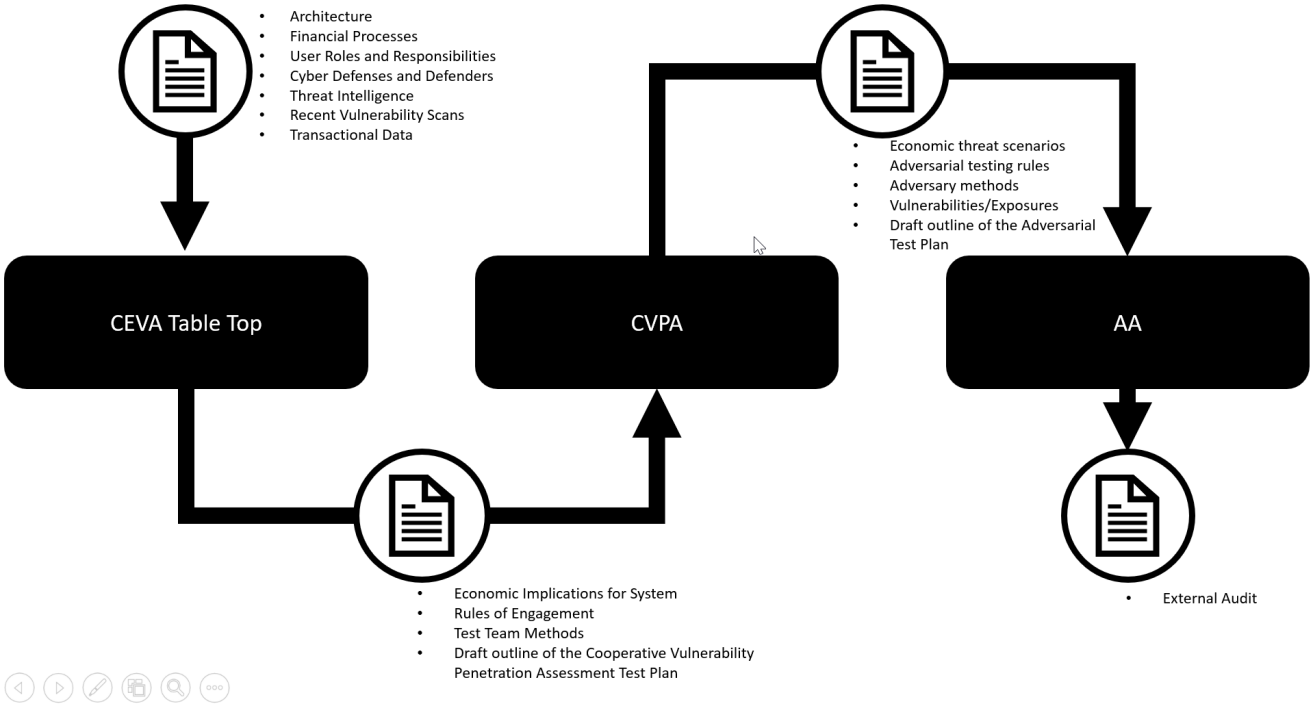

Figure E-1. Inputs and Outputs of the CEVA Process

Table E-1. Stages, Inputs, and Expectations of a CEVA

Stage	Prior	During	After
Economic-Based Cyber Tabletop	The CEVA team should use a MBCRA (Section 4.2.2) or similar approach to develop economic-based cyber threat scenarios. Inputs include: • Documentation for the architecture including subsystems, interfaces, interconnections, external connections, physical access points, and configurations. • Detailed processes for account management and financial services. • User roles and responsibilities related to accounting, financial, business operations, and enterprise-wide system management. • Cyber defenses and cyber defenders. • Threat intelligence, threat actors, and threat actor goals. • Results of recent system scans and vulnerability assessments. • Representative set of past and current transaction data.	The CEVA team will walk through the cyber threat scenarios and wargame defender actions taken in response to threat actions.	The CEVA team should select: • Threat scenarios to use in adversarial testing that will generate mission effects. • Adversarial testing rules, scope, and requirements (e.g., certifications or ATOs). • Methods and stages for technical penetration tests and economic outcomes for adversarial testing. • Required adversarial testing data and methods to collect that data. • Draft outline of the adversarial test plan.
Cooperative Testing	In addition to the CVPA (Section 4.4.1) requirements, the CEVA portion of the test should include: • The set of cyber economic-specific considerations defined in economic-based cyber tabletop. • Access to non-production environments (e.g., pre-production or laboratory instances) to cause effects if the test plan includes limitations to the production environment.	The CEVA team will ensure all economic and financial considerations are included in the CVPA test planning, to be in accordance with the CEVA tabletop exercise.	In addition to CVPA (Section 4.4.1) requirements, the test report should include transactional data and results regarding system cyber economic effects.
Adversarial Testing	In addition to AA (Section 4.4.2) requirements, the CEVA should include: • The set of cyber economic attack scenarios defined in economic-based cyber tabletop.	The CEVA team will execute the adversarial test plan scenarios against the system in a realistic operational environment to create mission effects.	In addition to AA (Section 4.4.2) requirements, the test report should include transactional data and results regarding system cyber economic effects.

Stage	Prior	During	After
	• Access to non-production environments (e.g., pre-production or laboratory instances) to cause effects if the test plan includes limitations to the production environment.		

Appendix F Glossary

Unless otherwise noted, these terms and their definitions are for the purpose of this guidebook.

F.1 ACRONYMS

ACRONYM	MEANING
AA	Adversarial Assessment
AAF	Adaptive Acquisition Framework
ATO	Authority to Operate
CEVA	Cyber Economic Vulnerability Assessment
CONOPS	Concept of Operations
CVPA	Cooperative Vulnerability Assessment
CyWG	Cyber Working Group
DoD	Department of Defense
DoDI	DoD Instruction
DoDM	DoD Manual
DOT&E	Director, Operational Test and Evaluation
DT	Developmental Test
DT&E	Developmental Test and Evaluation
LFT&E	Live Fire Test and Evaluation
MBCRA	Mission-Based Cyber Risk Assessment
OT	Operational Test
OT&E	Operational Test and Evaluation
OTA	Operational Test Agency
OTO	Operational Test Organization
RFP	Request for Proposal
RMF	Risk Management Framework
SME	Subject Matter Expert

ACRONYM	MEANING
SUT	System Under Test
T&E	Test and Evaluation
TTP	Tactics, Techniques, and Procedures
VV&A	Verification, Validation, and Accreditation

F.2 DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

accreditation	The official certification that modeling and simulation results are acceptable for their intended use. *Defined in DoDI 5000.98.*
acquisition decision	A key acquisition decision outlined in each of the AAF pathway policy documents including interim acquisition decisions, outcome determination decisions, production decisions, and fielding decisions, also referred to as deployment decisions. *Defined in DoDI 5000.98.*
adversarial test	Identifies new vulnerabilities or exploits predicted vulnerabilities during the mission execution in the presence of opposing forces and capabilities emulating the adversary. Evaluates the performance of self-defense systems, trained operators including defenders, and the ability of the unit equipped with the system to identify and respond to the adversary. *Defined in DoDM 5000.99.*
contested environment	Caused by enemy activities that detect, disrupt, exploit, degrade, deny, deceive, or destroy friendly capabilities for the purpose of military advantage in uncertain and hostile environments. *Defined in DoDI 5000.98.*
continuity of operations	Implementation of an alternate capability using a different system or process.
cooperative test	Identifies new or exploits predicted vulnerabilities and their effect on operational effectiveness, suitability, survivability, and lethality (if applicable) in an overt manner using live

	kinetic or non-kinetic threats. Conducted at the sub-component, component, sub-system, system level using prototypes or early system configurations, and full-up system level. Takes into consideration susceptibility to attack, the performance of self-defense systems, and evaluates the performance of defenders and recoverability teams or capabilities. Evaluates user casualties, as applicable. *Defined in DoDM 5000.99.*
cyber restore	The complete removal of the adversary from the affected system.
cyber survivability	The ability of warfighter systems to prevent, mitigate, recover from and adapt to adverse cyber-events that could impact mission related functions, by applying a risk managed approach to achieve and maintain an operationally relevant risk posture, throughout its life cycle. *Defined in JCIDS Manual (October 2021)*.
cyberspace	A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. *Defined in DoDM 5000.99.*
cyberspace attack	Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain and is considered a form of fires. *Defined in DoDM 5000.99.*
cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. *Defined in DoDM 5000.99.*
cybersecurity service provider	An organization that provides one or more cybersecurity services to implement and protect the DoD information network. *Defined in DoDM 5000.99.*

defender	The operator, maintainer, or person responsible for the cyber defense of the SUT. In the absence of a mission defense team, the operator is the first line of defense to the SUT in its operational use. There may be multiple lines of defense.
integrated test and evaluation	T&E event that enables the program manager, the OTAs and LFT&E organizations to use contractor test and DT events to generate data required to meet OT&E or LFT&E objectives, while preserving the primary contractor test or DT objective of the test. *Defined in DoDI 5000.98.*
iterative test	A repeated and/or routine assessment of a system that is initiated by some set of criteria (these may include system maturation, system capability additions, system vulnerability mitigations, software updates, changes in how a system is employed, or changes in TTP). The cadence of the iterations is dependent on the AAF pathway and is most applicable to the software acquisition pathway. Iterative testing can range from smaller, DT-level tests that investigate the differences in the system only, to complete operational/OT events. The scale at which that testing takes place is determined by the criteria that triggered the need for the test, and the subsequent risk those criteria pose for the program/system.
LFT&E	Includes realistic full spectrum survivability testing of the DoD system configured for combat by firing kinetic and non-kinetic threats likely to be encountered in combat at it, or their accredited surrogates. Also includes realistic full spectrum lethality testing of DoD offensive capabilities configured for combat by firing it against kinetic and non-kinetic targets likely to be encountered in combat or their accredited surrogates. A DoD system configured for combat must include all hardware, materials, and software that may influence the measured performance. *Defined in DoDI 5000.98.*
multi-domain operations	The employment of the joint capabilities of all combat power from each domain to accomplish missions at cost. The five domains are air, sea, land, cyber, and space. *Defined in DoDI 5000.98.*
operational effectiveness	Degree to which the unit equipped with the system can execute and support the required missions in contested, congested, and constrained operational environments, while taking into equal

	consideration survivability and lethality effects (as applicable). *Defined in DoDI 5000.98.*
operational restore	The recovery of affected system functions.
operational suitability	Degree to which a system can be placed and sustained satisfactorily in field use, including contested, congested, and constrained environments, with consideration being given to availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human system interface, habitability, manpower, logistics, natural environmental effects and impacts, documentation, and training requirements. *Defined in DoDI 5000.98.*
OT&E	Operationally realistic and relevant testing of the fielding- or production- representative system or service, their key components, as integrated with other systems or services, under realistic combat conditions, using typical military users; and the evaluation of the results of such test. *Defined in DoDI 5000.98.*
penetration testing	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a DoD system. *Defined in DoDM 5000.99.*
program manager	Plans acquisition programs, prepares programs for key decisions, and executes approved acquisition and product support strategies. Continually reviews and evaluates program progress. Works closely and substantially with program prime contractors to provide leadership and ensure program objectives are achieved within stringent cost, schedule, and technical and operational performance requirements. *Defined in DoDI 5000.98.*
system under test	A complete system (or system of systems) that is the object of evaluation during the test. The complete system comprises of hardware, software the network environment, end users, administrators, cyber defenders, and cyber threats.
system-of-systems	Collection of independent systems, integrated into a larger system that delivers unique capabilities. The independent constituent systems collaborate to produce global behavior that they cannot produce alone. *Defined in DoDI 5000.98.*

supply chain	A linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer. *Defined in DoDM 5000.99.*
supply chain risk	The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system. *Defined in DoDM 5000.99.*
Systems Security Working Group	A cross-functional team that applies scientific, mathematical, engineering, and measurement principles, concepts, and methods to coordinate, orchestrate, and direct the activities of various security engineering specialties and other contributing engineering specialties to provide a fully integrated, system-level perspective of system security. *Defined in forthcoming Cyber DT DoDM.*
T&E	Includes Cyber Test & Evaluation, Developmental Test & Evaluation, integrated Test & Evaluation, Operational Test & Evaluation, Live Fire Test & Evaluation, and relevant Modeling & Simulation. *Defined in DoDI 5000.98.*
T&E Oversight List	List of DoD systems acquired via the Defense Acquisition System that are being overseen by DOT&E for OT&E and LFT&E and by the Under Secretary of Defense for Research and Engineering for DT&E. The T&E Oversight List is unclassified and is published at https://www.dote.osd.mil/Oversight/. *Defined in DoDI 5000.98.*
TTP	Patterns of behavior used to create a standard way of operating. TTP can also be adversarial patterns used to gain actionable intelligence against an enemy style of attacking. *Defined in DoDM 5000.99.*
validation	The process of determining the degree to which a model or simulation and its associated data are an accurate representation of the real world from the perspective of the intended uses of the model. *Defined in DoDI 5000.98.*

verification	The process of determining that a model or simulation and its associated data accurately represent the developer's conceptual description and specifications. *Defined in DoDI 5000.98.*
vulnerability	A weakness in a system design or tactics, techniques, and procedures that that an actor or event could exploit or trigger to cause user injuries, degrade or diminish operational effectiveness and suitability, including security incidents and catastrophic effects. Examples include but are not limited to poorly designed system security procedures, internal controls, lack of mission critical component or system redundancies, component exposure and lack of physical or logical separation, lack of passive and active damage and malfunction suppression through hardening (e.g., shock hardening, coating, cybersecurity hardening such as host-based security system, antivirus), lack of component and system capability recovery, lack of component shielding. *Defined in DoDI 5000.98.*
white card	Simulated event in a test. White cards are used when pursuing an exploitation or penetration of DoD system(s) where live testing is expensive and impractical. *Defined in DoDM 5000.99.*

Appendix G References

- Cyber Survivability Endorsement Implementation Guide (CSE IG), version 3.0, July 2022, Joint Staff J6.
- Defense Intelligence All-Source Analytic Enterprise. https://intellipedia.intelink.gov/wiki/Acquisition_Intelligence_Support_Working_Group
- DoDI 5000.02, The Operation of the of the Adaptive Acquisition Framework, January 2020
- DoDI 5000.82, Requirements for the Acquisition of Digital Capabilities, June 2023.
- DoDI 5000.86, Acquisition Intelligence, September 2020.
- DoDI 5000.89, Test and Evaluation, November 2020.
- DoDI 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Manager, December 2020.
- DoDI 5000.98, Operational Test and Evaluation and Live Fire Test and Evaluation, December 2024.
- DoDI 8585.01, DoD Cyber Red Teams, January 2024.
- DoDM 5000.96, Operational and Live Fire Test and Evaluation of Software, December 2024.
- DoDM 5000.99, Realistic Full Spectrum Survivability and Lethality Testing, December 2024.
- DoDM 5000.100, Test and Evaluation Master Plans and Test and Evaluation Strategies, December 2024.
- DoDM 5000.102, Modeling and Simulation Verification, Validation, and Accreditation for Operational Test and Evaluation and Live Fire Test and Evaluation, December 2024.
- DoDM 5000,[TBD], Cyber Developmental Test and Evaluation, [forthcoming]
- DoD Cybersecurity Test and Evaluation Guidebook, version 2.0, Change 1, February 2020.
- DoD Test and Evaluation Enterprise Guidebook, August 2022.
- DOT&E TEMP Guidebook 3.1, , January 2017.
- Joint Publication 3-12, Joint Cyberspace Operations, December 2022.
- Manual for the Joint Capabilities Integration and Development System, October 2021.
- MITRE ATT&CK.
- Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, National Institute of Standards and Technology Special Publication 800-37, Rev. 2, December 2018, National Institute of Standards and Technology.