Department of Defense

Cybersecurity Test and Evaluation Guidebook

1 July 2015

Version 1.0

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Purpose

Department of Defense (DoD) systems increasingly depend upon complex, interconnected information technology (IT) environments. These environments are inherently vulnerable, providing opportunities for adversaries to compromise systems and negatively impact DoD missions. Potential cyber vulnerabilities, when combined with a determined and capable threat, pose a significant security problem for the DoD and its warfighters. Cybersecurity test and evaluation (T&E) assists in the development and fielding of more secure, resilient systems to address this problem.

The purpose of this guidebook is to provide guidance to Chief Developmental Testers, Lead Developmental Test and Evaluation (DT&E) Organizations, Operational Test Agencies (OTAs) and the larger test community on planning, analysis, and implementation of cybersecurity T&E. Cybersecurity T&E consists of iterative processes, starting at the initiation of an acquisition and continuing throughout the entire life cycle.

1.2 Organization of This Guidebook

This guidebook has three main sections, including this introductory section. Section 2 provides the information that is essential to T&E personnel for supporting the Risk Management Framework (RMF). Section 3 lays out the implementation of cybersecurity T&E across the acquisition life cycle.

The appendices provide additional guidance and information on specific topics of interest as follows:

- Appendix A: Guidance for analysis of RMF documents and artifacts to support T&E
- Appendix B: Guidance on the cybersecurity elements of the Developmental Evaluation Framework (DEF)
- Appendix C: Minimum measures to guide cybersecurity operational evaluations
- Appendix D: Guidance for the review and use of Program Protection Plans (PPPs) from a T&E perspective
- Appendix E: Descriptions of cybersecurity T&E test team resources
- Appendix F: Descriptions and contact information for cyber ranges
- Appendix G: Examples of common vulnerabilities related to cybersecurity
- Appendix H: A description of primary stakeholders for cybersecurity T&E
- Appendix I: A glossary of terms and list of acronyms
- Appendix J: References on cybersecurity

1.3 Audience

The intended audience for this guidebook includes Chief Developmental Testers, Lead DT&E Organizations, OTAs, and the test teams for DoD acquisition programs.

2 Cybersecurity – Risk Management Framework

This section provides an overview of the RMF process for the Chief Developmental Tester, Lead DT&E Organization, and the T&E community. RMF activities and artifacts provide significant information to the T&E community. Understanding the RMF process is vital for the T&E community as they plan, test, and evaluate cybersecurity as part of the acquisition program.

2.1 Cybersecurity Procedures Overview, DoDI 8500.01

DoD Instruction (DoDI) 8500.01, *Cybersecurity*, defines the policy and procedures for cybersecurity. Cybersecurity is defined as the prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure their availability, integrity, authentication, confidentiality, and nonrepudiation.

For the Chief Developmental Tester, Lead DT&E Organization, and the T&E community, the key elements of the policy are that it:

- Extends applicability to all DoD IT, including Platform IT (PIT)[1]
- Emphasizes operational resilience, integration, and interoperability
- Adopts common Federal cybersecurity terminology, consistent with the Intelligence Community (IC) and the National Institute of Standards and Technology (NIST)
- Incorporates cybersecurity early and continuously within the acquisition life cycle
- Transitions to the National Institute of Standards and Technology (NIST) Special Publication 800-53 Security Control Catalog for use in the DoD[2]

[1] Platform IT is defined as information technology, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. Examples of platforms that may include PIT are: weapons systems, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical devices and health information technologies, vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.), utility distribution, telecommunications systems designed specifically for industrial control systems including supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering, including associated data transport mechanisms (e.g., data links, dedicated networks).

[2] NIST Special Publication 800-53 may be found at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

The cybersecurity policy defines the following activities for the Chief Developmental Tester, Lead DT&E Organization and the T&E community:

- Integrating cybersecurity assessments into DT&E, including planning for and ensuring that vulnerability assessments, vulnerability evaluations and intrusion assessment, cybersecurity inspections, and adversarial test operations (using internal or external capabilities) are performed to provide a systemic view of enclave[3] and information system cybersecurity posture
- Incorporating cybersecurity planning, implementation, testing, and evaluation in the DoD acquisition process and reflecting these in the program Test and Evaluation Master Plan (TEMP)
- Ensuring that cybersecurity T&E is conducted throughout the acquisition life cycle, integrated with interoperability and other functional testing, and that a cybersecurity representative participates in planning, execution, and reporting of integrated T&E activities
- Coordinating with DoD Test Resource Management Center (TRMC) for establishment of required T&E-specific cybersecurity test architectures, infrastructure, and tools
- Planning, resourcing, and performing cybersecurity assessments as part of T&E assessments

The policy and additional implementation information is provided in the RMF Knowledge Service (KS) at https://rmfks.osd.mil.

The RMF Knowledge Service was established as the online, Web-based resource that:

- Is the authoritative source for RMF implementation guidance and assessment procedures
- Provides requirements, guidance, and tools for implementing and executing the RMF
- Is available to individuals with IT risk management responsibilities
- Provides convenient access to security controls baselines, overlays, individual security controls, and security control implementation and assessment procedures
- Supports both automated and non-automated implementation of the RMF.

The RMF KS website (https://rmfks.osd.mil) is accessible by individuals with a DoD Public Key Infrastructure (PKI) certificate (common access card [CAC]), or External Certification Authority certificate in conjunction with DoD sponsorship (e.g., for DoD contractors without a CAC and who work off-site).
The RMF KS hosts a library of tools, diagrams, process maps, documents, etc., to support and aid in the execution of the RMF. It is also a collaboration workspace for the RMF user community to develop, share, and post lessons learned, best practices, cybersecurity news and events, and other cybersecurity-related information resources.

[3] An enclave, as defined by DoDI 8500.01, is a set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

2.2 Risk Management Framework

One component of organizational risk that is addressed to ensure the success of the DoD mission is risk related to the operation and use of IT. Management of that risk includes the implementation of a carefully coordinated set of activities to ensure that fundamental requirements for information security[4] are addressed. The Risk Management Framework (RMF), defined in NIST Special Publication 800-37,[5] provides a structured, flexible approach for managing risk related to IT. DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, mandates the use of the RMF within the DoD.

2.2.1 RMF Procedures Overview, DoDI 8510.01

DoDI 8510.01defines policy and procedures that:

- Adopt NIST's RMF
- Direct the use of the Committee on National Security Systems Instruction (CNSSI) 1253[6] for security control categorization and selection and the use of overlays
- Clearly define what IT should undergo the full RMF life cycle
- Promote DT&E and operational test and evaluation (OT&E) integration
- Codify reciprocity
- Strengthen enterprise-wide IT governance
- Emphasize continuous monitoring

For the T&E community, DoDI 8510.01 requires that RMF activities be integrated with developmental and operational test activities. This includes defining specific concepts and rules for testing related to reciprocity (i.e., the acceptance by all parties of security terms and conditions, security controls assessment, and all documents pertaining to those decisions).

Cybersecurity reciprocity[7] (referred to in the DoDI 8510.01 as "reciprocity") is an essential element in ensuring IT capabilities are developed and fielded rapidly and efficiently across the DoD Information Enterprise. Applied appropriately, reciprocity reduces redundant testing, assessing, and documentation, and the associated costs in time and resources. The DoD RMF presumes acceptance of existing test and assessment results and authorization documentation, and DoDI 8510.01 defines specific concepts and rules to facilitate reciprocity.

[4] Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, in order to provide confidentiality, integrity, and availability.

[5] NIST Special Publication 800-37, which describes the RMF, may be accessed at http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

[6] CNSSI 1253, which describes the process of categorization, may be accessed at http://www.sandia.gov/FSO/PDF/flowdown/Final_CNSSI_1253.pdf

[7] Reciprocity may be defined in this context as the mutual recognition of analysis and testing by consenting organizations. Reciprocity is described in detail in DoDI 8510.01, Enclosure 5.

The RMF defines several key positions that are summarized in Table 1. For a full description of RMF roles and responsibilities, see NIST Special Publication (SP) 800-37.

Table 1. RMF Roles and Responsibilities

RMF Role	Responsibilities
Authorizing Official (AO)	Ensures that all appropriate RMF tasks are initiated and completed, with appropriate documentation, for assigned information systems and PIT systems; signs the Security Plan, reviews and approves the security assessment report; monitors and tracks overall execution of system-level RMF Plans of Action and Milestones (POA&Ms); promotes reciprocity; and renders authorization decisions.
Security Control Assessor (SCA)	Has the authority and responsibility for conducting a security control assessment; prepares the security assessment report; supports development of the continuous monitoring strategy, and continuously assesses and guides the quality and completeness of RMF activities and tasks and the resulting artifacts.
Program Manager / Information System Owner (ISO)	Categorizes systems and then documents the categorization in the appropriate Joint Capabilities Integration and Development System (JCIDS) document (e.g., capabilities development document); and develops, maintains, and tracks the security plan.
Information System Security Manager (ISSM)	Maintains and reports IS and PIT systems assessment and authorization status and issues, provides direction to the Information System Security Officer, and coordinates with the organization's security manager to ensure that issues affecting the organization's overall security are addressed.
Information System Security Officer (ISSO)	Maintains the appropriate operational security posture for an information system or program.

The RMF consists of six steps that fully integrate information security into the DoD enterprise architecture and system development life cycle. The steps provide a common set of security controls that promote reciprocity and reuse of test results and assessment documentation as a norm, thus saving time and resources while enhancing interoperability.

A high-level description of each RMF step is provided below and is shown in Figure 1. Additional information is available on the RMF KS at https://rmfks.osd.mil.

RMF Step 1, Categorize: The Program Manager, with support from the AO, categorizes systems in accordance with CNSSI 1253. Categorization is performed using three security objectives (confidentiality, integrity, and availability) with one impact value (low, moderate, or high) assigned for each of the security objectives. The Chief Developmental Tester will ensure that system categorization is reflected in the TEMP, typically before Milestone (MS) B.

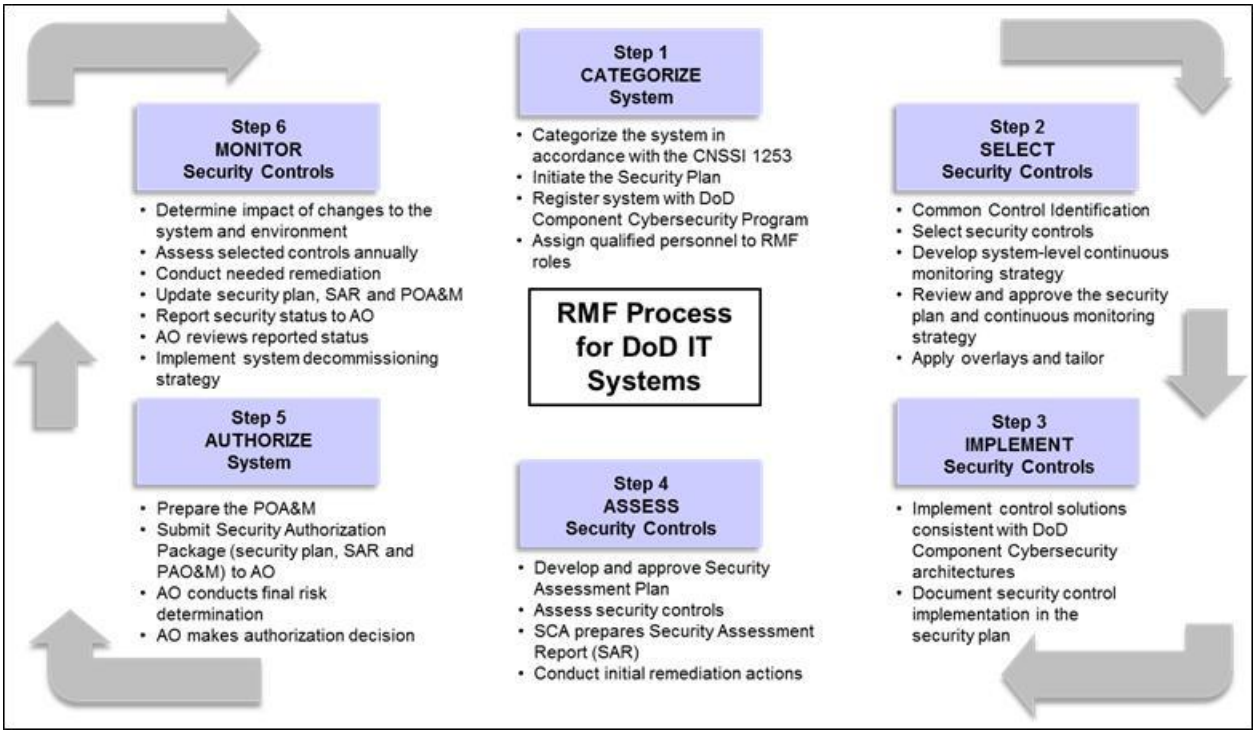


Figure 1. Summary of RMF Steps

RMF Step 2, Select Security Controls: The AO, in coordination with the PM, the Chief Developmental Tester, the Chief Information Officer (CIO), and systems security engineering, will assist in defining, tailoring, and supplementing the control baseline. To ensure that the controls are included in applicable contracts, the controls are typically included in technical requirements documents or similar system engineering artifacts. Test planning should include consideration of security controls. The RMF KS[8] provides tools for selecting controls, such as the Controls Explorer, shown in Figure 2, which supports viewing controls and implementation guidance.

[8] The RMF KS may be accessed at https://rmfks.osd.mil.

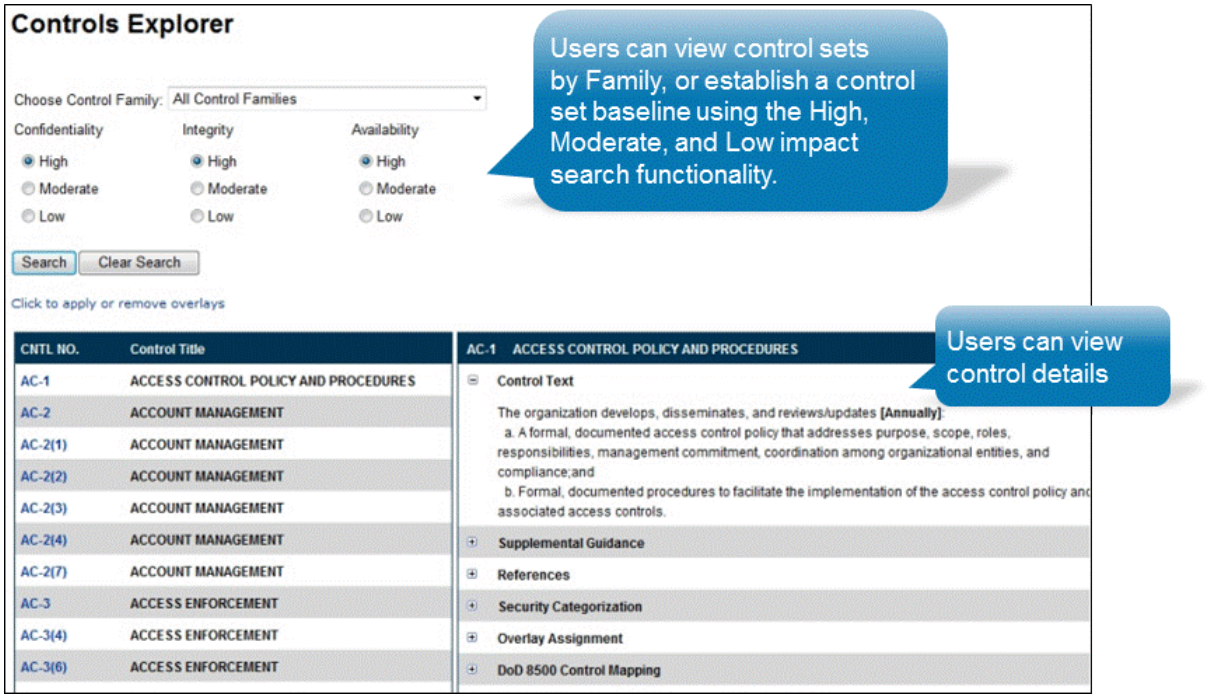


Figure 2. RMF KS Controls Explorer

RMF Step 3, Implement: The Program Manager is primarily responsible for ensuring that security controls are implemented. The Program Manager documents security control implementation in the Security Plan. The program's Systems Engineer will collaborate with the Program Manager to appropriately implement controls and the Chief Developmental Tester will ensure that appropriate test planning is performed for assessment of the controls.

RMF Step 4, Assess: The Security Controls Assessor is primarily responsible for assessing the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The Security Controls Assessor prepares a Security Assessment Plan, assesses the implementation of the security controls in the system, assigns vulnerability severity values for non-compliant controls, determines risk level for security controls, aggregates risk for the system, and prepares a Security Assessment Report. The Chief Developmental Tester should ensure security control assessment activities are coordinated with certification efforts, DT&E, and OT&E. The Chief Developmental Tester should also ensure the coordination of activities is documented in the security assessment plan and the TEMP.

RMF Step 5, Authorize: The AO authorizes information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable. The Program Manager prepares the RMF POA&M based on the findings and recommendations in the Security Assessment Report, excluding any remediation actions taken. The Program Manager assembles the Security Authorization Package and

provides it to the AO, who conducts a final risk determination and makes an authorization decision. The Chief Developmental Tester ensures that authorization is integrated into the overall test strategy and is reflected in the TEMP.

RMF Step 6, Monitor: The ISO and network system administrator monitor and assess selected security controls in the information system on an ongoing basis, including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, reporting the security state of the system to appropriate organizational officials and conducting annual assessments.

2.2.2 Key RMF Artifacts for the T&E Community

Several key artifacts (or documents) defined by or affected by the RMF are used in the acquisition process. Guidance on the use of RMF artifacts by the Chief Developmental Tester and the T&E community is provided below and is summarized in Appendix A. Artifacts include:

- **Security Plan** – The Program Manager prepares the Security Plan. It provides an overview of the security requirements for the system, system boundary description, the system identification, common controls identification, security control selections, subsystems security documentation (as required), and external services security documentation (as required). The plan can also contain, as supporting appendixes or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. The RMF Security Plan should be reviewed as part of the first phase of cybersecurity T&E to assist in understanding cybersecurity requirements. The Chief Developmental Tester should review Security Plan with the assistance of the SCA to leverage key components, such as the description of interconnected information systems and networks, the Security Architecture, and the Authorization Boundary, for use in the development the TEMP. More information on the content of the Security Plan may be found in the RMF KS, https://rmfks.osd.mil, which provides a template and instructions for the Security Plan. Additional information may be found in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, at http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf, and in NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, at http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf.
- **Security Assessment Plan** – The SCA prepares the Security Assessment Plan. It provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. It is highly recommend that the Chief Developmental Tester include the SCA within the T&E Working Integrated Product Team (WIPT). This will inform the SCA in developing the Security Assessment Plan concurrent with the development of the program TEMP, which allows coordination of information. The Security Assessment Plan should be aligned with the pre-MS B decisional TEMP delivery. The TEMP should reflect RMF activities and include a schedule of controls assessment (Part II) and resources required for controls assessment (Part IV). The Chief Developmental Tester and the SCA should coordinate TEMP and Security Assessment Plan development

to ensure that the RMF is fully integrated with the TEMP and detailed test plans. In particular, the Chief Developmental Tester should review security controls and reflect in the TEMP and detailed test plans:

- Which security controls must be complete for the Initial Authority To Test (IATT), post-Critical Design Review (CDR), and ensure that this is reflected in the TEMP
- Which security controls should be considered for inclusion in the RFP for design, development, and assessment by the contractor, e.g., controls for security banners and default password requirements
- The order in which security controls must be designed, developed, and assessed

The Chief Developmental Tester should coordinate with the Program Manager to ensure that any contractor security controls assessment is addressed in the TEMP. The RMF KS, https://rmfks.osd.mil, provides key activities and steps for the Security Assessment Plan, and Appendix A provides Security Assessment Plan review guidance for the test community.

- **Cybersecurity Strategy** (formerly Information Assurance Strategy) – The Program Manager (PM) prepares the Cybersecurity Strategy and appends it to the PPP. The Cybersecurity Strategy includes cybersecurity requirements, approach, testing, shortfalls, and authorization for the system being acquired and the associated development, logistics, and other systems storing or transmitting information about that system. The Cybersecurity Strategy also helps facilitate consensus among PM, Component CIO, and DoD CIO on pivotal issues. The Chief Developmental Tester should ensure that the Cybersecurity Strategy is referenced by and coordinated with the TEMP. The Cybersecurity Strategy provides input for the definition of requirements for vulnerability and adversarial testing. Guidance on the Cybersecurity Strategy may be found Chapter 7.5 of the Defense Acquisition Guidebook and in DoDI 5000.02, *Operation of the Defense Acquisition System*, at http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf.
- **Program Protection Plan** – The PPP is the integrating process for managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability, or supply chain exploit/insertion, and battlefield loss throughout the acquisition life cycle. Program Protection is the Department's holistic approach for delivering trusted systems throughout the acquisition process during design, development, delivery, and sustainment. The scope of information includes information that alone might not be damaging and might be unclassified, but that in combination with other information could allow an adversary to clone, counter, compromise, or defeat warfighting capability. Guidance for review and use of the PPP by the T&E community, in conjunction with the TEMP, is included in Appendix D. For further information on the format and content of the PPP, see the *Defense Acquisition Guidebook* (DAG), Chapter 13.
- **Security Assessment Report** – The SCA prepares the Security Assessment Report, which should be coordinated with the Chief Developmental Tester. The Security Assessment Report provides the results of assessing the implementation of the security controls

identified in the security plan to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the specified security requirements. The Security Assessment Report also contains a list of recommended corrective actions for any weaknesses or deficiencies identified in the security controls. The Chief Developmental Tester should review the Security Assessment Report and coordinate any concerns with the SCA, prior to the completion and final signature of the report. The report should be used as input during the development of the DT&E Assessment[9] as an additional source of data. A template and instructions for the Security Assessment Report are provided at the RMF KS, https://rmfks.osd.mil. More information on the content of the Security Assessment Report may be found in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, at http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf and in NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, at http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf.

- **RMF Plan of Action and Milestones** – The Program Manager prepares the RMF POA&M. It describes the specific measures planned: (i) to correct weaknesses or deficiencies noted in the security controls during the assessment; and (ii) to address known vulnerabilities in the information system. A template and instructions for the RMF POA&M are provided at the RMF KS, https://rmfks.osd.mil.
- **Security Authorization Package** – The Security Authorization Package consists of the SP, the Security Assessment Report, and the RMF POA&M. The SCA assembles the Security Authorization Package and provides it to the AO. The AO conducts a final risk determination and makes an authorization decision.
- **Authorization Decision** – An authorization decision applies to a specifically identified IS or PIT system and balances mission need against risk to the mission, the information being processed, the broader information environment, and other missions reliant on the shared information environment. A DoD authorization decision is expressed as an authorization to operate (ATO), an ATO with conditions, an interim authority to test (IATT), or a denial of authorization to operate (DATO). The product of the final risk determination is the authorization decision memorandum that documents the AOs decision along with the authorization termination date and any terms or conditions the AO attaches to the decision.

[9] For programs on OSD oversight, DASD(DT&E) prepares a DT&E assessment that includes cybersecurity for the Milestone Decision Authority to review and use during MS C decision. For programs not on OSD oversight, follow the Component policy. The DT&E assessment is an in-depth analysis beginning at MS B that assesses the results of DT&E and the progress against KPPs, key system attributes, and critical technical parameters in the TEMP. For details on the DT&E assessment, refer to the DAG, Chapter 9.

3 Cybersecurity Test and Evaluation

3.1 Introduction

Information Technology is included in virtually all new combat and support systems. With cyber-attacks on those systems becoming commonplace, it is clear that a broader cybersecurity T&E approach is needed that focuses on military mission objectives and their critical support systems to address the cyber threat.

Figure 3 provides a high-level view of how cybersecurity-related artifacts, information and events are embedded throughout the acquisition life cycle. The figure demonstrates the inclusion of cybersecurity as an integral part of program management, systems engineering, and T&E artifacts and events. Additional guidance for program management and systems engineering is provided in the *Cybersecurity Implementation Guidebook for Acquisition Program Managers* at https://acc.dau.mil/CommunityBrowser.aspx?id=721696&lang=en-US.

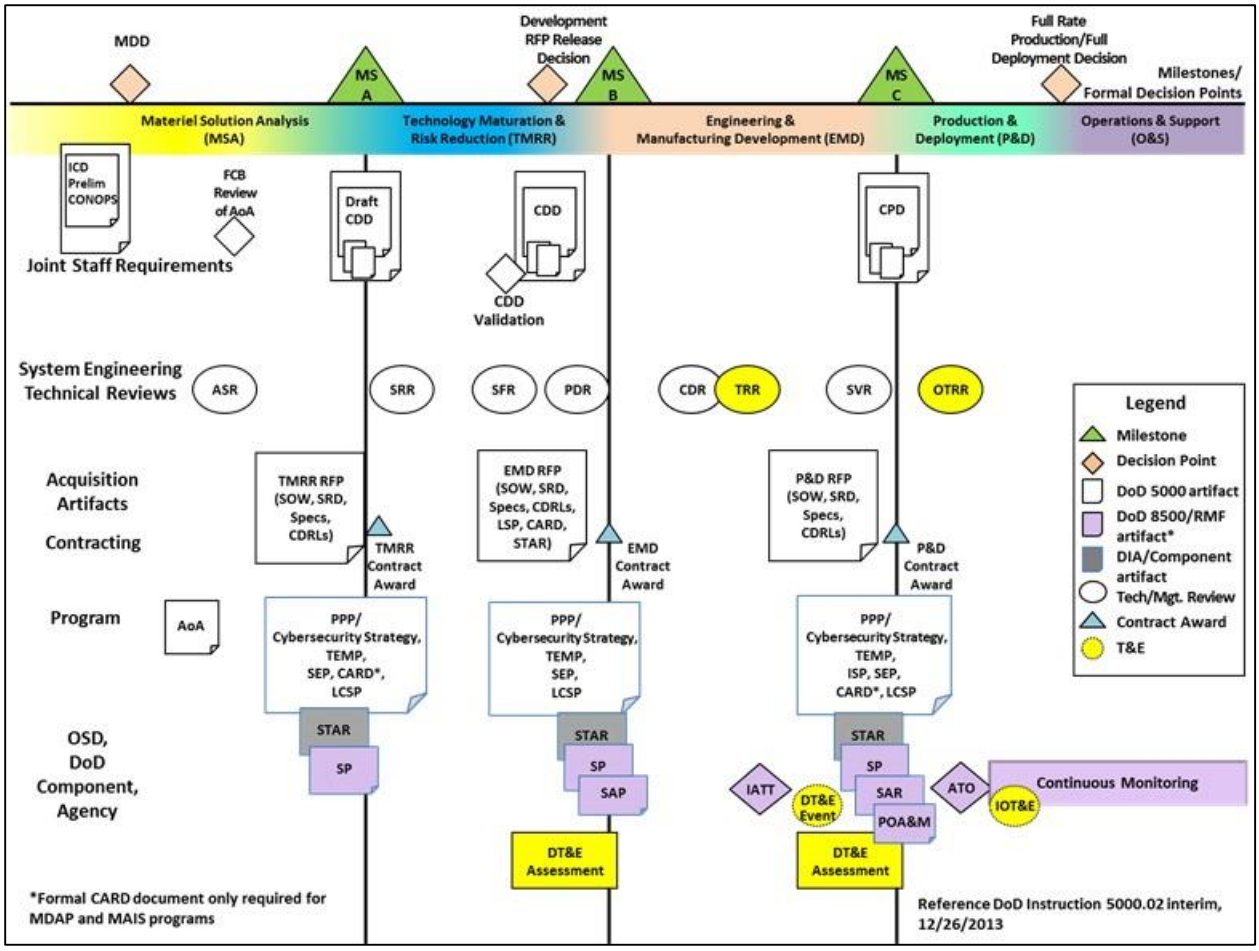


Figure 3. Artifacts and Events Mapped to the Acquisition Life Cycle

T&E events and artifacts, shown in yellow, include DT&E assessments, representing comprehensive assessments of the program at major milestones, to include an assessment of cybersecurity. The T&E phase descriptions in the following subsections provide additional information on these assessments. Although these assessments are shown at MS B and MS C, cybersecurity T&E activities that support those assessments begin before MS A. The guidance in the following subsections define the cybersecurity T&E phases, providing detailed guidance to the Chief Developmental Tester, Lead DT&E Organization, Operational Test Agency (OTA), T&E WIPT, SCAs, and the program's cybersecurity subject matter experts (SMEs).

3.2 DoDI 5000.02

DoDI 5000.02 was signed on January 7, 2015. It includes the following instructions related to cybersecurity T&E:

- The PM will take full advantage of DoD ranges, labs, and other resources (Enclosure 4).
- DT&E activities will start when requirements are being developed to ensure that key technical requirements are measurable, testable, and achievable (Enclosure 4).
- The DT&E program will support cybersecurity assessments and authorization (Enclosure 4)
- The PM will develop a strategy and budget resources for cybersecurity testing. The test program will include, as much as possible, activities to test and evaluate a system in a mission environment with a representative cyber threat capability (additional guidance is included in the DAG) (Enclosure 4).
- For Major Defense Acquisition Programs (MDAPs), Major Automated Information System (MAIS) programs, and Under Secretary of Defense for Acquisition, Technology, and Logistics (AT&L)) - designated special interest programs, the DT&E TEMP approval authority will provide the Milestone Decision Authority (MDA) with an assessment at each milestone review or decision point (Enclosure 4).
- Beginning at Milestone (MS) A, the TEMP will document a strategy and define resources for cybersecurity T&E (Enclosures 4 and 5).
- Beginning at MS B, appropriate measures will be included in the TEMP and used to evaluation operational capability to protect, detect, react, and restore to sustain continuity of operation (Enclosure 5).

The policy clearly provides direction to integrate cybersecurity T&E early and continuously in the acquisition life cycle.

3.3 Cybersecurity T&E Phases

Figure 4 depicts the cybersecurity T&E phases, occurring from pre-MS A test planning, through developmental test, to cybersecurity T&E after MS C. A key feature of cybersecurity T&E is early T&E involvement in test planning and execution. Planning is a part of each cybersecurity T&E phase and some activities may be accomplished concurrently.

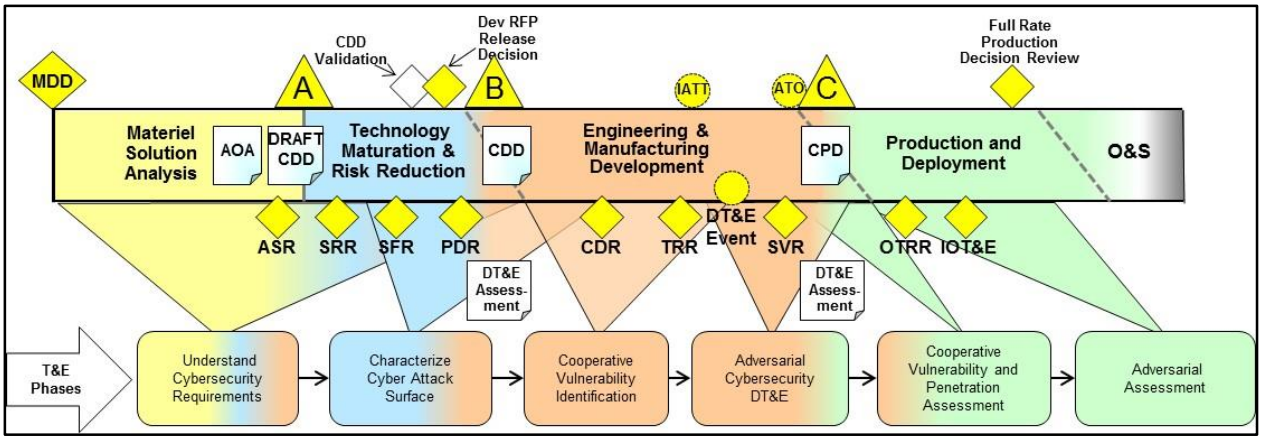


Figure 4. Cybersecurity T&E Phases Mapped to the Acquisition Life Cycle

Cybersecurity T&E phases are iterative, (i.e., activities may be repeated several times due to changes in the system architecture, new or emerging threats, and changes to the system environment). For example, the first two phases, which involve analysis to understand requirements and identify the cyber-attack surface, may be iterated with a significant change to the system architecture, as shown in Figure 5. These activities would coincide with updates to the TEMP and with systems engineering (SE) activities to update requirements, architecture, and design and they might be performed concurrently.

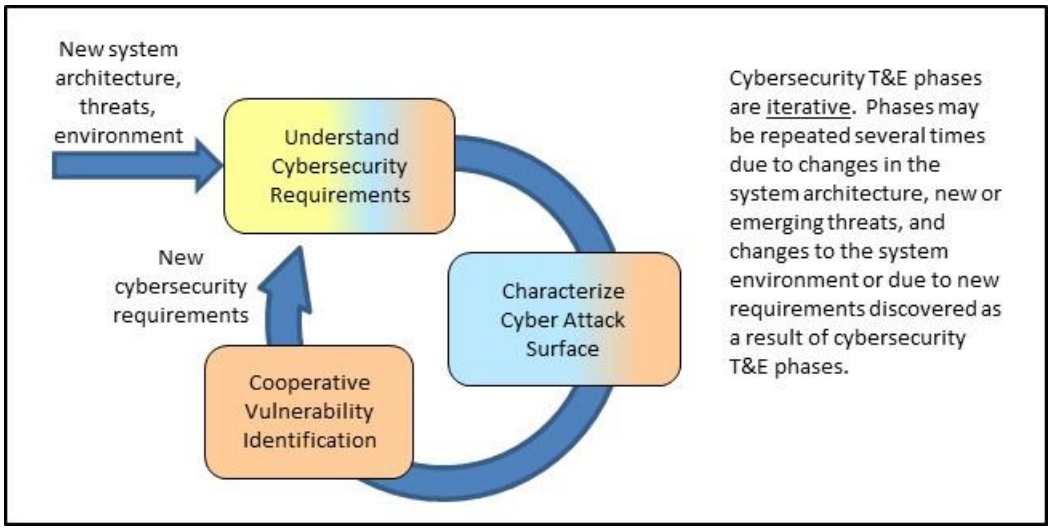


Figure 5. Cybersecurity T&E Phases are Iterative

The first four cybersecurity T&E phases primarily support DT&E. The goal of cybersecurity DT&E is to identify issues before MS C that are related to resilience of military capabilities from cyber threats. Early discovery of system vulnerabilities can facilitate remediation and reduce impact on cost, schedule, and performance. The Deputy Assistant Secretary of Defense, Develop-

mental Test and Evaluation (DASD(DT&E)) will include an evaluation of cybersecurity in Defense Acquisition Executive Summary reviews and DT&E Assessments provided at major decision points for programs under DASD(DT&E) oversight. The figure shows DT&E assessments at major milestones within the acquisition life cycle, as mandated by DoDI 5000.02.

The last two cybersecurity T&E phases support OT&E. The purpose of cybersecurity OT&E is to evaluate the ability of a unit equipped with a system to support assigned missions in the expected operational environment.

The overarching guidelines for cybersecurity T&E are:

- Planning and executing cybersecurity DT&E should occur early in the acquisition lifecycle, beginning before MS A or as early as possible in the acquisition lifecycle.
- Test activities should integrate RMF security control assessments with tests of commonly exploited and emerging vulnerabilities early in the acquisition life cycle. More information on RMF security controls is available in the RMF KS at https://rmfks.osd.mil.
- The TEMP should detail how testing will provide the information needed to assess cybersecurity and inform acquisition decisions. Historically, TEMPs and associated test plans have not adequately addressed cybersecurity measures or resources. The activities described in this guidebook facilitate development and integration of cybersecurity T&E, including the use of specialized resources, and facilitate the documentation of cybersecurity T&E in the TEMP.
- The cybersecurity T&E phases support the development and testing of mission-driven cybersecurity requirements, which may require specialized systems engineering and T&E expertise. The Chief Developmental Tester may request assistance from SMEs such as vulnerability testers and adversarial testers (Red Team-type representatives) to assist in implementation of cybersecurity testing.

The cybersecurity T&E phases are described in more detail in the subsections below.

3.3.1 Understand Cybersecurity Requirements

3.3.1.1 Understand Cybersecurity Requirements - Purpose

The purpose of this first phase is to understand the program's cybersecurity requirements and to develop an initial approach and plan for conducting cybersecurity T&E. Figure 6 shows this phase within the acquisition life cycle.

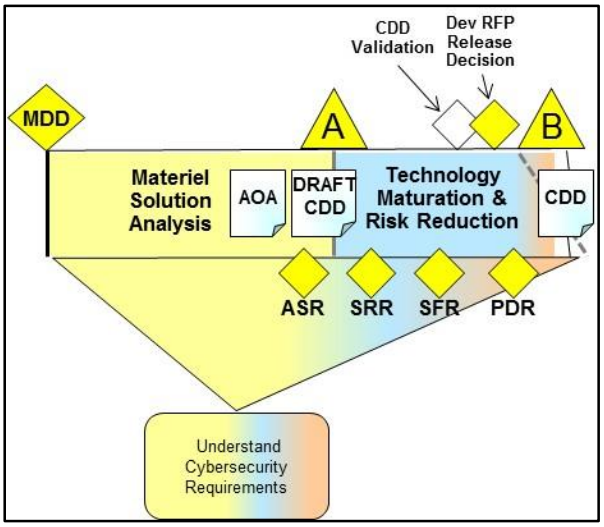


Figure 6. Understand Cybersecurity Requirements Phase in the Acquisition Life Cycle

Prior to MS A, the security requirements and specifications are aligned and documented in the Initial Capabilities Document (ICD), the PPP (and attached Cybersecurity Strategy), and the RMF Security Plan as defined in DoDI 8510.01. As early as possible in the acquisition process, the Chief Developmental Tester, in collaboration with the T&E WIPT, should examine all available program documents to gain an understanding of system cybersecurity requirements. These activities support understanding cybersecurity requirements. As a member of the T&E WIPT, the Lead Operational Test Agency participates in understanding cybersecurity requirements, consistent with DOT&E August 1, 2014 procedures.[10]

3.3.1.2 Understand Cybersecurity Requirements - Schedule

Understanding cybersecurity requirements typically begins prior to MS A. This phase should occur as early in the acquisition process as testable cybersecurity requirements are identified, to plan for cybersecurity T&E and test resources as part of the T&E strategy. Analysis and planning may be repeated when additional materials and information are available, (e.g., with the update of the TEMP at each milestone).

Understanding cybersecurity requirements should be performed regardless of where the program is in the acquisition life cycle. For example, if a program is currently moving toward MS C and has previously not performed any of the phases within the Cybersecurity T&E Process, then the program would start with understanding the cybersecurity requirements and move through the entire process. At a minimum at MS A, the Chief Developmental Tester could note the RMF security categorization and any other pertinent information from the RMF Security Plan and include it within the TEMP. For Milestone B, the TEMP should be updated with information from

[10] DOT&E Memorandum, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, August 1, 2014.

the updated Security Plan, the updated PPP, the Security Assessment Plan, and information learned during the Technology Maturation and Risk Reduction (TMRR) acquisition phase.

3.3.1.3 Understand Cybersecurity Requirements - Inputs

Some or all of the following program artifacts are inputs to understanding cybersecurity requirements:

- Acquisition Strategy.
- Capabilities documents (i.e., ICD, draft Capability Development Document [CDD], or CDD), depending on entry into the acquisition life-cycle process.
- PPP, including a criticality analysis. The Cybersecurity Strategy will be attached to the PPP.
- Validated cyber threat description from the System Threat Assessment Report (STAR)[11], Capstone Threat Assessment[12], or other Service/Component document.
- TEMP (or draft TEMP).
- RMF Security Plan and Security Assessment Plan. Coordinate with the SCA for the Security Assessment Plan.

Reviewing the Program Protection Plan

Program Protection is a component of mission assurance that helps programs ensure that they adequately protect their technology, components, and information. The PPP provides input to the Chief Developmental Tester and the test community by identifying critical components and information, defining potential countermeasures, and linking these to cybersecurity controls defined in the RMF process. The PPP is required at MS A and is updated in preparation for subsequent milestones; the PPP is reviewed and used as input to the TEMP and other test artifacts prepared for each milestone. The PPP Analysis Guidance and Checklist for T&E (see Appendix D) may be used by the Chief Developmental Tester and test team to review and use information included in the PPP for cybersecurity T&E planning.

3.3.1.4 Understand Cybersecurity Requirements - Major Tasks

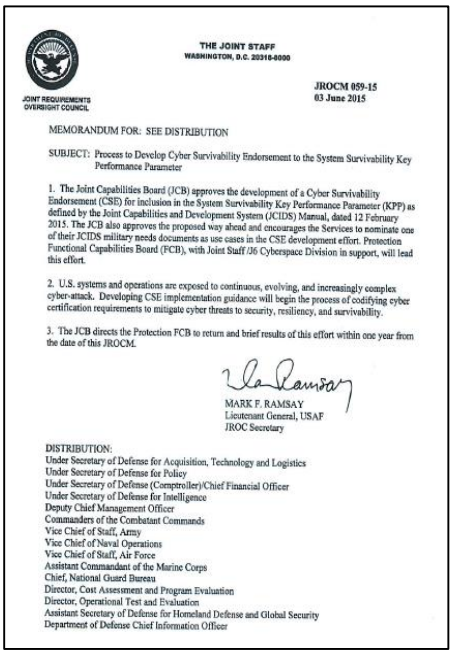
Ensure Appropriate T&E WIPT Representation: The Chief Developmental Tester and the test community should ensure that the T&E WIPT includes all of the appropriate stakeholders and representatives from such resources as Cyber Ranges to address cybersecurity. Refer to Appendix F for more information on Cyber Ranges.

[11] The STAR provides a holistic assessment of enemy capabilities to neutralize or degrade a specific U.S. system by addressing both threat-to-platform and threat-to-mission. The STAR is intended to serve as the authoritative threat document supporting the acquisition decision process and the system development process.

[12] Capstone Threat Assessments (CTAs) address, by warfare area, current and future foreign developments that challenge U.S. warfighting capabilities. CTAs present the validated DoD Intelligence Community position with respect to those warfare areas, and constitute the primary source of threat intelligence for the preparation of Defense Intelligence Agency (DIA) or Service-validated threat assessments (e.g., STARs) and threat portions of documents supporting the JCIDS process. The Cyberspace Operations CTA addresses adversary threat capabilities within the cyberspace domain.

Compile the List of Cybersecurity Requirements: Review the capabilities documents, the PPP, and the Security Plan to understand the system mission focus and the critical components, critical program information, and critical interfaces and data exchanges. Based on this information, compile the initial list of cybersecurity requirements.

Note that the Joint Requirements Oversight Council (JROC) released a memorandum on June 3, 2015, shown in Figure 7, approving the development of a Cyber Survivability Endorsement for inclusion in the System Survivability Key Performance Parameter (KPP). The memo references the *Manual for the Operation of The Joint Capabilities Integration and Development System* (JCIDS Manual), 12 February 2015, which can be accessed here: https://dap.dau.mil/policy/Documents/2015/JCIDS_Manual_-_Release_version_20150212.pdf.



THE JOINT STAFF
WASHINGTON, D.C. 20318-9000

JOINT REQUIREMENTS OVERSIGHT COUNCIL

JROCM 059-15
03 June 2015

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Process to Develop Cyber Survivability Endorsement to the System Survivability Key Performance Parameter

1. The Joint Capabilities Board (JCB) approves the development of a Cyber Survivability Endorsement (CSE) for inclusion in the System Survivability Key Performance Parameter (KPP) as defined by the Joint Capabilities and Development System (JCIDS) Manual, dated 12 February 2015. The JCB also approves the proposed way ahead and encourages the Services to nominate one of their JCIDS military needs documents as use cases in the CSE development effort. Protection Functional Capabilities Board (FCB), with Joint Staff J6 Cyberspace Division in support, will lead this effort.

2. U.S. systems and operations are exposed to continuous, evolving, and increasingly complex cyber-attack. Developing CSE implementation guidance will begin the process of codifying cyber certification requirements to mitigate cyber threats to security, resiliency, and survivability.

3. The JCB directs the Protection FCB to return and brief results of this effort within one year from the date of this JROCM.

MARK F. RAMSAY
Lieutenant General, USAF
JROC Secretary

DISTRIBUTION:
Under Secretary of Defense for Acquisition, Technology and Logistics
Under Secretary of Defense for Policy
Under Secretary of Defense (Comptroller)/Chief Financial Officer
Under Secretary of Defense for Intelligence
Deputy Chief Management Officer
Commanders of the Combatant Commands
Vice Chief of Staff, Army
Vice Chief of Naval Operations
Vice Chief of Staff, Air Force
Assistant Commandant of the Marine Corps
Chief, National Guard Bureau
Director, Cost Assessment and Program Evaluation
Director, Operational Test and Evaluation
Assistant Secretary of Defense for Homeland Defense and Global Security
Department of Defense Chief Information Officer

Figure 7. JROC Memo on Cyber Survivability Endorsement

Requirements for cybersecurity should be included as part of the System Survivability KPP. Additional cybersecurity requirements may be implied or derived from system characteristics, e.g., operation on a public network, the host environment, and system access methods. All of these sources of requirements should be considered when planning cybersecurity testing.

Identify Cyber Threats: Identify cyber threats from the STAR or qualified document that can be used to guide test planning. Threat-based testing focuses on emulating the exploits that the adversary uses, described in the validated threat assessment documents. Test planning is dependent on discovering the validated cyber threats so that testing for those threats can be factored into infrastructure planning as early as possible. These validated cybersecurity threats can be used to guide an evaluation of how mission functions may be impacted in the later phases. If the STAR does not adequately describe the cyber threats, the Service/Component Capstone Threat Assessment document may be used. If cyber threat details are lacking in specificity, consult with the Service threat organization or Defense Intelligence Agency (DIA) point of contact to obtain details.

Document Cybersecurity Activities in the TEMP: Document cybersecurity in the overarching T&E strategy in the TEMP, including:

- Plan cybersecurity test events before MS B, if possible, with further specification and updates continuing through program deployment
- Ensure that defined cybersecurity T&E events are included within the overall T&E schedule

- Ensure that cybersecurity T&E events and cybersecurity test objectives that are included in general T&E events are not traded away due to schedule or resource constraints
- Identify cybersecurity T&E resources and activities, including:
  - RMF security controls assessment
  - Vulnerability assessment, which may be executed via a Blue Team-type activity (these could be a contractor or government organization)
  - Adversarial assessment, which may be executed via a Red Team-type activity (these could be a National Security Agency [NSA]-certified government organization)
  - Use of Cyber Ranges (e.g., National Cyber Range, DoD Cybersecurity Range, Joint Information Operations Range, contractor labs) and tools (e.g., vulnerability analysis software, modeling and simulation) necessary to evaluate cybersecurity, including resource (funding) requirements
  - Cybersecurity SMEs and other required personnel resources.

The TEMP should discuss the integration of cybersecurity T&E events, test organization(s), cooperative vulnerability testing, adversarial assessment, SCA, cyber threats to be emulated during test events, and cybersecurity T&E resources (such as Cyber Ranges, modeling and simulation, and test tools).

Develop the Initial Developmental Evaluation Framework: Evaluation issues for cybersecurity should be included as part of the DEF. Measures to address cybersecurity issues should be scoped appropriately for the SUT and should be suitable to the nature of the system. The requirements, development, and operational communities should work with the T&E WIPT to identify appropriate issues and measures for the system. The evaluation framework should be based on relevant developmental test (DT) objectives. Appendix B provides examples of the cybersecurity definitions within the DEF. Refer to the Defense Acquisition Guidebook, Chapter 9 for specific details on the DEF.

Develop the Initial OT Evaluation Framework: As part of the OT Evaluation Framework, the TEMP should include measures for cybersecurity as part of operational test plans. The Director, Operational Test and Evaluation (DOT&E) will consider the adequacy of the integrated test strategy in the TEMP and of individual test plans to provide information for the measures and to resolve the issues during the review and approval of these documents. Cybersecurity measures should be scoped appropriately for the SUT, addressing issues such as rapid identification of hostile cyber activity, rapid reaction to penetration and exploitation, and related operational issues. Appendix C provides examples and additional information. The requirements, development, operational, and test community representatives should work together to identify appropriate measures for the system. Refer to the Director, Operational Test and Evaluation (DOT&E) Memorandum dated 1 August 2014, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs" and to the DAG, Chapter 9, for specific details on required OT&E metrics and measures.

Linkage of the RMF artifacts with the TEMP: The Chief Developmental Tester should review the RMF artifacts (i.e., the Security Plan and Security Assessment Plan) with the assistance of the SCA to leverage key areas for use in the development of the TEMP. The RMF Security Assessment Package should include a Security Plan that has been approved by an AO and

that contains the system categorization, tailored controls, and a continuous monitoring strategy. The initial RMF Security Plan, with system categorization and the initial security control set, is used at the Alternative Systems Review (ASR).

The Chief Developmental Tester should coordinate with the SCA to align development of the RMF Security Assessment Plan with development of the TEMP. The SCA develops the Security Assessment Plan and gets in approved by the AO. The Security Assessment Plan should be aligned with the pre-MS B decisional TEMP delivery. The TEMP should reflect RMF activities and include a schedule of controls assessment (TEMP Part II) and resources required for controls assessment (TEMP Part IV). The Chief Developmental Tester and the SCA should coordinate TEMP and Security Assessment Plan development to ensure that the RMF is fully integrated with the TEMP and detailed test plans. Section 2 of this guidebook describes the RMF process; further information is available in DoDI 8510.01 and the RMF KS.

The Chief Developmental Tester should also work with the program's systems engineering team to ensure that the controls included within the Security Plan are combined with any additional system engineering countermeasures and included within the Technical Requirements Document (TRD) or similar system engineering artifacts so they can be reviewed for inclusion within the developmental Request for Proposal (RFP) and later the program contract. The TRD should include all applicable security requirements that are needed in the system, and therefore should be considered in T&E activities

Prepare DT&E Analysis: The Chief Developmental Tester should consider providing a preliminary DT&E analysis in support of the Preliminary Design Review (PDR) that delineates the cybersecurity testing during TMRR phase, along with any cybersecurity assessments to date. This analysis should include a discussion of the following:

- Critical missions and mission functions
- System components associated with the critical missions/functions
- Critical developmental software items
- System security categorization in the RMF Security Plan
- Cybersecurity testing that has occurred to date
- Cybersecurity assessment that has occurred to date,
- Initial DEF, including cybersecurity with consideration of software assurance, RMF security controls, anti-tamper, and supply chain risk management (see Appendix B for additional information on the DEF)
- Initial OT Evaluation framework
- Test infrastructure considerations.

Provide Input to the RFP: Review and provide input to RFPs, e.g.:

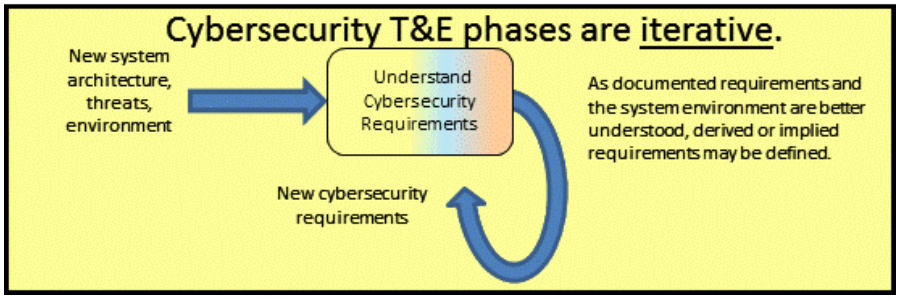
- Consider including a requirement for contractors to develop software abuse cases, network resiliency abuse cases (e.g. Denial of Service attacks) and other system abuse cases and to include testing for these cases.
- Require the prime contractor to demonstrate that the system can be accredited.

- Include specific contract requirements for cybersecurity testing and include pedigree of the data.

For additional guidance, reference "Incorporating Test and Evaluation into DoD Acquisition Contracts" at https://acc.dau.mil/CommunityBrowser.aspx?id+497349&lang=en-US.

3.3.1.5 Understand Cybersecurity Requirements - Outputs

- Preliminary DT&E analysis prepared by the Chief Developmental Tester in support of the PDR.
- Inclusion of T&E items within the program MS B RFP.
- Development of a draft TEMP (pre-MS B and developmental RFP release decision), with inclusion of cybersecurity within the overall T&E strategy. This strategy should be coordinated with the Security Assessment Plan. The draft TEMP will be updated as necessary for approval at MS B, including planned cybersecurity events and required resources.



3.3.2 Characterize the Cyber-Attack Surface

3.3.2.1 Characterize the Cyber-Attack Surface - Purpose

In this phase, the opportunities an attacker may use to exploit the system are identified in order to plan testing that evaluates whether those opportunities continue to allow exploitation. The cyber-attack surface should be characterized in conjunction with the systems security engineering process. The T&E WIPT should collaborate with SE and system developers to determine and prioritize the elements and interfaces of the system that, based on criticality and vulnerability analysis, need specific attention in the cybersecurity part of the T&E strategy. The attack surface is the system's exposure to reachable and exploitable vulnerabilities; in other words, any hardware, software, connection, data exchange, service, removable media, etc. that might expose the system to potential threat access. Systems engineers and system contractors identify these vulnerabilities, as well as critical program information and critical components, as part of the system security engineering process that is executed during the engineering development phase. The T&E WIPT should include in the MS B TEMP the plans for testing and evaluating the elements and interfaces of the system deemed susceptible to cyber threats.

The Chief Developmental Tester should take advantage of component subject matter expertise, key documentation, and other references in performing this phase. Component subject

matter experts may include Blue Team/Red Team-type representatives and key system documentation may include Systems Viewpoint (SV)-1, SV-6, and Operational Viewpoint (OV)-6 documents,[13] operational concepts, and RMF artifacts, such as relevant Security Technical Implementation Guides (STIGs) (reference http://iase.disa.mil/stigs/ for more information). Characterizing the cyber-attack surface is shown within the acquisition life cycle in Figure 8.

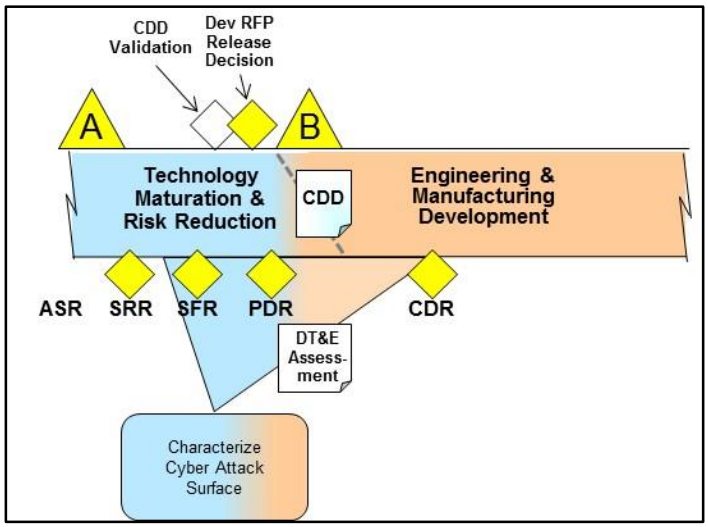


Figure 8. Characterize the Cyber-Attack Surface Phase in the Acquisition Life Cycle

3.3.2.2 Characterize the Cyber-Attack Surface - Schedule

This phase will ideally start prior to EMD, during TMRR, as shown in Figure 8. This phase should be performed wherever the program enters the acquisition life cycle. Throughout the development process, this phase will be revisited at each milestone and may be iterated as design changes are made, since they may introduce new vulnerabilities.

3.3.2.3 Characterize the Cyber-Attack Surface - Inputs

Some or all of the following program artifacts may be inputs for characterizing the cyber-attack surface:

- Results, or results to date, of the understanding cybersecurity requirements (i.e., the prior phase) to identify all cybersecurity requirements
- System architecture products (SV-1, SV-6) to assist in understanding system boundaries and interfaces
- Concept of Operations (CONOPS) to assist in understanding system operations and threats relevant to the CONOPS

[13] Key system documentation, such as the SV-1, SV-6, and OV-6 DoD Architecture Framework documents are defined in the DAG, Section 7.2.5.

- Identification of the assigned cybersecurity service provider or Computer Network Defense Service Provider (CNDSP) and host enclave to understand network connectivity
- PPP, to identify critical components and data
- RMF Security Plan and Security Assessment Plan to understand selected security controls.

3.3.2.4 Characterize the Cyber-Attack Surface - Major Tasks

Identify the Cyber-Attack Surface: Examine system architecture products (e.g., SV-1, SV-6 viewpoints) to identify interfacing systems, services, and data exchanges that may expose the system to potential threat exploits, including:

- Direct network connections: Some systems connect directly to a DoD network (and thus may connect to the Internet). Cyber adversaries take advantage of configuration and architectural weaknesses found on perimeter systems, network devices, and Internet-accessing client machines to gain access into a secure enclave and subsequently expand their reach within the system.
- Indirect DoD network connections: Indirect connections occur when a system connects to a trusted system and that trusted system is connected to the DoD network. Attackers can compromise a trusted system and then use it as a point from which to compromise other systems that are not directly connected to the DoD network.
- Temporary connections and unused connections (e.g., storage devices used to upload new software, maintenance ports, enabled ports that are not in use).
- Delivered support components that are defined by the PPP as critical technology, components, and information that may be at risk.
- The presence of the common vulnerabilities: Examples of common vulnerabilities are listed Appendix G and also may be reviewed at the National Vulnerability Database at http://nvd.nist.gov.

Note that system architecture artifacts may not provide the necessary fidelity to understand the cyber-attack surface. The Chief Developmental Tester, in conjunction with the SE team, may develop a ports, protocols, and services spreadsheet as the system moves through the lifecycle.

Figure 9 shows examples of system elements that may be considered in identifying the cyber-attack surface. The Chief Developmental Tester may consider this list of elements as a starting point for defining possible avenues of attack. Analysis of the system with its exposure to threat exploits should be performed to define the list of elements. Particular attention should be paid to all modes of system access, especially passwords and manufacturer-default access mechanisms.

Review RMF Artifacts to Help Identify the Attack Surface: RMF artifacts such as the Security Plan and Security Assessment Plan may be useful in identifying additional components that constitute the system's attack surface. Note that there may be a delta between the security controls assessment test boundaries as compared to the DT&E system of systems (SoS) scope. The SoS scope may be represented in multiple RMF packages that should be reviewed.

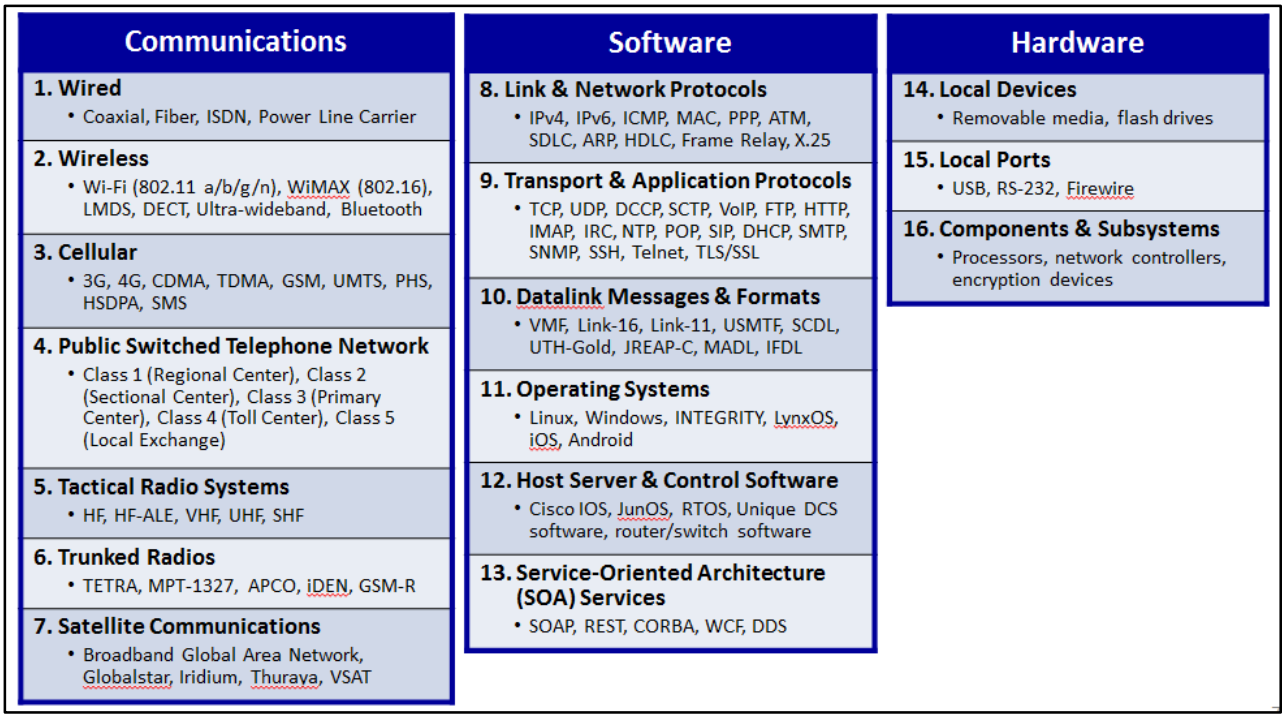


Figure 9. Example Elements of the Cyber-Attack Surface

Analyze the Attack Surface: Analyze the attack surface to identify likely avenues of cyber-attack. The Chief Developmental Tester is encouraged to bring in SMEs (e.g., CNDSP, Blue or Red Team-type representatives, the ISSM, Engineering) to assist with such considerations as:

- The cyber-attack avenues that pose the highest risk for the system. Factors may include accessibility, technical ability required to use different avenues of attack, and exposure of different system components. Special attention should be paid to critical components and critical information that is defined in the PPP.
- Compliance of system components with all applicable STIGs and technical specifications in SE documents.
- Use of the contractor system integration lab to analyze the cyber-attack surface and contractor test events.

Understand Roles and Responsibilities: Examine the system CONOPS to understand roles and responsibilities of system operators, system administrators, and the CNDSP. Knowing who is responsible for each activity ensures that the attack surface and associated countermeasures and defensive activities are considered in the analysis.

Consider Host Environment: Identify host environment provisions for system protection, monitoring, access control, system updates, and so on. Gaining an understanding of the host security systems helps to ensure that systems are designed to work together more efficiently and effectively—from system to host enclave to CNDSP. Review requirements documents to assist in identifying derived requirements and other controls requirements.

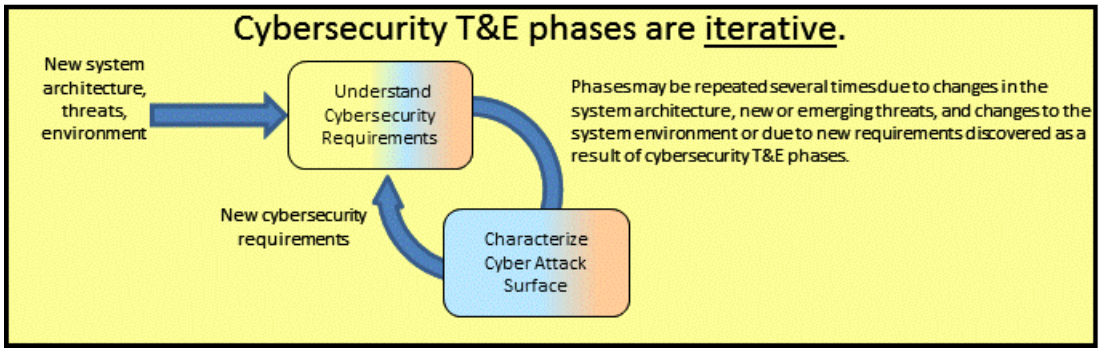
Formulate Test Strategy: Based on the identification of the attack surface, identify the vulnerabilities that are most likely to exist in the system and formulate a test strategy to address them. Include the strategy within the overall T&E Strategy Part III of the TEMP.

3.3.2.5 Characterize the Cyber-Attack Surface - Outputs

The characterization of the cyber-attack surface provides input into subsequent test planning. Products that should be complete at the end of this phase are:

- List of interfacing systems and data connections that may expose the system to potential threats
- Updated list of common vulnerabilities that may exist in systems, including those identified through the RMF process (as documented in the RMF POA&M, if available)
- Identification of planned cybersecurity responsibilities, including:
  - CNDSP and host environment (enclave) roles and responsibilities as required in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01 and DoDI O-8530.2
  - System administration roles and responsibilities.
- List of additional security measures required or provided by host enclave or CNDSP
- List of derived cybersecurity requirements that will be added to the specified requirements
- Updated TEMP (test schemes, test articles, test facilities, test expertise) at MS B. Part II of the TEMP should include the RMF security assessment schedule. A threat profile or model should be created in such a way that it allows the addition of information as it becomes known in order to continually review the attack surface. Threats will evolve and new vulnerabilities will become known in the future.

The characterization of the cyber-attack surface will provide input to the DT&E Assessment at MS B (e.g., it will inform the requirements considered and the test events and resources assessed).



3.3.3 Cooperative Vulnerability Identification

3.3.3.1 Cooperative Vulnerability Identification - Purpose

The Cooperative Vulnerability Identification phase is illustrated in Figure 10. This phase includes detailed test planning and execution of vulnerability testing. This testing and analysis is performed to support and provide feedback to the Critical Design Review (CDR) and as input to and in preparation for the Test Readiness Review (TRR). Note that vulnerability testing may consist of one or more test events.

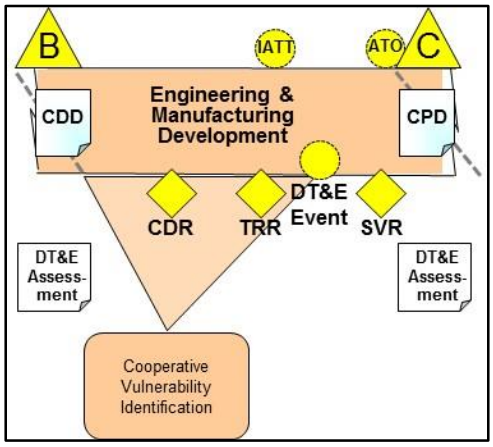


Figure 10. Cooperative Vulnerability Identification in Preparation for the TRR

The purpose of this phase is to identify vulnerabilities that may be fed back to systems designers, developers, and engineers so that mitigations can be implemented to improve resilience. This test, analyze, fix, test process, shown in Figure 11, provides the early and ongoing feedback, addressing cybersecurity vulnerabilities throughout system development so that mitigations may be cost effectively implemented early in the acquisition lifecycle

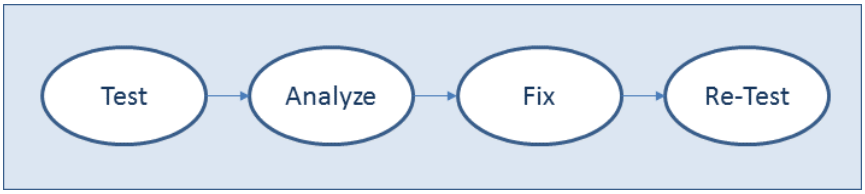


Figure 11. Test, Analyze, Fix, Re-Test process

3.3.3.2 Cooperative Vulnerability Identification - Schedule

This phase begins after MS B, with vulnerability testing results providing input to the CDR and preparation for the TRR. An assessment of security controls performed after the CDR may result in an IATT. The IATT provides input to the TRR in support of DT&E events post-CDR.

3.3.3.3 Cooperative Vulnerability Identification - Inputs

Some or all of the following program artifacts are inputs to this phase:

- List of interfacing systems and data connections that may expose the system to potential threats (based on documents examined in previous activities).
- Attack surface analysis and RMF security controls assessment, including vulnerabilities that may exist in the system, along with those identified through the RMF process (as documented in the RMF POA&M).
- Updated Security Plan that lists additional security measures required or provided by host enclave or CNDSP.
- List of derived cybersecurity requirements. Note that derived requirements may be included in the Technical Requirements Documents issued to the contractor in the RFP. However, derived requirements may also have to be specified once technology choices, such as the use of commercial off-the-shelf/government off-the-shelf (COTS/GOTS), planned system interfaces, and protocols are completed.
- IATT, if available, with supporting Security Assessment Plan and RMF POA&M.
- The vulnerability test environment is a system of systems (SoS) environment. The SoS should include the following components as discovered during the analysis in previous activities:
    - SUT
    - CNDSP inherited protections
    - Critical data exchanges
    - Critical interfaces to mission systems that may introduce attack vectors
    - Vulnerabilities discovered through the RMF process as available.

3.3.3.4 Cooperative Vulnerability Identification - Major Tasks

Finalize the SoS Testing Environment: Identify test opportunities in which representative systems and services will be available to conduct cybersecurity testing in a SoS context.

Review RMF Artifacts: The output of the security controls assessment performed for IATT is a Security Assessment Report, including an RMF POA&M. The Security Assessment Report may require another update of the Security Plan to document any deviations from security specifications. The Security Assessment Report and Draft RMF POA&M, if available, can provide input to vulnerability testing. Note that there may be a delta between the test boundaries for security controls assessment as compared to the system of systems scope that will be used for adversarial cybersecurity DT&E. The system of systems scope may be represented in multiple RMF packages that should be reviewed to understand the entire system of systems scope.

Perform a Vulnerability Assessment of the SUT:

Note that the vulnerability testing performed in this phase is different from RMF security controls assessment. The primary difference is system scope—developmental test will likely involve testing of components (critical data exchanges and system interfaces) that are not usually included in the security controls assessment. Critical data exchanges and interfacing systems with

critical mission impact should be tested in developmental testing. Another difference is the mission focus on critical components that is introduced by developmental test analysis. Vulnerability test events may focus more on critical mission assets late in the systems development life cycle versus a compliance effort across all components.

Like other test events, developmental vulnerability test events should be documented in detailed test plans. The Chief Developmental Tester, in collaboration with the vulnerability test team, will describe the overarching test objectives, such as comprehensive system scanning or vulnerability mitigation assessment. Test planners will scope the tests, providing specific information on what systems, data exchanges, and interfaces will be tested and how they will be tested. The test plan should detail any test limitations or special cases that will require unique treatment. A schedule should provide information on when vulnerability tests will be conducted and their estimated duration. The plan should specify any required resources (cyber SMEs, tools, contractor development labs, Cyber Ranges, etc.) or data (previous security controls assessments). For more information on test plans, see the DAG, Section 9.4.3.

The vulnerability assessment should identify likely avenues of cyber intrusion and the most likely threat exploitation. Test data from the security controls assessment may be reused to supplement cybersecurity DT data. Where mitigations have been identified in the RMF POA&M, the vulnerability test teams should ensure that mitigations pertaining to critical mission components have been tested and any deficiencies corrected prior to adversarial assessment. Any vulnerability discovered during the vulnerability assessment should be addressed, and any remaining non-remediated vulnerabilities should be noted and tracked by the DT test team and in the RMF POA&M. Developmental vulnerability testing may include a wide range of formal and informal test events that are unique for each program.

The Chief Developmental Tester should ensure that the vulnerability testing results in a report that identifies technical and non-technical vulnerabilities at the conclusion of the analysis. The report may be used as an input to the cybersecurity kill chain analysis. For example the Vulnerability Assessment report should answer the following questions at a minimum:

- What are the initial results of the RMF security controls assessment?
- What are the results of the Vulnerability Assessment analysis and what are the outstanding recommended corrective actions? This may include recommended fixes for consideration by the PM.

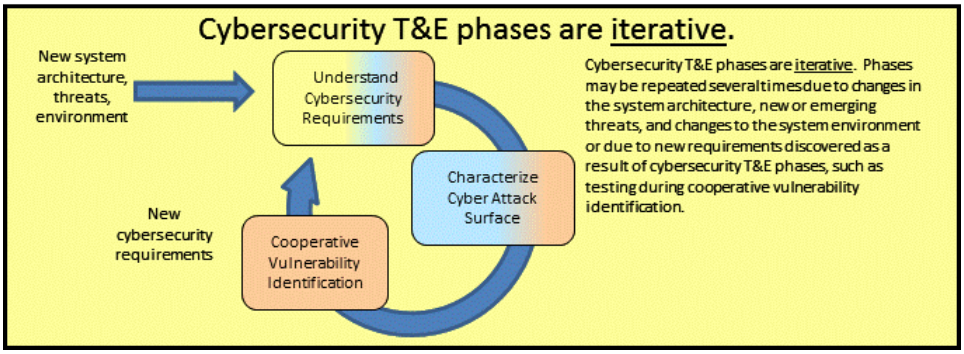
To prepare for the Adversarial cybersecurity DT&E event, the following recommended questions are worthy of consideration:

- What potential vulnerabilities remain that are likely to be exploited?
- What are the likely tactics, techniques, and procedures (TTPs) an adversary will use to gain access to the system?
- What operational activities can the adversary perform when it gains access to a system?
- What *essential* cybersecurity requirements should be met to mitigate operational impacts of documented vulnerabilities and predicted adversary activities?

Verify and Finalize Infrastructure in Preparation for Cybersecurity DT&E Event: The completion of this phase includes finalizing infrastructure planning for the cybersecurity DT&E event, which is performed in the next phase. Issues to consider include system under test technology maturity, classification, and closed loop testing, data collection, among others.

3.3.3.5 Cooperative Vulnerability Identification - Outputs

- Formal cooperative vulnerability assessment (Blue Team-type report)
- Planning for Cybersecurity DT&E performed in the next phase (which may include a TRR)
- Verification of T&E infrastructure requirements for the cybersecurity DT&E event
- Evidence that known system vulnerabilities are remediated and enumeration of residual vulnerabilities completed and tracked.



3.3.4 Adversarial Cybersecurity DT&E

3.3.4.1 Adversarial Cybersecurity DT&E - Purpose

The Adversarial Cybersecurity DT&E phase, shown in Figure 12, includes an evaluation of the system's cybersecurity in a mission context, using realistic threat exploitation techniques, while in a representative operating environment. Using the Vulnerability Report, the Security Assessment Report, and DT&E artifacts, the DT team performs a cybersecurity kill chain analysis to determine what an attacker could do if it gained access to the SUT, and how the SUT would respond to such attacks. It includes adversarial assessment testing, which emulates the threats described in the program's validated threat capabilities document. Though adversarial assessment, including penetration testing, may result in destruction to the SUT, it is not the intent during DT&E to default to this destructive type testing. Rather, penetration testing may be used to better understand the risk to the SUT. Depending on risk, cybersecurity DT&E may involve the use of a Cyber Range to reduce the risk of collateral damage to live networks and authoritative data sources.

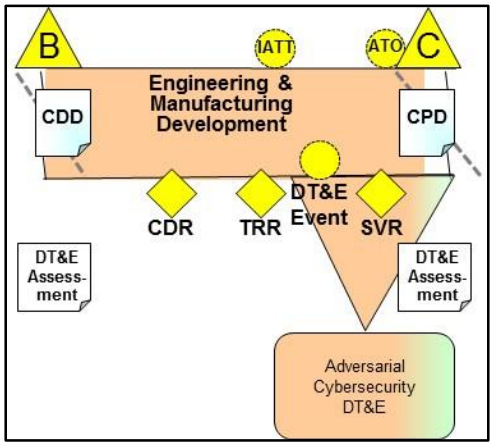


Figure 12. Adversarial Cybersecurity DT&E in the Acquisition Life Cycle

The goal of the adversarial cybersecurity DT&E event is to discover critical vulnerabilities and determine their impacts. This will include:

- How will critical mission objectives be impacted if the data or processes required to execute the mission objectives are altered due to cyber-attack and/or exploitation?
- How will critical mission objectives be compromised if required data or processes are unavailable?
- How will critical mission objectives be compromised if mission data or processes are exploited in advance of mission execution?

3.3.4.2 Adversarial Cybersecurity DT&E - Schedule

This phase should be planned for execution prior to MS C to support a production decision.

3.3.4.3 Adversarial Cybersecurity DT&E - Inputs

Some or all of the following program artifacts may be inputs to cybersecurity DT&E:

- Successful completion of the TRR
- Vulnerability assessment which may be executed via a Blue Team-type activity
- Verification of cybersecurity T&E infrastructure requirements
- Evidence that known system vulnerabilities are remediated and enumeration of residual vulnerabilities completed and tracked, based on the RMF POA&M, the PPP, or program artifacts
- Development test results to date
- RMF test results to date.

3.3.4.4 Adversarial Cybersecurity DT&E - Major Tasks

Cybersecurity Kill Chain Analysis: A cybersecurity kill chain analysis is performed to determine what an attacker may be able to do if they were able to gain access to the system and to identify possible response scenarios. The cybersecurity kill chain is depicted in Figure 13.

A cybersecurity kill chain is a sequence of actions performed by a specified threat adversary that executes cyber intrusions with specific objectives, such as data theft. Although there are variations of the kill chain, the typical adversary stages include reconnaissance (recon), weaponization, delivery, exploitation, control, execution, and persistence. All cybersecurity kill chain stages will not necessarily apply to every system. SUTs should be analyzed in a manner consistent with the cyber threat assessment documented in the STAR or similar document. As part of this phase, the DT team may contact the DIA and Component activities to develop threat vignettes[14]. Figure 13 demonstrates the type of activities that may be performed during the kill chain analysis, the threat and defender objectives and the types of data that may be collected during the analysis.

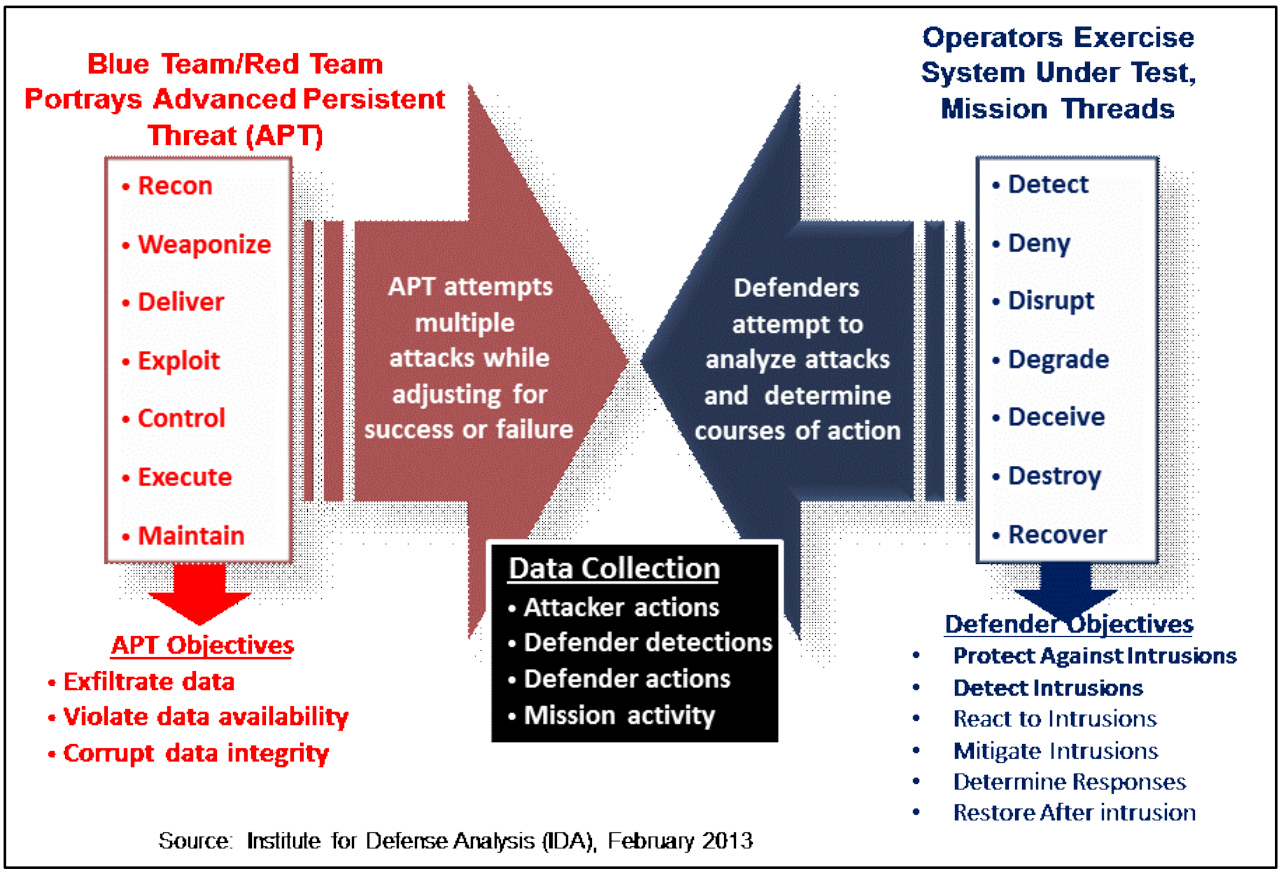


Figure 13. Cybersecurity Kill Chain

The cybersecurity kill chain analysis is based in large part on the vulnerability assessment, performed in the previous phase, of the system and its interfaces. The vulnerability assessment may have identified likely avenues of cyber intrusion and the most likely threat exploitation.

[14] The Chief Developmental Tester may coordinate with DIA or the Component Intelligence activity to develop vignettes to assist in test plan development and use during penetration testing.

Complete Preparation of Test Infrastructure: Careful infrastructure planning is required for adversarial cybersecurity DT&E. It is generally not recommended that this event be performed on the Department of Defense Information Networks (DoDIN) and it is important to note that an NSA Certified Red Team is required for any adversarial event conducted on DoDIN. A representative test infrastructure, including cybersecurity test range facilities, should be used to replicate the CNDSP and cyber-realistic environment during DT&E. Ensure the use of an isolated infrastructure environment with connections to sources of critical data exchanges and interfaces as needed. A shared test event may be used, e.g., testing both interoperability and cybersecurity, but the program should plan carefully for a mix of dedicated and shared test events for cybersecurity testing. Shared test events should focus on the possible use of shared infrastructure, which reduces time to set up the range environment and can provide economy of scale for multiple test events. However, executing concurrent test events, particularly cybersecurity, on the same infrastructure at the same time can seriously skew the test results in unpredictable ways and should be avoided. Test events should be conducted serially, allowing time for reset of the test environment before the next test cycle occurs.

Preparing Adversarial/Penetration Test Events

Penetration Test Events are sometimes referenced as "adversarial" (Red Team) in their approach. The PM and the assessment organization should agree on the rules of engagement and the scope of the assessment prior to its start. This agreement may involve legal counsel and CNDSP involvement to ensure all legal and technical provisions are taken into consideration. Although they will vary depending on the organization performing the assessment, typical pre-conditions required for an assessment are:

- All legal procedures, including restrictions related to Classified networks and systems are defined and appropriate authority is granted.
- A stable system and network environment exists
- The program has defined a trusted agent to observe the activity and halt it if required.
- The test team understands the system mission.

The following are examples of costs that may be considered by the program when planning for the assessments:

- System configuration in a stable environment (hardware and software) on which to perform testing.
- Necessary training.
- Licensing.
- Impact/dependency on existing services
- Personnel requirements to support testing
- Network availability and bandwidth (as applicable)
- Tools and equipment for the assessment

Appendix F provides additional information regarding the selection and us of Cyber Ranges.

The Chief Developmental Tester may coordinate with DIA or the Component intelligence activity to develop vignettes to assist in developing test plans that the adversarial assessment team may use during penetration testing.

Adversarial (Red team-type) test teams, testers (Chief Developmental Tester, OTA), test infrastructure providers, and system owners should agree on specific rules of engagement before testing begins. These rules of engagement will generally provide the test team with flexibility during testing (not tied to a specific script) while it still operates within a rule set agreed to by all parties. A flexible and restorable test environment would ease restrictions in the rules of engagement. The less flexible the environment, the tighter the rules of engagement will be, resulting in less effective and less thorough cybersecurity testing.

Plan Adversarial DT&E: The Adversarial DT&E Team (often a Red Team) should meet with the Chief Developmental Tester to develop a detailed test plan. The team will share its rules of engagement and will describe its threat portrayal based on its knowledge and the information provided by the program. Through its analysis, the team will identify assets of value, system processes, vulnerabilities, attack plans and methods, and scheme types and indicators.

The Adversarial DT&E Team should be given time to conduct reconnaissance on the SUT and its surrounding protections. This mimics real-world situations where an adversary may have a great deal of time to study a system operating in the field. Additionally, providing the team with information on the targeted systems during test planning may help to accelerate reconnaissance.

Ideally, the targeted systems will have the flexibility to be altered, compromised, and corrupted during Adversarial DT&E Team testing. This will allow the team to represent most accurately the actions an adversary might conduct. This flexibility would require that targeted systems have the ability to be restored to their original operating conditions within a short time (to allow multiple test runs).

Time should be allotted between test runs to make configuration changes. This will allow the system to explore configuration settings to optimize cyber defenses—a limited test-fix-test methodology. Changes would be limited to minor configuration or tactics changes, as there would not be time to make significant changes.

The Chief Developmental Tester, in collaboration with the Adversarial DT&E Team (which may be the Red Team-type activity) should formally document detailed test plans. Like the vulnerability (Blue team-type) test events and other test events, Adversarial DT&E Team detailed test plans should describe test objectives, systems under test, test methods to be used, test timelines, rules of engagement (how far can they go within the SUT to include destruction) and required resources. The detailed test plan should include if the SUT will be tested via LVC, any and all connections. The plan should also include if the SUT or any portion of the SUT will be emulated. The detailed test plans should also include the items described in the paragraphs above, including the basis for threat portrayal, specific threat vignettes, likely targets, and the agreed-upon rules of engagement (which may act as limitations or boundaries to test activities). For more information on test plans, see the DAG, Section 9.4.3.

Care should be taken when combining cybersecurity test objectives with other test objectives (e.g., interoperability). Cybersecurity testing, particularly intrusive, corrupting, or destructive testing, can have an impact on achieving other testing objectives. Note that destructive testing is not always required and agreements about destructive / non-destructive testing should be explicitly defined in the rules of engagement that are included in the detailed test plan. If destructive testing is included, testers may want to sequence testing such that cybersecurity testing takes place later in a series of test runs.

Perform Adversarial DT&E Assessment: Cybersecurity DT&E includes conducting an Adversarial T&E Team assessment to identify remaining vulnerabilities, resulting in an Adversarial T&E Assessment Report. The test event will include launching attacks at the various elements of this SoS (system, enclave, data connections) to expose vulnerabilities. The Adversarial T&E Team will use methods typical of cyber threat adversaries (as described by threat documents) to expose additional vulnerabilities. They will report any remaining vulnerabilities, including, but not limited to, those from the Common Vulnerabilities List.

During adversarial cybersecurity DT&E, the test team may be able to directly show what the mission impacts of exploited vulnerabilities would be. If the test team is unable to fully execute an attack due to caution or constraints, further study may be required (by system engineers, testers, and security experts) to show what the adversary may have been able to accomplish.

The test team report will identify vulnerabilities discovered in system components, the team's assessment of possible impacts to mission operations, and the recommended corrective actions.

Recommended corrective actions may include:

- TTP changes
- Configuration changes
- Software or hardware modifications.

These recommended corrective actions may not be limited to the SUT, but may extend to the host enclave and CNDSP. Shortfalls identified in this and previous phases should be resolved prior to proceeding to operational test and evaluation, and programs should plan sufficient time and resources for these resolutions.

Prepare DT&E Assessment: The comprehensive DT&E assessment that includes a cybersecurity evaluation is prepared as input to the MS C decision. For MDAPs, MAIS, and programs on the AT&L Special Interest list, DASD(DT&E) will include a cybersecurity analysis within the DT&E assessment in support of MS C. For programs not under oversight, the component assessment process should include an analysis of cybersecurity.

Cybersecurity DT&E should answer the following:

- What are the final results of the RMF security controls assessment?
  - – Have all deficiencies been resolved?
  - – Is there a plan and schedule for remediating critical unresolved vulnerabilities?
  - – If mitigation or remediation efforts have been completed, have they been tested and included in the DT evaluation report?
- What are the results of the Adversarial DT&E test?
  - – What kill chain activities was the test team successful in implementing?
  - – What common vulnerabilities were successfully exploited?
  - – What were the test limitations?
- How resilient is the system to cyber-attack when supporting mission operations?
- What are the recommended corrective actions
  - – For the PM?
  - – For the user?
  - – For the host environment and/or CNDSP?
- When should the next cybersecurity tests occur in support of new capability development and/or threat assessment?

3.3.4.5 Adversarial Cybersecurity DT&E - Outputs

- Adversarial DT&E event conducted; Adversarial DT&E Assessment report
- A cybersecurity evaluation to be included in the DT&E assessment for MS C
- Critical operational mission impact assessment
- TEMP updated for MS C.

3.3.5 Cooperative Vulnerability and Penetration Assessment

3.3.5.1 Cooperative Vulnerability and Penetration Assessment - Purpose

The OTA completes Cooperative Vulnerability and Penetration Assessment, shown in Figure 14, either before or following MS C (as appropriate). The purpose of this phase is to provide a comprehensive characterization of the cybersecurity status of a system in a fully operational context, and to substitute for reconnaissance activities in support of adversarial testing when necessary. This phase consists of an overt and cooperative examination of the system to identify vulnerabilities. Refer to the DOT&E Memorandum dated 1 August 2014, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs" for specific details on required OT&E metrics and measures.

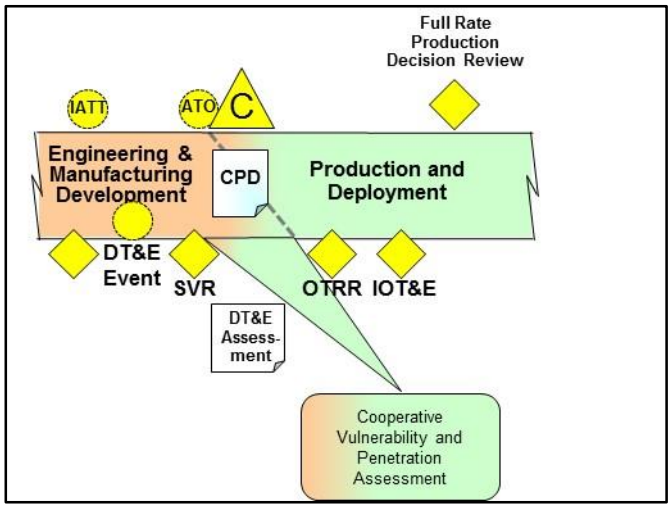


Figure 14. Cooperative Vulnerability and Penetration Assessment in the Acquisition Life Cycle

This operational test shall be conducted by a vulnerability assessment and penetration testing team through document reviews, physical inspection, personnel interviews, and the use of automated scanning, password tests, and applicable exploitation tools. The assessment should be conducted in the intended operational environment with representative operators. The minimum (core) data to be collected in this test is identified in Appendix C, and includes the evaluation of selected cybersecurity compliance metrics; cybersecurity vulnerabilities discovered; intrusion, privilege escalation and exploitation techniques used in penetration testing; and metrics for password strength. The assessment should consider operational implications of vulnerabilities as they

affect the capability to protect system data, detect unauthorized activity, react to system compromise, and restore system capabilities. This testing may be integrated with DT&E activities if conducted in a realistic operational environment and approved in advance by DOT&E. It may use data from earlier OT or OT of related systems as appropriate. OTAs should share the results from this assessment to permit the correction of deficiencies or when necessary to support a comprehensive adversarial assessment.

3.3.5.2 Cooperative Vulnerability and Penetration Assessment - Schedule

This phase should begin after the SUT has received an ATO or an IATT in an operationally representative network(s). This phase will occur preferably before MS C, but might occur afterward, depending upon the following considerations:

- System developmental and design maturity. The Cooperative Vulnerability and Penetration Assessment examines a mature system design in a representative operational environment. The timing for delivery and availability of mature representative systems for this evaluation should be considered when developing the test schedule.
- Software/system maturity (status of previously identified shortfalls). The intent is to begin the Cooperative Vulnerability and Penetration Assessment either with previously identified significant shortfalls resolved or with mitigations that are documented in the test plan. The inability to either resolve or document mitigations to vulnerabilities from earlier test events should be considered when developing the test schedule.
- DOT&E or appropriate OT&E guidance. The test strategy as documented in an approved TEMP will provide guidance on the composition and timing of the Cooperative Vulnerability and Penetration Assessment. This guidance will establish expectations on the specific timing of this phase for the program.
- Data available to support the MS C decision. The OTA and DOT&E for oversight programs will provide operational assessment input to the MS C decision using the information available from completed testing. When the Cooperative Vulnerability and Penetration Assessment cannot be completed until after MS C, the operational assessment will use information from previous phases. Integrated testing is encouraged to maximize information from testing resources.

3.3.5.3 Cooperative Vulnerability and Penetration Assessment - Inputs

The following program artifacts or activities are inputs to this phase:

- An ATO or IATT is obtained before conducting operational testing. This includes all systems and environments needed to support a continuity of operations evaluation.
- Previously identified significant shortfalls are resolved or mitigated and documented in the test plan.
- All residual DT&E is completed and an updated DT&E assessment is provided by DASD(DT&E) or the Component in support of an Operational Test Readiness Review (OTRR).
- OTRR is completed.

- The appropriate authority (DOT&E for programs under oversight) has approved the operational test plan, including cybersecurity testing.

3.3.5.4 Cooperative Vulnerability and Penetration Assessment - Major Tasks

Plan T&E: The OTA has the lead role for conduct and reporting. Because this is an OT&E event, the OTA is responsible for planning, conducting, and reporting the Cooperative Vulnerability and Penetration Assessment. The OTA is responsible for developing the analytical framework of issues, measures, and data requirements; the data collection procedures to include instrumentation, recording of observations and actions, and surveys; the framework of the test design such as length, scenarios, vignettes; and providing a formal report that addresses the collected data and evaluation results. Details should be coordinated through the T&E WIPT and documented in the operational test plan and reports. Test planning should consider the following resources:

- Qualified Team to act as the cybersecurity Vulnerability Assessment Team.
- Authorized tools to assess system cybersecurity (typically provided by the Blue Team).
- The SUT and all interfacing systems needed to exercise critical data exchanges and information services.
- Representative network architecture to include supporting network infrastructure (routers, servers) and network defense capabilities (computer network defense service providers, firewalls, network and host-based intrusion detection devices). The intent is to create a representative cybersecurity posture that includes layered defenses at least one level removed from the SUT (e.g., Tier 2 computer network defenses if the SUT typically operates within the Tier 3 defenses).

Qualified and Certified Red and Blue Teams
While there are no set criteria for certifying Blue Teams, Red Teams must be certified by the NSA and accredited through the U. S. Strategic Command and U. S. Cyber Command to ensure they are able to transit DoD networks without doing harm to government systems. Blue Teams are usually qualified by the sponsoring agency.

- Representative operators and cybersecurity defenders, including computer network defense service providers.
- Operational facilities or platforms that are representative of those expected for use when the SUT is deployed.
- Operational test range(s) and system/network simulations where appropriate and authorized.
- Cyber Ranges, if necessary, with appropriate Verification, Validation and Accreditation completed for OT&E.

Coordinate with a Cybersecurity Vulnerability Assessment Team: The Program Office supports the planning and execution of the evaluation by coordinating with the OTA to identify required resources. Identifying and scheduling a cybersecurity vulnerability assessment team (a qualified and certified Blue Team) for the event is among the most important tasks to

begin early in the test planning. Coordination should include establishing a schedule, desired capabilities, and expected products such as annexes to the operational test plan, data collection and reporting, and a formal report of activities and findings. If the evaluation is planned as an integrated test event, then the PM should facilitate coordination among all involved test organizations and agencies to clearly identify all data requirements.

Ensure Sufficient Post-Test Availability for Correction/Mitigation of Test-Discovered Vulnerabilities.

3.3.5.5 Cooperative Vulnerability and Penetration Assessment – Outputs

The following are outputs from this phase:

- The OTA has documented all discovered vulnerabilities and provided the documentation to the Program Office, OT&E authority, and DOT&E (as appropriate).
- The Program Office has developed a POA&M for remediating all major vulnerabilities before entering the next phase, adversarial assessment.
- The Program Office has documented operational implications of vulnerabilities that cannot be corrected.

3.3.6 Adversarial Assessment

3.3.6.1 Adversarial Assessment - Purpose

This phase, shown in Figure 15, assesses the ability of a unit equipped with a system to support its missions while withstanding validated and representative cyber threat activity. In addition to assessing the effect on mission execution, the OTA shall evaluate the ability to protect the system, detect threat activity, react to threat activity, and restore mission capability degraded or lost due to threat activity. Refer to the DOT&E Memorandum dated 1 August 2014, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs" for specific details on required OT&E metrics and measures.

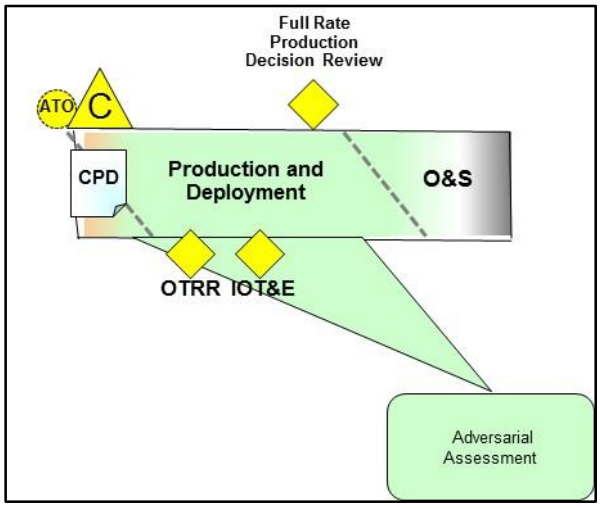


Figure 15. Adversarial Assessment in the Acquisition Life Cycle

This phase should be conducted by an OTA employing a certified adversarial test team (Red Team) to act as a cyber-aggressor. The adversarial test team should attempt to induce mission effects by exploiting vulnerabilities to support evaluation of operational mission risks. The adversarial assessment should include representative operators and users, local and non-local cyber network defenders (including upper tier computer network defense providers), an operational network configuration, and a representative mission with expected network traffic. When necessary due to operational limits or security, tests may use simulations, closed environments, or other validated and operationally representative tools approved by DOT&E to host cyber threat activity and demonstrate mission effects. The aggressor team may use data from the vulnerability and penetration assessment phase to develop and execute this assessment when insufficient opportunity exists for the adversarial team to conduct independent reconnaissance or to ensure that all critical vulnerabilities are assessed during this phase. The minimum (core) data to be collected is specified in Appendix C, including metrics characterizing the system protect, detect, react, and restore capabilities, as well as the mission effects induced by the cyber threat activity.

A meaningful evaluation of mission effects will be system-specific, and should be expressed in terms of performance parameters already being used to assess operational effectiveness. Mission effects could include shortfalls in the confidentiality, integrity, and availability of critical mission data. In cases where direct measurement of mission effects in the operational setting or in a simulated environment is not feasible due to safety or operational concerns, the OTA shall propose an alternative assessment method, involving SMEs, by which they ascertain the effect of the vulnerabilities discovered on system performance. For enterprise systems, the assessment should consider continuity of operations, and for systems primarily concerned with financial data, financial fraud should be evaluated alongside other mission effects.

3.3.6.2 Adversarial Assessment - Schedule

The schedule for Adversarial Assessment is as follows:

- The Adversarial Assessment is conducted before the Full Rate Production or Full-Deployment Decision. The Adversarial Assessment can be conducted during or in support of the IOT&E.
- Duration of Adversarial Assessment will depend upon the details of the system design and cyber threat, but a minimum of one to two weeks of dedicated testing is a nominal planning factor, with a potentially longer preparation period for threat reconnaissance and research activity

3.3.6.3 Adversarial Assessment - Inputs

The inputs for this phase are:

- An ATO or IATT is in place for the SUT.
- Previous testing confirms that the system is capable of operation in the intended operational environment, to include all interfaces, systems, and environments needed to support a continuity of operations evaluation.
- All major cybersecurity vulnerabilities identified in previous testing are remediated by verified corrections, documented user-accepted mitigation procedures, or documented acceptance of risk by the Service Acquisition Agent.

- The appropriate authority (DOT&E for programs under oversight) has approved the operational test plan.
- Verification, Validation and Accreditation for all ranges and simulations involved in the event are completed.
- Operators, system administrators, and network administrator have completed training.

3.3.6.4 Adversarial Assessment - Major Tasks

Plan T&E: The OTA has the lead role for conducting and reporting the Adversarial Assessment. The OTA is responsible for developing the analytical framework of issues, measures, and data requirements; the data collection procedures to include instrumentation, recording of observations and actions, and surveys; the framework of the test design such as length, scenarios, and vignettes; and providing a formal report that addresses the collected data and evaluation results. Details should be coordinated through the T&E WIPT and documented in the operational test plan and reports. Test planning should consider the following resources:

- Qualified and certified adversarial test team (may be a Red Team) to act as the threat representative cyber-attack team.
- Authorized tools to assess system cybersecurity (typically provided by the cybersecurity team).
- The SUT and all interfacing systems needed to exercise critical data exchanges and information services.
- Operational facilities and platforms that are representative of those expected when the SUT is deployed.
- Representative network architecture, to include supporting network infrastructure (routers, servers), network defense capabilities (computer network defense service providers, firewalls, network and host-based intrusion detection devices). The intent is to create a representative cybersecurity posture that includes layered defenses at least one level removed from the SUT (which may include either enterprise or Service-level security services and service providers in support of the local network on which the SUT is operated).
- Representative operators and cybersecurity defenders, including Cybersecurity Defense Service Providers.
- Operational test range(s) and system/network simulations where appropriate and authorized.
- Cyber Ranges, if necessary, with appropriate Verification, Validation and Accreditation.

Coordinate with the OTA Team: The Program Office supports the planning and execution of the evaluation by coordinating with the OTA to identify required resources. Identifying and scheduling the event are among the most important tasks to begin early in the test planning. Coordination should include establishing a schedule, desired capabilities, and expected products such as annexes to the operational test plan, data collection and reporting, and a formal report of activities and findings. If the evaluation is planned as an integrated test event, then the PM

should facilitate coordination among all involved test organizations and agencies to clearly identify all data requirements.

3.3.6.5 Adversarial Assessment - Outputs

- The OTA has an authenticated database to support evaluation requirements that includes collected data and any required reports from the adversarial test team.
- The OTA and DOT&E for oversight programs provide reports that assess implications from Cyber Operational Resiliency Evaluation findings for operational effectiveness, operational suitability, and operational survivability.

Appendix A. Analysis Guidance for RMF Artifacts

The following is guidance for the Chief Developmental Tester and the test team in the analysis and use of RMF Artifacts and Documents.

Cybersecurity Strategy – The PM prepares the Cybersecurity Strategy and includes it in the PPP. The Cybersecurity Strategy includes cybersecurity requirements, approach, testing, shortfalls, and authorization for the system being acquired and the associated development, logistics, and other systems storing or transmitting information about that system. The Cybersecurity Strategy should be referenced by and coordinated with the TEMP by the Chief Developmental Tester. The Cybersecurity Strategy provides input for the definition of requirements for vulnerability and adversarial testing.

Security Plan – The RMF Security Plan should be reviewed as part of the first phase of cybersecurity T&E to assist in understanding cybersecurity requirements. The Security Plan provides an overview of the security requirements for the system, system boundary description, the system identification, common controls identification, security control selections, subsystems security documentation (as required), and external services security documentation. The Chief Developmental Tester should review Security Plan with the assistance of the SCA to leverage key components of the Security Plan, such as the description of interconnected information systems and networks, the Security Architecture, and the Authorization Boundary, for use in the development the TEMP.

The initial Security Plan, with system categorization and the initial security control set, is used at the Alternative Systems Review (ASR). The Chief Developmental Tester should ensure that the controls and overlays included within the Security Plan are combined with any additional system engineering countermeasures; these should be included within the Technical Requirements Document (TRD) or similar system engineering artifacts so they can be reviewed for inclusion within the developmental Request for Proposal and later the program contract. It is a good idea to have the TRD include <u>all</u> applicable security requirements that are needed in the system, and that therefore should be considered in T&E activities. Conversely, system engineering countermeasures not accounted for in the Security Plan should be added to it so that a complete picture of all cybersecurity mechanisms required for the system is documented in one place.

Security Assessment Plan –It is highly recommend that the Chief Developmental Tester include the SCA within the T&E Working Integrated Product Team (WIPT) and reference the Security Assessment Plan within the TEMP. The SCA should develop the Security Assessment Plan concurrent with the development of the program TEMP, which allows coordination of information.

The Chief Developmental Tester should coordinate with the SCA to align development of the RMF Security Assessment Plan with development of the TEMP. The SCA develops the Security Assessment Plan, with approval by the AO or AOR. As the Security Assessment Plan is developed, the Chief Developmental Tester should review the selected security controls, the order in which the security controls will be implemented, and who is responsible for security control assessment, and the schedule of controls assessment in order to ensure:

- Security controls assessment is reflected in and coordinated with developmental test events defined in the TEMP.
- The schedule of security controls assessment identifies which controls are implemented and assessed by the contractor and which are assessed by the government.

The Security Assessment Plan should be aligned with the pre-MS B decisional TEMP delivery. The TEMP should reflect RMF activities and include a schedule of controls assessment (Part II) and resources required for controls assessment (Part IV). The Chief Developmental Tester and the SCA should coordinate TEMP and Security Assessment Plan development to ensure that the RMF is fully integrated with the TEMP and detailed test plans. The Chief Developmental Tester should coordinate with the Program Manager to ensure that RFPs address those security controls that will be implemented and assessed by the contractor and that any contractor security controls assessment is addressed in the TEMP.

Security Assessment Report –The Security Assessment Report documents the SCA's findings of compliance with assigned security controls based on actual assessment results. It addresses security controls in a non-compliant status, including existing and planned mitigations. The Security Assessment Report is the primary document used by an authorizing official to determine risk to organizational operations and assets, individuals, other organizations, and the Nation. The Chief Developmental Tester and DASD(DT&E), for programs under oversight, should use the Security Assessment Report as input to their assessment of developmental test results and risk.

Appendix B. Developmental Evaluation Framework

In accordance with DoDI 5000.02, Enclosure 4, paragraph 5(a(11)), starting at MS A, the TEMP includes a developmental evaluation methodology that provides essential information on programmatic and technical risks as well as information for major programmatic decisions. DoDI 5000.02 requires that the developmental evaluation methodology be reflected in a developmental evaluation framework starting with the MS B TEMP. However, it is recommended that the Developmental Evaluation Framework's (DEF) thought and communication process be used from the onset of program DT&E strategy development, and be included in the MS A TEMP.

Starting at MS B, the developmental evaluation framework will identify key data that contributes to assessing progress toward achieving KPPs, CTPs, KSAs, interoperability requirements, cybersecurity requirements, reliability growth plan, maintainability attributes, developmental test objectives, and others (as needed). Note that cybersecurity is covered within the DEF along with other areas such as interoperability, maintainability, etc.; there is no separate cybersecurity evaluation framework, as cybersecurity is fully covered by the DEF.

The DEF describes the key programmatic, acquisition, technical, and operational decisions that will be informed by DT&E. The DEF highlights the information needed to inform those key decision points in terms of Decision Support Questions (DSQ), capabilities, and the technical measures used to quantify the capabilities. The DEF shows the test and modeling and simulation events that will be used to generate the data to evaluate performance and inform program decisions. The integrated test schedule in Section 2.5 of the TEMP and the resources described in Part IV of the TEMP should be logically linked to the DEF, to complete the DT&E strategy description.

The DEF articulates a logical evaluation strategy that informs:

- How acquisition, programmatic, technical and operational decisions will be informed by DT&E
- How system will be evaluated
- What test and M&S events will provide data for evaluation
- The resources / schedule required to execute test, conduct evaluation, and inform decisions

This information is put into a matrix format, as shown in Figure 16.

Guidance for the DEF and its inclusion in the TEMP is provided in DAG Chapter 9.4.2.2.

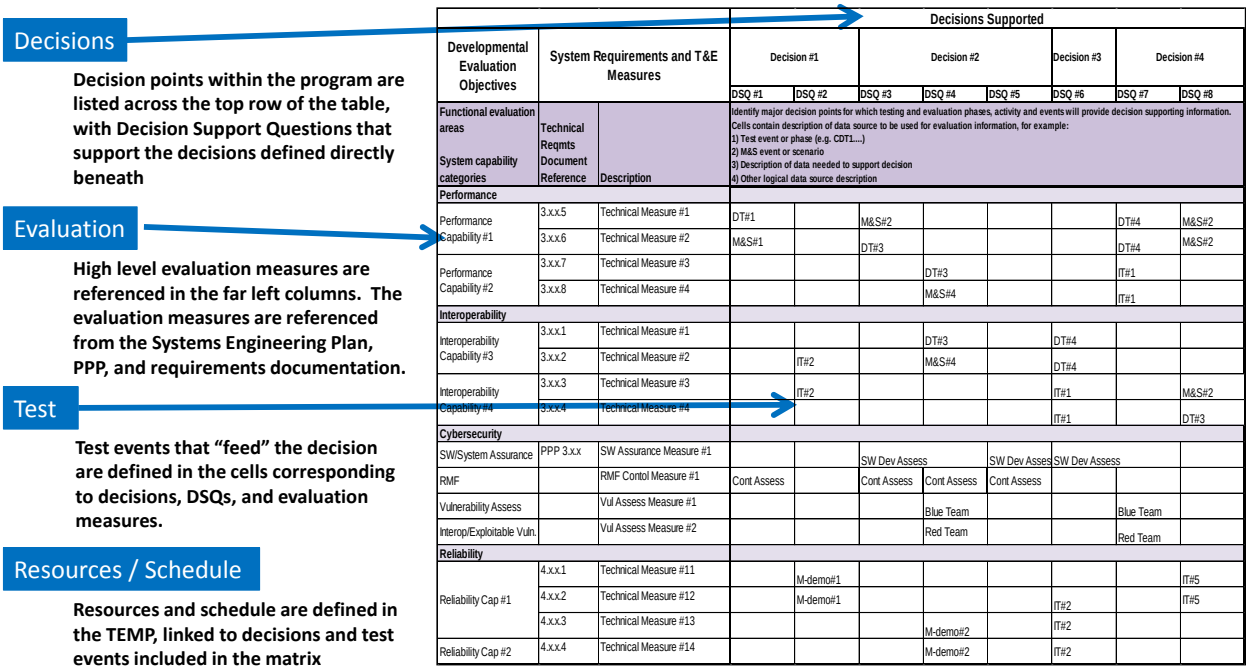


Figure 16. Developmental Evaluation Framework

Cybersecurity is an integral part of the DEF with specific Decision Support Questions and evaluation measures tied directly to cybersecurity. The cybersecurity-related Decision Support Questions and evaluation measures should be scoped appropriately for the SUT. Table 2 lists examples of cybersecurity Decision Support Questions and evaluation measures that may be considered in the development of the DEF.

Table 2. Example DT&E DEF Entries

Functional Evaluation Area	Decision Support Question	Technical Requirements Examples	Measures Sources	Test Activity / Data Sources
Systems and Software Assurance	Are the system and the software developed securely?	• Software vulnerabilities have been eliminated in critical components (source: CVE, CWE, Common Attack Pattern Enumeration and Classification) • Secure software development processes • Secure software development environment • Anti-tamper protections implemented • Supply chain risks mitigated	• Software Development Plan • PPP Table 5.3.3.1 (example measures: number/category of SDRs, CVEs eliminated, CWEs remaining • Information Assurance Strategy or equivalent • PPP Appendix D: Anti-tamper plan • Supply chain risk addressed in PPP Section 5.3.4, in RFP and contracts	• Contractor T&E/ Functional Qualification Testing/ • Anti-tamper Implementation Plan/Report • Supply Chain Risk Management Report

Functional Evaluation Area	Decision Support Question	Technical Requirements Examples	Measures Sources	Test Activity / Data Sources
RMF Requirements	Does the system satisfy baseline cybersecurity technical standards?	• Identified attack surfaces	• Security Assessment Plan, DoDI 8510.01, NIST Special Publication 800-53/53A, CNSSI 1253, and cybersecurity acquisition strategy (example measures include percentage of controls verified, number/category of outstanding deficiencies) • Include technical standards appropriate for the attack surface	• Security Controls Assessor/ ACAs/ vulnerability assessment team • Contractor T&E and government technical standard testing as appropriate

Vulnerability Assessment	Do exposed vulnerabilities adversely affect system resiliency?	• System and supporting networks resilience and ability to disrupt the cybersecurity kill chain
		  ○ Deny and disrupt attacks
		  ○ Degrade attacks
		  ○ Deceive attacks
		• Capability to:
		  ○ Detect exploitations
		  ○ Recover from system degradation
			• Percentage of cyber resources properly configured
			• Number of attempted intrusions stopped at network perimeter/deflected to honeypot
			• Percentage of mission-essential capabilities for which multiple instantiations are available
			• Length of time between initial disruption and restoration
			• Quality of restored data
			• Quality of choices made during design and engineering that affect resiliency
			• Length of time between initial disruption and restoration.
				• Vulnerability assessment Team

System interoperability and functionality in response to exploited cyber vulnerabilities	Is the system sufficiently interoperable and able to sustain critical missions in response to exploited cyber vulnerabilities?	• Entry and management on a network • Secure exchange of information • Support for net-centric military operations • Response to exploited cyber vulnerabilities • Support for military operations in a cyber-contested environment.	• Interoperability measures derived from capabilities documents, Information Support Plan, integrated architectures, Technical Standards (CJCSI 6212.01F) • Cybersecurity measures and scope of adversarial and penetration testing will be based on cyber evaluation measures developed during all prior phases, to potentially include threat portrayals and penetration testing.	Red Team type testing with Test team functioning as an adversary without knowledge or access to the system.

Appendix C. OT&E Cybersecurity Measures

This appendix provides the minimum measures to guide cybersecurity operational evaluations. OTAs as well as DOT&E oversight authorities may also develop measures specifically tailored to the SUT or the type of test anticipated. The use of additional measures is subject to DOT&E approval. Where appropriate, test data from cybersecurity DT&E may be used to resolve cybersecurity OT&E measures, subject to review and approval by the lead OTA and DOT&E.

The TEMP must identify all resources required to execute the cybersecurity T&E, to include funding sources, responsible organizations, threat documentation, critical operational issues, and measures to be employed. DOT&E will approve all cybersecurity measures and test methods included in the TEMP and Operational Test Plans (OTPs). When constructing test plans, ensure that the evaluation of cybersecurity is structured using specific issues and measures for the system under T&E, but consider other cyber-centric testing, potentially including software assurance testing, financial and fraud testing for business systems, and even tests conducted to obtain authorization to connect and operate on DoD information networks.

DOT&E will use the results of cyber testing to determine, in part, operational effectiveness, suitability, and survivability of the system. Cyber tests can be structured under the appropriate critical issues, and should be described by measures of effectiveness and measures of performance that examine not only the "compliance" of the system with known standards, configurations, and operation/management processes, but also the "performance" of the system in terms of supporting the operational missions for which the system was designed. Therefore, testing of cyber systems primarily involved in financial or resource management should consider fraud testing, and examine vulnerabilities in terms of potential financial losses; testing of cyber systems primarily involved in operational force employment should consider testing scenarios that allow examination of system vulnerabilities and their impacts on operational missions. Testing of systems that are not principally cyber systems but are exposed to cyber networks and vulnerable to cyber-attack should consider the impact of losses in operational integrity due to cyber events.

The following subsections detail several categories of cyber testing metrics. Compliance metrics (C.1) are drawn specifically from the NIST RMF, and are considered essential context to the performance testing of a cyber or cyber-connected system. The intent is neither to repeat the risk management assessment conducted to obtain authorization to connect/operate nor simply to reuse the risk management documentation, but to independently verify these elements as part of a test. Compliance with this minimal set of standards is necessary but not sufficient to characterize system effectiveness. Therefore, the subsequent annexes provide minimal measures for assessing key attributes that protect the system (C.2) and the performance of the system in a hostile cyber environment (C.3). The protection metrics can largely be measured through the use of a cooperative vulnerability assessment team (such as a Technical Blue Team) and should include scans, basic penetration testing, and password cracking. The performance metrics are organized by the phases of cyber operations, and are focused on capturing data to analyze the system's defensive capabilities when faced with an offensive threat. The metrics described allow for the collection of "ground truth" for both the aggressor (normally a certified Red Team) and the defenders.

Annexes C.4 and C.5 describe the key issues that should be present in all TEMPs and test plans for systems that will undergo cybersecurity testing.

C.1 Core System Protection Data

System Protection Data		
Title	**Measurement**	**Notes**
Vulnerabilities	Cyber vulnerabilities with descriptions and Defense Information Systems Agency severity codes[15]	Descriptions should include the nature of the vulnerability, affected subsystem(s), and implications for system protect, detect, react, and restore capabilities.
Intrusion/Privilege Escalation/Exploitation Techniques	Intrusion/privilege escalation/exploitation techniques • Starting point • Success/failure • Time to execute • Level of effort (novice/skilled/expert).	If technique is successful, state affected system(s). Level of effort grades: • Novice: Technique can be executed by an actor without formal training or material support (e.g., a "script kiddie"). • Skilled: Technique can only be executed by an actor with some formal training and material support, but does not require an expert actor. • Expert: Technique can only be executed by an actor with state-of-the-art training and ample material support (e.g., a nation state).
Password Strength	Number of passwords attempted to crack Number of passwords cracked For each cracked password: • User or administrator account • Reason for password weakness (e.g., default password, low complexity).	

[15] Defense Information Systems Agency, *Application Security and Development Security Technical Implementation Guide (STIG)* Version 3, Release 6 (24 January 2014).

C.2 Core Cybersecurity Compliance

Cybersecurity Compliance *(Met/Not Met/Not Applicable)*		
Title	**Measurement**	**Notes**
Account Management	Accounts are established after screening users for membership, need-to-know, and functional tasks.	NIST SP 800-53 Revision 4: Control AC-2
Least Privilege	Accesses are granted to users following the principle of least privilege.	NIST SP 800-53 Revision 4: Control AC-6
Identification and Authentication	Organizational users are uniquely identified and authenticated when accessing the system, including when using group accounts.	NIST SP 800-53 Revision 4: Control IA-2
Content of Audit Records	Audit records contain information that establishes the nature, time, location, source, and outcome of malicious events, as well as the identity of any individuals associated with such events.	NIST SP 800-53 Revision 4: Control AU-3
Audit Review, Analysis, and Reporting	Audit records are reviewed and analyzed regularly for indications of inappropriate activity, and any findings are reported to the appropriate cyber defenders.	NIST SP 800-53 Revision 4: Control AU-6
Configuration Settings	The system is installed in accordance with an established baseline configuration following the principle of least functionality, and any deviations from this baseline are recorded.	NIST SP 800-53 Revision 4: Control CM-6
Backup, Recovery, and Restoration	System data is routinely backed up and preserved, and a recovery and restoration plan for the system is provided.	NIST SP 800-53 Revision 4: Controls CP-9, CP-10
Device Identification and Authentication	The information system uniquely identifies and authenticates devices before establishing a connection.	NIST SP 800-53 Revision 4: Control IA-3
Authenticator Management	The cryptographic strength, maximum lifetime, and storage methods for system authenticators (e.g., password, tokens) are compliant with organizational policy.	NIST SP 800-53 Revision 4: Control IA-5

Cybersecurity Compliance ***(Met/Not Met/Not Applicable)***		
Title	**Measurement**	**Notes**
Default Authenticators	System authenticators (e.g., password, tokens) are changed from their default settings.	NIST SP 800-53 Revision 4: Control IA-5
Physical Access Control	The information system, including data ports, is physically protected from unauthorized access appropriate to the level of classification.	NIST SP 800-53 Revision 4: Controls MP-7, PE-3
Boundary Protection	The system monitors and controls data exchanges at the external boundary and at key internal boundaries, including: • Firewalls or guard • Intrusion Protection System/Intrusion Detection System/Host-Based Security System	NIST SP 800-53 Revision 4: Control SC-7
Secure Network Communications	Network communications are secure, and remote sessions require a secure form of authentication.	NIST SP 800-53 Revision 4: Controls SC-8, SC-23
Update Management	Security-related software and firmware updates are applied to the system in a timely manner.	NIST SP 800-53 Revision 4: Control SI-2
Malicious Code Protection	Mechanisms for preventing the deployment of malicious code (e.g., viruses, malware) are installed, configured, and kept up-to-date.	NIST SP 800-53 Revision 4: Control SI-3

C.3 Core Cyber Defense Performance Data

Cyber Defense Performance Data		
Title	**Measurement**	**Notes**
Protect	Adversarial activities • Description • Level of effort (novice/skilled/expert) • Time span • Success/failure.	Include starting position, nature of the technique(s) used, target system, cyber objective (e.g., exfiltration), and other data as specified in the Red Team Collection Matrix (attached).
Detect	Time for defenders to detect each intrusion/escalation of privilege/exploitation	For each detected event, include the means of detection (e.g., Intrusion Detection System [IDS] alert).
React	White cards used • Description • Time issued. Defense activities • Description • Time span • Success/failure. Time for defenders to mitigate each detected intrusion/escalation of privilege/exploitation	Include origin of response (e.g., user, system administrator, cyber defender) and nature of response (e.g., containment, quarantine, reporting).
Restore/Continuity of Operations	White cards used • Description • Time issued. Time taken to restore mission effectiveness after each degradation	Include description of restoration activities undertaken (e.g., restore from backup, failover to alternate site).
Mission Effects	Percentage reduction in quantitative measures of mission effectiveness Where direct measurement not feasible, independent assessment of mission effects (minor, major, severe) using SMEs	Adverse effects could include the confidentiality, integrity, and availability of critical mission data.

Appendix D. PPP Analysis Guidance for T&E

Program Protection is an iterative risk management process across the acquisition lifecycle. Commanders, Program Executive Officers (PEOs), Science and Technology Project Site Directors, PMs, SE, system security, cybersecurity, T&E, and acquisition personnel should be aware of the Program Protection process and should be engaged in supporting it. The Program Protection process is described in detail in the DAG, Section 13. PMs are responsible for complying with this process holistically such that protection decisions are made in the context and trade space of other cost, schedule, and performance considerations. It is important to implement this process across the full acquisition life cycle in order to build security into the system. The process is repeated at each of the following points in the life cycle, building on the growing system maturity:

- Systems Engineering Technical Reviews (see the DAG, Section 13.10.2 for further elaboration on specific Systems Engineering Technical Reviews event expectations), starting pre-MS A with the ASR
- SE analyses that support preparation for each Acquisition Milestone (see the DAG, Sections 13.7.6 and 13.14 for further elaboration on how this process is tied to life cycle phase-related systems security engineering)
- Development and release of each RFP (see the DAG, Section 13.13.1 for further details on what should be incorporated in the RFP package).

At each of these points, the process is iterated several times to achieve comprehensive results that are integrated into the system design and acquisition.

The PPP provides input to the Chief Developmental Tester and the test community by identifying critical components and information, identifying threats and vulnerabilities, and defining potential countermeasures. The PPP is required at MS A and is updated in preparation for subsequent milestones; the PPP should be considered as the TEMP and other test artifacts are prepared for each milestone. The Chief Developmental Tester and test team may use this "PPP Analysis Guidance and Checklist for T&E" to assist in the analysis and use of information included in the PPP for cybersecurity T&E planning.

PPP Analysis for T&E V0.02		
PPP Section	**T&E Analysis Guidance**	**Response**
1.2 Program Protection Responsibilities	Is the Chief Developmental Tester identified in the chain of responsibility for the PPP?	
2.1 Schedule	Are PPP and TEMP schedules consistent and do they include Security Controls Assessments, Vulnerability and Adversarial Assessments in advance of MS C?	
2.2 Critical Program Information (CPI) and Critical Functions and Components Protection	Do the CPI, critical functions, and components correspond with those identified in the TEMP and the Technical Requirements Document?	
	Is the TEMP consistent with the PPP (i.e., does the TEMP address testing the specified CPI, critical functions, and critical components)?	
	Does the program plan to exercise systems where Trusted Systems Design Countermeasures such as anti-counterfeits, export controls, and trusted foundry are explicitly implemented? Inherited? If so, are these addressed in the TEMP?	
3.0 CPI and Critical Components	Does the PPP consider mission packages, government-furnished components, and interdependent systems that may be outside a PM's control? Is this consistent with the TEMP?	
	Is inherited CPI from other acquisition programs, subsystems, or projects incorporated or implemented into this program? Are these considered within the T&E strategy, Part III of the TEMP?	

PPP Analysis for T&E V0.02		
PPP Section	**T&E Analysis Guidance**	**Response**
5.0 Threats, Vulnerabilities, and Countermeasures	Are all CPI and critical functions and components identified in Table 5.0-1? Are identified countermeasures measureable, testable, effective and suitable?	
	Are cybersecurity T&E activities identified in the PPP and consistent with the TEMP in order to evaluate CPI and critical components countermeasures where appropriate?	
	Are the results of vulnerability assessments, Blue/Red teams, etc., performed to date summarized in Table 5.2-1?	
	What are the key cybersecurity schedule milestones? Are these milestones consistent with the T&E Schedule, Part II, and T&E Strategy, Part III, of the TEMP?	
	Are inherited cybersecurity protections (if any) specified in the PPP addressed in any planned Blue Team or vulnerability testing specified in the TEMP?	
6.0 Other System Security-Related Plans and Documents	Are the TEMP and TEMP Approval Authority identified?	
7.0 Program Protection Risks	Does the PPP explicitly call out how cybersecurity T&E activities (identified in Section 5.0) are being used to understand and reduce residual CPI risks? Confirm critical functions, countermeasures? Used to discover any unmitigated risks?	
8.0 Foreign Involvement	Will vulnerabilities identified during cybersecurity T&E be releasable to foreign partners, or must they be NOFORN?	

PPP Analysis for T&E V0.02		
PPP Section	**T&E Analysis Guidance**	**Response**
9.0 Process for Management and Implementation of PPP	Does the PPP explain how the program will integrate system security requirements testing within the T&E Strategy, Part III, of the TEMP? Does it list the Chief Developmental Tester as the responsible person? Is this linked and integrated within the T&E Strategy, Part III, of the TEMP?	
11.0 Program Protection Costs	Does Acquisition and Systems Engineering Protection Costs, Section 11.2, define costs related to cybersecurity T&E resources as defined within Part IV of the TEMP, such as Cyber Ranges and Blue and Red Teams?	
Appendix E: Cybersecurity Strategy	Is cybersecurity T&E discussed in Section VI, IA Testing? Does it point to the TEMP for additional information?	

Appendix E. Cybersecurity T&E Resources

Cybersecurity T&E resources include SCAs, Vulnerability Assessment Teams (Blue Teams), and Adversarial or Threat Representative Teams (Red Teams). These resources and their differences are listed below:

Security Controls Assessment Team	Vulnerability Assessment (Blue Team)	Threat Representative Testing (Red Team)
Assess compliance with security controls	Comprehensive	Exploit one or more known or suspected weaknesses
Execute the Security Assessment Plan	Identifies any/all known vulnerabilities present in systems	Attention on specific problem or attack vector
Linked to the Security Assessment Report Activities	Reveals systemic weaknesses in security program	Develops an understanding of inherent weaknesses of system
Based on STIGs or similar documentation	Focused on adequacy and implementation of technical security controls and attributes	Both internal and external threats
Can be determined by multiple methods: hands-on testing, interviewing key personal, etc.	Multiple methods used: hands-on testing, interviewing key personal, or examining relevant artifacts	Model actions of a defined internal or external hostile entity
Include a review of operational and management security controls	Feedback to developers and system administrators for system remediation and mitigation	Report at the end of the testing
Conducted with full knowledge and assistance of systems administrators, owner, and developer	Conducted with full knowledge and cooperation of systems administrators	Conducted covertly with minimal staff knowledge
No harm to systems	No harm to systems	May harm systems and components and require cleanup

Appendix F. Cyber Ranges and Other Facilities

F.1 Introduction to Cyber Ranges

Cyber Ranges provide capabilities and environments that can be integrated at the appropriate classification levels to conduct research, development, experimentation, and testing of military capabilities within a cyberspace environment. They also can support training military personnel in conducting cyber operations; developing TTPs; and demonstrating the sustainment of critical missions in cyber-contested environments. Use of Cyber Ranges can provide a more realistic environment while minimizing risk to operational networks, particularly where the employment of cyber effects is impractical or high risk. Other applications of Cyber Ranges include:

- Assessment of the scope and duration of advanced cyber effects
- Component-level system interoperability testing
- Combinations of developmental, operational, and integrated testing
- Assessment and authorization (RMF) processes
- Immersive training with rapid experience building.

Adequate DT&E, OT&E, and assessments might require testing on Cyber Ranges for one or more of the following reasons:

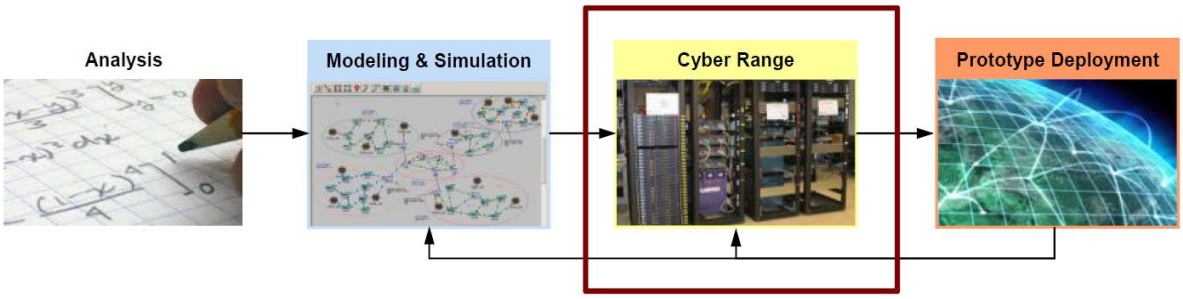
- Testing cannot occur on open operational networks.
- Representations of advanced cyber adversarial TTPs are not suitable for operational networks.
- Scaling requirements (e.g., number of users, hosts, or interconnected systems; amount of network traffic) cannot be otherwise achieved.
- Operational complexity and associated mission risk are such that impact to operational networks should be avoided.

The Program Office/Chief Developmental Tester should work with the Lead Developmental Test & Evaluation Organization, cybersecurity dedicated professionals, Operational Test Agencies, DASD(DT&E), and DOT&E to incorporate Cyber Ranges into the overall test, evaluation, and assessment strategy. In general, the Chief Developmental Tester, SCA, OTA, and PM should do the following as early as possible in the acquisition life cycle:

- Identify all testing that will occur on a Cyber Range.
- Identify cyber events that should be integrated with DT&E, OT&E, and assessment activities.
- Plan for integration of system operators, network defenders, and threat emulations on the Cyber Range.
- Coordinate with Cyber Range staffs to ensure that they understand the SUT, operational environment, user space, threat, test objectives, and planned test scenarios.
- Ensure IC support to accurately represent adversarial threats and targets.
- Verify that targets and offensive capabilities emulated on the range are realistic and representative.

- Ensure that the entire emulated environment is of adequate fidelity to accomplish test objectives, support technical assessment, and demonstrate impact on operational mission. Emulated environments include:
    - Red – Any capability or environment attributed to the adversary forces
    - Blue – Any capability or environment attributed to own forces
    - Gray – Cyber environment that is not owned by any military force, but is leveraged by all cyber forces to obfuscate their actions
- Coordinate with Cyber Range staffs to investigate any automated data collection capabilities that could support the test.

Figure 17 provides some guidance for choosing a cyber-event environment.



	Analysis	Modeling & Simulation	Cyber Range	Prototype Deployment
Fidelity	Low	Low	Moderate to High	High
Scalability	High	High	Moderate	Low
Cost	Low	Low	Moderate	High
Repeatability	N/A	High	Moderate to High	Low
Program Phase	Early	Early	Mid-term	Mid-term to Late

Figure 17. Cyber Event Environment

F.2 Cyber Ranges

Range	Mission	Capabilities
C4 Assessment Division (C4AD) Suffolk, VA Contact E-Mail: JS.DSC.J6.MBX.C4AD-operations@mail.mil	Conduct assessments of existing and emerging Command, Control, Communications, and Computers (C4) capabilities in a persistent C4 environment to achieve interoperable and integrated solutions that satisfy joint operational requirements. Replicates Joint Warfighter C4 systems and addresses the interoperability of those systems.	• C4AD can connect to the Joint Information Operations Range (JIOR) or operate in stand-alone mode. • Replicates operational Command and Control environments with actual hardware and software, enabling assessments of system and SoS interoperability, operational capability, procedural compliance, and technical suitability to confirm readiness for deployment. • The Joint Systems Integration Command/Joint Staff Integration Lab have demonstrated experience combining training exercises and test events to accomplish both test, training, and assessment objectives.
DoD Cybersecurity Range Quantico, VA Contact E-Mail: IARangeCMT@ITSFAC.com	Provide a persistent environment to support T&E, exercise support, training, and education. A simulated representation of the DoDIN Tier 1 environment complete with network services for realistic system/network evaluation.	• The DoD Cybersecurity Range can operate in stand-alone mode, or the Combatant Commands, Services, and Agencies, with their individual cyber environments, can connect to the Cybersecurity Range through: ▪ The JIOR ▪ A virtual private network over the Internet and Defense Research Engineering Network • Persistent environment focused on cybersecurity and computer network defense. • Representation of the DoDIN Tier 1 Environment, complete with network services, for realistic system/network evaluation. • Generic DoD Tier II and Tier III capabilities. • Services include traffic generation, configurable user emulation. Malware, spyware, and BOTnets can be emulated and employed in the environment to stimulate training.

Range	Mission	Capabilities
Joint IO Range (JIOR) Norfolk, VA Contact Phone Numbers: (757) 836-9787 or (757) 836-9848	Create a flexible, seamless, and persistent environment (infrastructure) that enables Combatant and Component Commanders to achieve the same level of confidence and expertise in employing information operations (IO) weapons that they have in kinetic weapons.	• Closed, multilevel security (Top Secret/Sensitive Compartmented Information [SCI]) environment built to conduct cyber and other non-kinetic activities. • Distributed network with service nodes at approximately 68 locations. • Forms a realistic and relevant live-fire cyberspace environment supporting Combatant Command, Service, Agency, and Test Community training, testing, and experimentation across the IO and cyberspace mission areas. • Can provide secure connectivity and transport for coalition partners. • Multiple simultaneous events at multiple levels of security. • Meets Capstone Concept for Joint Operations intent and provides a critical Joint Force cyberspace training and testing environment. It is the only "live-fire" range supporting cyberspace and IO related objectives in the Joint Training Enterprise.
National Cyber Range (NCR) Orlando, FL Contact E-Mail: osd.pentagon.ousd-atl.mbx.trmc@mail.mil	Provide realistic, quantifiable assessments of the Nation's cyber research and development technologies. The NCR will enable a revolution in national cyber capabilities and accelerate technology transition. Includes agile setup of Multiple Independent Levels of Security (MILS) sanitized Unclassified, Secret, or SCI environments for Program of Record testing.	• NCR can connect to the JIOR or operate in stand-alone mode. • Specialized software facilitates rapid network design, reconfiguration, and sanitization, as well as network scaling. • Security architecture enables a common infrastructure to be partitioned into MILS and leverage real malware. • End-to-end toolkit that automates the lengthy process of creating high-fidelity test environments. • Unique combination of expertise in cyber domain, cyber testing, Cyber Range management, and cyber testing tools.

F.3 Other Resources and Facilities

Resource/Facility	Mission	Capabilities

Joint Mission Environment Test Capability (JMETC)
Test Resource Management Center (TRMC)
Alexandria, VA
 	
Contact E-Mail:
osd.pentagon.ousd-atl.mbx.trmc@mail.mil
 	
Contact Phone Number(s):
571-372-2697
571-372-2701
571-372-2702
	JMETC provides the persistent, robust infrastructure (network, integration software, tools, reuse repository) and technical expertise to integrate Live, Virtual, and Constructive systems for test and evaluation in Joint Systems-of-Systems and Cyber environments.	• JMETC SECRET Network provides a distributed network infrastructure with 76 geographically separated nodes connecting Live systems, Hardware-in-the-Loop, Installed Systems Test Facilities, and Virtual/Constructive simulations representing the System Under Test on Range and Laboratory facilities.
		• JMETC Multiple Independent Levels of Security Network provides closed connectivity between and among Cyber Ranges, and Live, Virtual, and Constructive test assets at multiple levels of classification (S, TS, TS/SCI, SAP/SAR). JMN provides the ability to peer with JIOR.
		• JMETC also maintains and provides access to Regional Service Delivery Points (RSDP) which provides the ability to create virtualized cyber environments for cybersecurity testing. RSDPs:
		  ○ Are extensible to cyber ranges to create more complex, higher scale environments
		  ○ Provide enterprise compute, storage as well as hosting common tools and services for the Cyber T&E, Training, and Experimentation communities
		  ○ Are geographically distributed to minimize latency and accessed through the JMN. There are currently two deployed RSDPs with others planned for deployment.
		• Capabilities typically provided at no additional cost to the customer.

Appendix G. Examples of Common Vulnerabilities

Common vulnerabilities are defined in the current STIGs and vulnerability databases such as the National Vulnerability Database at http://nvd.nist.gov. Some examples of common vulnerabilities are defined below.

Password Practices

- Use of well-known default passwords on devices and software (failure to change default passwords)
- Poor user password practices (contrary to policy guidance)
- Improperly secured user identification (UID) and password lists stored and readable from the trusted network
- Passwords stored on network devices without encryption or with weak encryption
- Use of keyboard pattern password
- Pass-the-Hash exploit (Microsoft Active Directory vulnerability)
- Login credential discovered during Web searches (reconnaissance)

Privileged Access

- Standard user credentials with administrative privileges granted
- Use of shared administrator accounts
- Administrator accounts using identical UID/passwords across multiple server platforms
- Administrators using privileged accounts to access Internet Web servers
- Administrators using privileged accounts continuously

Access Control

- Use of unsecure ports and protocols (Port 80: Hypertext Transfer Protocol [HTTP])
- Use of prohibited ports and protocols
- Unsecure network services enabled on network devices and systems
- Secure Sockets Layer (SSL) vulnerabilities accepting invalid certificates
- Anonymous File Transfer Protocol (FTP) allowed
- Lack of Access Control Lists implemented on border router
- Phishing emails with SSL exploits

CNDSP Monitoring and Operations

- Inadequate detection of insertion of removable media (host-based security system)
- HBSS misconfiguration
- HBSS not monitored properly
- Unauthorized (rogue/malicious) devices installed on network not detected
- Use of physical intrusion devices not detected
- Unauthorized software installed on workstations not detected (host-based security system)
- Misconfigured Intrusion Detection Systems
- IDS not properly monitored

 Ineffective use of system audit logs
 Data exfiltration not detected
 Poor incident handling procedures
 Lack of Tier 3 network defense collaboration cell

Workstations and Server Configurations

 Non-secure configurations for hardware and software on mobile devices, laptops, workstations, and servers (noncompliant remediation of known vulnerabilities)
 Unpatched server and workstation vulnerabilities (Buffer Overflow and Code Injection vulnerabilities)
 Use of unauthorized software
 Unreliable software baselining practices (lack of adequate configuration management)
 SharePoint server unsecure/noncompliant configuration (unauthenticated, unrestricted access to files)
 SharePoint server failure to implement anti-virus scanning for file uploads
 Unsecured SharePoint server
 Noncompliance with software and hardware backup requirements
 Misconfigured services and vulnerable drivers
 Misconfigured servers
 Network credentials, system configurations, and network diagrams stored insecurely
 Web application vulnerable to Standard Query Language injection attack (input validation vulnerability)
 Unauthorized data manipulation due to weak data protections
 Operational information stored insecurely (no authentication or encryption used)
 Unsecured chat systems

Infrastructure

 No Wireless Intrusion Detection devices implemented
 Logging for infrastructure (network) devices not implemented
 Layer 2 virtual local area network software vulnerable (unpatched)
 Exploitation of two-way trust relationship between domains
 Physical security of critical components

Appendix H. Primary Stakeholders

The following is a definition of stakeholders and their responsibilities with regard to cybersecurity T&E. Primary stakeholders are identified with supporting stakeholders listed below them and indented.

1. **Deputy Assistant Secretary of Defense (Developmental Test and Evaluation):** Statute and policy prescribe the management of DT by the DASD(DT&E), who, for all programs on DASD(DT&E) oversight, acts as the final approval authority for DT&E planning in the TEMP. Office of the DASD(DT&E) staff representatives actively participate in acquisition program T&E WIPTs and provide advice to the T&E WIPT and PM, as well as providing independent assessments to DASD(DT&E) on progress of the test program and overall performance of the system.

2. **Director, Operational Test and Evaluation:** For programs under oversight, DOT&E oversees, reviews, and approves all operational test activities, TEMPs, and OTPs and will provide an independent report following all OT events.
   a. **Operational Test Agency:** The OTA) plans and executes testing in an operational environment including representative users and realistic threats. For cybersecurity testing, this includes both risk evaluation and operational resiliency testing. The OTA will prepare a TEMP and OTP to include critical issues, measures, data collection, and resources required, and provides a formal report of the operational test, including cybersecurity findings.

3. **Program Manager:** The PM is the designated individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment to meet the user's operational needs. The PM shall be accountable for credible cost, schedule, and performance reporting to the MDA (DoDD 5000.01). Management responsibility for an acquisition program's T&E resides with the PM. However, the planning, executing, and reporting of T&E involves interactions, support, and oversight from other organizations within OSD, the Services, Defense Agencies, and in some cases, other government agencies; as well as the system contractor(s). The PM charters a T&E WIPT early in the acquisition model to support development of test strategies and estimates of resource requirements, strengthening the overall input to the program's integrated product team. Specific cybersecurity guidance for the PM is provided in the *Cybersecurity Implementation Guidebook for Acquisition Program Managers* https://acc.dau.mil/CommunityBrowser.aspx?id=721696&lang=en-US.
   a. **Program Office:** The Program Office is responsible for providing the Components, developmental system, and the production representative SUT and facilitating coordination among the test WIPT for other resources needed to conduct the Cyber Operational Resiliency Evaluation.
   b. **Lead DT&E Organization:** The Component organization providing primary DT&E support.

c. **Chief Developmental Tester:** Title 10 U.S.C. 139b(c) requires that the Secretary of Defense shall require that each MDAP and MAIS program be assigned a Chief Developmental Tester. The Chief Developmental Tester is responsible for:

   i. Coordinating the planning, management, and oversight of all DT&E activities for the program

   ii. Maintaining insight into contractor activities under the program

   iii. Overseeing the T&E activities of other participating government activities under the program

   iv. Helping PMs make technically informed, objective judgments about contractor DT&E results under the program.

d. **Chief Engineer / Lead Systems Engineer:** Each PEO, or equivalent, is required by DoDI 500.2 to have a lead or Chief Systems Engineer on his or her staff responsible to the PEO for the application of SE across the PEO's portfolio of programs. The PEO lead or Chief Systems Engineer reviews assigned programs' System Engineering Plans (SEPs), oversees their implementation, and assesses the performance of subordinate lead or Chief Systems Engineers assigned to individual programs in conjunction with the PEO and PM. A Systems Security Engineer may be included in the Chief Systems Engineer's team to act as an SME for systems security.

4. **Test and Evaluation Working Integrated Product Team:** In addition to standard T&E WIPT members, SMEs who should be considered when chartering the WIPT include the following. Refer to the DAG, Chapter 9, for more information on the T&E WIPT.

a. **Information System Security Manager:** Develop and maintain an organizational or system-level cybersecurity program that includes cybersecurity architecture, requirements, objectives and policies, cybersecurity personnel, and cybersecurity processes and procedures; ensure that IOs and stewards associated with DoD information received, processed, stored, displayed, or transmitted on each DoD IS and PIT system are identified in order to establish accountability, access approvals, and special handling requirements; maintain a repository for all organizational or system-level cybersecurity-related documentation; Ensure that ISSOs are appointed in writing and provide oversight to ensure that they are following established cybersecurity policies and procedures; monitor compliance with cybersecurity policy, as appropriate, and review the results of such monitoring; ensure that cybersecurity inspections, tests, and reviews are synchronized and coordinated with affected parties and organizations; ensure implementation of IS security measures and procedures, including reporting incidents to the AO and appropriate reporting chains and coordinating system-level responses to unauthorized disclosures for classified information and CUI; ensure that the handling of possible or actual data spills of classified information resident in ISs, are conducted; act as the primary cybersecurity technical advisor to the AO for DoD IS and PIT systems under their purview; ensure that cybersecurity-related events or configuration changes that may impact DoD IS and PIT systems authorization or security posture are formally reported to the AO and other affected parties, such as IOs

and stewards and AOs of interconnected DoD ISs; and ensure the secure configuration and approval of IT below the system level (i.e., products and IT services) in accordance with applicable guidance prior to acceptance into or connection to a DoD IS or PIT system.

b. **Information System Security Officer:** Assists the ISSMs in meeting their duties and responsibilities; implements and enforces all DoD IS and PIT system cybersecurity policies and procedures, as defined by cybersecurity-related documentation; ensures that all users have the requisite security clearances and access authorization, and are aware of their cybersecurity responsibilities for DoD IS and PIT systems under their purview before being granted access to those systems; in coordination with the ISSM, initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered and ensure that a process is in place for authorized users to report all cybersecurity-related events and potential threats and vulnerabilities to the ISSO; and ensure that all DoD IS cybersecurity-related documentation is current and accessible to properly authorized individuals. .

c. **Security Controls Assessor:** The Component ISSO performs the security control assessment role for governed information technologies; establishes and oversees a team of qualified cybersecurity professionals responsible for conducting security assessments. DoD Component ISSOs may task, organize, staff, and centralize or direct assessment activities to representatives as appropriate. The SCA determines whether or not the selected controls for a system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system or enterprise. The SCA documents the planning for security controls assessment in the Security Assessment Plan. Post assessment, the SCA produces the Security Assessment Report, which documents the issues, findings, and recommendations from the security control assessment. The SCA must ensure that security control assessment activities are coordinated with DT and OT events (security control assessment activities should be documented in the TEMP). See DoDI 8510.01 for more information on the SCA.

d. **Blue Team and Red Team Representatives:** Representatives from vulnerability testing and threat representative testing organizations may be included in the WIPT.

5. **Other stakeholders external to the Program:**

a. **User Representative**: The User Representative is responsible for confirming and clarifying operational requirements, providing insights on operational conditions, reviewing all unresolved vulnerabilities and proposed work-arounds to identify effects on operations, and monitoring the conduct of the test events for operational realism and to provide inputs on operation implications of observed activities.

b. **Cybersecurity Service Provider or Computer Network Defense Service Provider:** The Cybersecurity Service Provider or CNDSP is identified in the system design and requirements documents and should be specified in the TEMP. The Cybersecurity Service Provider or CNDSP provides network connectivity and security (if applicable to the system).

c. **Authorizing Official:** AOs, appointed by the Component heads, are senior-level officials within a Component who have the authority to formally assume responsibility for operating an information system at an acceptable level of risk. The AO is responsible for ensuring that a system complies with the DoD CIO RMF process and makes system authorization decisions based on risk. The cybersecurity test process will provide the AO with data and information for those decisions. See DoDI 8500.01, DoDI 8510.01, and CNSSI 4009 for more information on the AO's roles and responsibilities.

Appendix I. Acronyms and Glossary of Terms

I.1 Acronyms

AO	Authorizing Official
ASR	Alternative Systems Review
AT&L	Acquisition, Technology, and Logistics
ATO	Authorization to Operate
C4	Command, Control, Communications, and Computers
C4AD	C4 Assessment Division
CAC	Common Access Card
CDD	Capability Development Document
CDR	Critical Design Review
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CNDSP	Computer Network Defense Service Provider
CNSSI	Committee On National Security Systems Instruction
CONOPS	Concept of Operations
COTS/GOTS	Commercial Off-The-Shelf/ Government Off-The-Shelf
CPD	Capability Production Document
CPI	Critical Program Information
CS	Computer Security
CTA	Capstone Threat Assessment
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DAG	Defense Acquisition Guidebook

DASD	Deputy Assistant Secretary of Defense
DECRE	DoD Enterprise Cyber Range Environment
DEF	Developmental Evaluation Framework
DIA	Defense Intelligence Agency
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Networks
DOT&E	Director, Operational Test and Evaluation
DT	Developmental Test
DT&E	Developmental Test and Evaluation
EMD	Engineering, Manufacturing, and Development
FD	Functional Design
FRP	Full-Rate Production
FTP	File Transfer Protocol
HBSS	Host-Based Security System
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IATT	Interim Authority To Test
IC	Intelligence Community
ICD	Initial Capabilities Document
IDS	Intrusion Detection System
IO	Information Operations
IS	Information System

ISP	Information Support Plan
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
JCIDS	Joint Capabilities Integration and Development System
JIOR	Joint Information Operations Range
JMETC	Joint Mission Environment Test Capability
JMN	JMETC Multiple Independent Levels of Security Network
KPP	Key Performance Parameter
KS	Knowledge Service
LCSP	Life-Cycle Sustainment Plan
MAIS	Major Automated Information System
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MILS	Multiple Independent Levels of Security
MS	Milestone
NCR	National Cyber Range
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OSD	Office of the Secretary of Defense
OT	Operational Test
OTA	Operational Test Agency
OT&E	Operational Test and Evaluation
OTP	Operational Test Plan

OTRR	Operational Test Readiness Review
OV	Operational View
PDR	Preliminary Design Review
PEO	Program Executive Officer
PIT	Platform Information Technology
PKI	Public Key Infrastructure
PM	Program Manager
POA&M	Plan of Action and Milestones
PPP	Program Protection Plan
RFP	Request for Proposal
RMF	Risk Management Framework
RMF KS	Risk Management Framework Knowledge Service
SCA	Security Controls Assessor
SCI	Sensitive Compartmented Information
SE	Systems Engineering
SEP	System Engineering Plan
SoS	System of Systems
SP	Special Publication
SSL	Secure Sockets Layer
STAR	System Threat Assessment Report
STIG	Security Technical Implementation Guide
SUT	System Under Test
SV	Systems Viewpoint
TAC	Threat Analysis Center

TEMP	Test and Evaluation Master Plan
T&E	Test and Evaluation
TMRR	Technology Maturation and Risk Reduction
TRD	Technical Requirements Document
TRR	Test Readiness Review
TTPs	Tactics, Techniques, and Procedures
UID	User Identification
WIPT	Working Integrated Product Team

I.2 Cybersecurity T&E Glossary of Terms

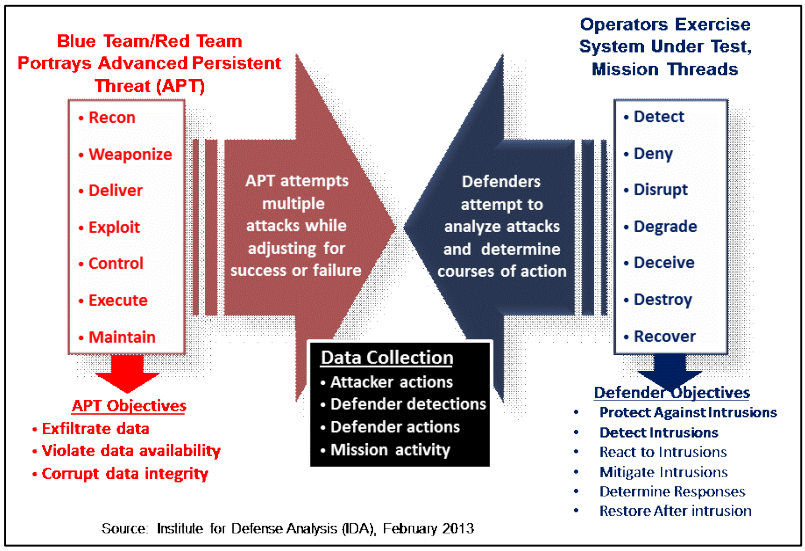
The following are definitions of terms useful for Cybersecurity T&E. Unless specified, all definitions are from CNSSI 4009.

Blue Team

The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically the Blue Team and its supporters must defend against real or simulated attacks 1) over a significant period of time, 2) in a representative operational context (e.g., as part of an operational exercise), and 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team).

The term Blue Team is also used for defining a group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cyber security readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems. For additional information on their application during T&E, refer to Defense Acquisition Guidebook, Chapter 9, T&E.

Cyber-attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Cyber-attack surface	The system's use of COTS, GOTS, planned system interfaces, protocols, and operating environment that represents a collection of vectors threats may use to access, disrupt, destroy, or deny use of a network service, information system, or other forms of computer based system. Vectors include, but are not limited to: hardware flaws, firmware, communications links (local area network, wide area network, wireless, etc.), physical interfaces (Universal Serial Bus, Firewire), software (operating system applications, basic input/output system), and open communication ports and communication protocols (HTTP, FTP, PPP).
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. (DoDI 8500.1)
Cybersecurity kill chain	A sequence of actions performed by a specified threat adversary that executes cyber intrusions with specific objectives, such as data theft. Although there are variations of the kill chain, the typical adversary stages include: reconnaissance, weaponization, delivery, exploitation, control, execution, and persistence. (Defense Acquisition Guidebook). See Figure 12, section 3.3.4.4.



Cybersecurity requirements	Those requirements levied on an information system as defined in the *Manual for the Operation Of The Joint Capabilities Integration And Development System* (JCIDS Manual), 12 February 2015, and that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. PMs for programs acquiring IT or PIT systems in accordance with DoDI 5000.02 must integrate the security engineering of cybersecurity requirements and cybersecurity testing considerations into the program's overall SE process, and document this approach in the program's Systems Engineering Plan and PPP. Working in concert with the Chief Developmental Tester, the SE activities will also conduct integration and tests of system elements and the system (where feasible), and demonstrate system maturity and readiness to begin production for operational test and/or deployment and sustainment activities.
Enclave	An enclave is a set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.
Implied cybersecurity requirements	Implied cybersecurity requirements (also sometimes called derived requirements) are those that can arise from technology choices, such as the use of COTS/GOTS, planned system interfaces, and protocols.
Interim Authority to Test (IATT)	Temporary authorization to test an information system in a specified operational information environment within the time frame and under the conditions or constraints enumerated in the written authorization. Per DoDI 8510.01 IATTs should be granted only when an operational environment or live data is required to complete specific test objectives (e.g., replicating certain operating conditions in the test environment is impractical), and should expire at the completion of testing (normally for a period of less than 90 days). Operation of a system under an IATT in an operational environment is for testing purposes only (i.e., the system will not be used for operational purposes during the IATT period). The application of an IATT in support of DT&E needs to be planned, resourced, and documented within the program T&E plan.

Platform IT	Platform IT is defined as information technology, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. Examples of platforms that may include PIT are: weapons systems, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical devices and health information technologies, vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.), utility distribution, telecommunications systems designed specifically for industrial control systems including supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering, including associated data transport mechanisms (e.g., data links, dedicated networks).
Qualified and certified	Red Teams and Blue Teams must be appropriately qualified and certified. Red Teams are certified by a board at NSA and accredited through Strategic Command to ensure that they are able to traffic the threads of cyberspace without doing harm to government systems. This stringent accreditation process is required every three years, and teams that do not fall in compliance are not allowed to access the DoDIN. The evaluation identifies the authorities that establish the respective service Red Team. (Based on CJCSM 6510.03)
Red Team	A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. For additional information on their application during T&E, refer to Defense Acquisition Guidebook, Chapter 9, T&E.
Test and Evaluation Working Integrated Product Team	A team formed by the PM that provides a forum for development of the T&E strategy, TEMP, and resolution of T&E issues. T&E oversight representatives may participate in or observe WIPT deliberations. To be effective, the T&E WIPT should have a charter empowering it that has been coordinated among all the member organizations. (Defense Acquisition Guidebook).

Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. This should be planned for and resourced within the programs T&E Master Plan and executed within DT&E (during the EMD phase), utilizing a Blue Team type activity to assist in the assessment. For more information, refer to Defense Acquisition Guidebook, Chapter 9, T&E. (NIST SP 800-39)

Appendix J. References

Additional information on RMF

- DoDI 8500.01, *Cybersecurity*, March 14, 2014.
- DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, March 12, 2014.
- RMF Knowledge Service at https://rmfks.osd.mil for documentation, tools, and information about DoD implementation of the RMF.
- NIST Special Publication 800-37 at http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf for information on RMF.
- CNSSI 1253 at http://www.sandia.gov/FSO/PDF/flowdown/Final_CNSSI_1253.pdf for information on system categorization.
- NIST Special Publication 800-53 at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf for security controls.

References for Cybersecurity T&E

- DOT&E Memorandum, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, August 1, 2014.
- DoD CIO Guidance, "Cybersecurity (CS) Implementation Guidebook for Acquisition Program Managers," currently in coordination.
- *Defense Acquisition Guidebook*, Chapter 9, under Cybersecurity T&E.

Other References

- *Manual for the Operation Of The Joint Capabilities Integration And Development System* (JCIDS Manual), 12 February 2015, https://dap.dau.mil/policy/Documents/2015/JCIDS_Manual_-_Release_version_20150212.pdf
- DoDI 5000.02, *Operation of the Defense Acquisition System*, January 7, 2015, particularly Enclosures 4 and 5 on DT&E and OT&E, respectively.